ACS10692 v1

Report No: ACS10692A

Socialist Republic of Vietnam

Study on e-ID Infrastructure to Improve Public Services Delivery

Electronic Identification Technical Report

April, 2015

GTIDR

EAST ASIA AND PACIFIC

Standard Disclaimer:

This volume is a product of the staff of the International Bank for Reconstruction and Development/ The World Bank. The findings, interpretations, and conclusions expressed in this paper do not necessarily reflect the views of the Executive Directors of The World Bank or the governments they represent. The World Bank does not guarantee the accuracy of the data included in this work. The boundaries, colors, denominations, and other information shown on any map in this work do not imply any judgment on the part of The World Bank concerning the legal status of any territory or the endorsement or acceptance of such boundaries.

Table of Contents

FIGURES AND TABLES

Abbreviations

Abbreviation	Expanded Form
AEBA	Aadhaar Enabled Bank Account
AES	Advanced Encryption Standard
AITA	Authority of IT Applications
ANSI	American National Standard Institute
APB	Aadhaar Payment Bridge
API	Application Programming Interface
ASA	Authentication Service Agency
ATM	Automated Teller Machine
AUA	Authentication User Agency
BC	Banking Correspondent
BFD	Best Finger Detection
BIN	Bank Identification Number
BoV	Bank of Vietnam
CA	Certification Authority
CBS	Customers/Beneficiaries/Subscribers
CBS	Core Banking System
CIC	Credit Information Center
CIDR	Central Identities Data Repository
CMB	Citizen Migration Board
CRIDS	Central Resident e-Identity Data Store
CRL	Certificate Revocation List
CSP	Certificate Service Providers
DDoS	Distributed Denial of Service
DDSVP	Demographic Data Standards and Verification Procedure
DIT	Department of Information and Technology
DMZ	Demilitarized Zone
DoB	Date of Birth
DoS	Denial of Service
EESA	ESignature Act
DSS	Decision Support System
ESS	ESignature Service
ECB	Electronic codebook
EIDAV	Electronic Identity Authority of Vietnam
eDocument	Electronic Document
eEBA	eID-enabled Bank Account

Abbreviation	Expanded Form
EHR	Electronic Health Record
eID	Electronic Identity
EISDF	Electronic Identity Service Delivery Framework
EISDP	Electronic Identity Service Delivery Platform
eKYC	Electronic Know Your Customer
EMS	Enterprise Monitoring Software
ePayment	Electronic Payment
ePB	eID Payment Bridge
eSP	eID Seeding Platform
FIR	Fingerprint Image Resolution
FIPS	Federal Information Processing Standards
FMR	Fingerprint Minutiae Resolution
GB	Gigabyte
GbE	Gigabit Ethernet
GoV	Government of Vietnam
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
HMAC	Hash-based Message Authentication Code
HTTP	Hyper-text Transmission Protocol
HTTPS	Hyper-text Transmission Protocol Secure
HVAC	Heating, Ventilation, and Air Conditioning
ICT	Information and Communication Technology
IDA	Identity Documents Act
IIR	Iris Image Resolution
IP	Internet Protocol
ISCA	Identity Service Consumer Agency
ISMS	Information Security Management System
ISO	International Standards Organization
ISPA	Identity Service Provider Agency
IT	Information Technology
ITU	International Telecommunication Union
IVR	Interactive Voice Response
KYC	Know Your Customer
KYR	Know Your Residence
LDAP	Lightweight Directory Access Protocol
LoB	Line of Business
LPG	Liquid Petroleum Gas
MB	Megabyte

Abbreviation	Expanded Form
MBPS	Megabits per Second
MIC	Ministry of Information and Communications
MIS	Management Information System
MISP	Managed Identification Service Provider
MIT	Ministry of Information Technology
MoE	Ministry of Environment
MoET	Ministry of Education and Training
MoF	Ministry of Finance
MoH	Ministry of Health
MoLISA	Ministry of Labor, Invalids and Social Affairs
MNO	Mobile Network Operator
MPS	Ministry of Public Security
NAF	National eAuthentication Framework
NEPS	National Electronic Payment Service
NESP	National Electronic Identity Seeding Platform
NFC	Near Field Communication
NID	National Identity System
NIDAV	National Identity Authority of Vietnam
NIN	National Identification Number
NIPS	Network Intrusion Protection System
NISDF	National Identity Service Delivery Framework
NISDP	National Identity Service Delivery Platform
NREGS	National Rural Employment Guarantee Scheme
NSP	Network Service Provider
OCSP	Online Certificate Status Protocol
OTA	Over-the-air
OTP	One-time Password
PAN	Permanent Account Number
PC	Personal Computer
PDCA	Plan-Do-Check-Act
PDPA	Personal Data Protection Act
PID	Personal Identity Data
PIN	Personal Identification Number
PKCS	Public Key Cryptographic Standards
PKI	Public Key Infrastructure
PoA	Proof of Address
PoI	Proof of Identity
PoP	Points of Presence

Abbreviation	Expanded Form
PoS	Point of Sales
PPP	Public Private Partnership
PSU	Public Service Undertaking
PUB	Publication
PUE	Power Usage Effectiveness
PUK	Personal Unblocking Key
QA	Quality Assurance
RA	Registration Authority
RAM	Random Access Memory
RDBMS	Relational Database Management System
RPM	Revolution per Minute
SAN	Storage Area Network
SAS	Serial-attached SCSI
SBV	State Bank of Vietnam
SDK	Software Development Kit
SHA	Secure Hash Algorithm
SI	Solution Integrator
SIM	Subscriber Identification Module (in physical, software or other forms)
SLA	Service-Level Agreement
SMS	Short Message Service
SMSC	Short Message Service Center
SOAP	Simple Object Access Protocol
SQL	Structured Query Language
SSCD	Secure Signature Creation Device
SSL	Secure Socket Layer
SSO	Single Sign-on
STQC	Standardization Testing and Quality Certification
TA	Technical Assistance
TB	Terabyte
ToR	Top of Rack
TPS	Transactions per Second
TSP	Trusted Service Provider
TSP	Timestamp Service Provider
UID	Unique Identification Number
UIDAI	Unique Identification Authority of India
UPS	Uninterrupted Power Source
URL	Uniform Resource Locator
USSD	Unstructured Supplementary Service Data

Abbreviation	Expanded Form
VGCA	Vietnam Government Certification Authority
VM	Virtual Machine
VNPT	Vietnam Posts and Telecommunications Group
VSS	Vietnam Social Security
W3C	World Wide Web Consortium
WPKI	Wireless Public Key Infrastructure
XAdES	XML Advanced Electronic Signatures
XML	Extensible Markup Language

Executive Summary

Government ministries and private sector organizations in Vietnam today face the challenge of having a unique identification number for identifying and authenticating residents at service delivery. The Government of Vietnam (GoV) recognizes this challenge, and is proactively piloting a new National Identity System (NID)

GoV has also has expressed interest in exploring the deployment of a full-fledged electronic identity-based service delivery framework. Such an electronic system could be developed based on the new NID system being piloted. In response to GoV's request, the World Bank is conducting a Technical Assistance (TA) activity to define the vision and strategy, and provide recommendations pertaining to its implementation. The study pays close attention to innovative Electronic Identity (eID) systems to enhance the accountability and efficiency of the service delivery.

The vision and implementation strategy suggested for the Electronic Identity-based Service Delivery Framework (EISDF) in Vietnam was developed based on the experiences of countries like India, Estonia and Belgium. The current state of Vietnam's information technology (IT) infrastructure and her institutional framework were also taken into consideration.

The lessons learned from international experiences cover key concepts such as the: (i) extension of the national identity system capabilities to include eID; (ii) eID profile of the resident which comprises of a unique National Identification Number (NIN), linked to demographic and biometric data that is accessible online; (iii) eID profile and NIN creation as a centralized biometric and deduplication process at the national level to ensure uniqueness; and (iv) eID profile could clearly establish the resident's identity to public and private agencies across the country, although it may not necessarily be used to prove citizenship.

The eID authentication service is one of the key offerings of a central identity authority on a national infrastructure. The purpose of eID authentication is to enable eID-holders to prove their identity digitally and online, and for service providers to be able to confirm the residents' identity claim in order to correctly deliver services and benefits. Other key services offered include eID seeding where the NIN is embedded in the service provider databases; electronic Know-Your-Customer (eKYC) process; electronic payment (ePayment); secure electronic document (eDocument); and mobile ID.

The technical learning involves setting up a highly secure Central Resident eID Data Store (CRIDS) to collect the demographic and biometric data gathered from the enrollment process following a

procedure of deduplication. The subsequent NIN is generated at random to prevent fraud and theft. The biometric data ensure uniqueness and are required to be used in conjunction with the demographic data.

The eID processes, such as eID authentication, eKYC, mobile ID, etc., may be exposed as a stateless web services emanating from the centralized eID infrastructure and extracting information from the CRIDS. The eID authentication may be single- or multiple-factor, and factors may be demographic, biometric, one-time password (OTP), digital certificate, or their combination. The interoperability of biometric authentication is supported by defining biometric device specifications, data standards and common software development kit (SDK), and application programming interface (API) across multiple device vendors. The IT infrastructure for running eID processes could be supported by fulltime domestic in-house technical capacity and in-country proven technology from local vendors. The design of the proposed eID system could ease the integration of existing/planned services of the GoV with those of the private sector.

The use of mobile ID would simplify eID authentication and eSignatures, by replacing the smart card and reader with the mobile phone and specialized SIM (could be a physical card, software, or other relevant subscriber identification mechanisms) issued to residents. The mobile ID could use biometrics or digital certificate with the implementation of a wireless public key infrastructure (wPKI) and the mobile gateway of a nationalized mobile network operator (MNO). The biometrics or digital certificate type authentication and eSignatures could use communication model-based services on the common standardized workflows, document format and open standards technologies. The GoV could set up a one-stop eGovernment portal for eServices offered by the various government agencies, and act as the gateway to all public offices.

The institutional learning also suggests an organizational structure with two separate government bodies: the overall regulator and overseer of eID services. The individual identity remains unique and independent of the service provided. There could be a cross-ministerial apex committee at the highest level of government as the decision makers for eID and related issues. A scalable public-private partnership (PPP) organizational structure would be needed to deliver highly secure and high-quality eID. A strong level of security is achieved by restricting direct access to the online eID process to a few authorized organizations defined as an eID service provider agency (ISPA); and only an eID consumer service provider (ISCA) registered under the former may request identity information for delivery.

The mobile ID, biometrics or digital certificate, and eSignature may require a PPP organizational structure to issue mobile ID SIM and activate them. These responsibilities could be assigned to one – or more – nationalized MNO, and they could include the generation of biometrics or digital

certificates and timestamps to the certificate service provider (CSP) and timestamp service provider (TSP), respectively. The eSignature Act (EESA) could define the roles and responsibilities pertaining to the issuance of eSignatures. The GoV creates the standard committees – with members from both public and private sectors – and defines the standards such as demographic and biometric data, technology and business processes.

The operating model learning necessitates the fresh enrollment of residents for eID. This is recommended – in lieu of reusing previous data entered by different government departmental applications – to ensure high-quality data. The eID is based on a secure and scalable PPP-based operating model wherein only the ISPA (public or private) has direct access. The ISCA, in turn, calls its designated ISPA for assistance with retrieving the eID information to fulfill its service delivery function. The central government agency responsible for eID could host a public-facing portal to build technical awareness and to provide technical support to the user-agencies. There could be a certification process for biometric devices to ensure their compliance with GoV specifications.

The operating model for mobile ID is also PPP-based, with the mobile ID provided by one or more operators through local outlets. The resident could activate the service on the handset with the new specialized SIM. The service provider could request the eID from the resident through short message service (SMS) using a TSP, referring to the global system for mobile communications (GSM) subscriber number, and/or require the entry of a personal identification number (PIN) for authentication. The GoV could set up round-the-clock call centers and online services, such as DocStop and CheckDoc, to prevent frauds.

The policy intervention learning suggests the creation or update of the Identity Documents Act (IDA) to establish national guidelines for the creation of the NIN, the National Identity System (NID) card, and the eID. It could grant the eID equal value to the paper-based identity document. The ESA could make digital and paper-based handwritten signatures legally equivalent. The Personal Data Protection Act (PDPA) could also be updated to regulate the use of personal data and databases by public authorities and private agencies. The service providers in both the public and private sectors may also update their KYC norms to include eID and eKYC functions.

Currently, the most common Proof of Identity (PoI) used by service providers in both the public and private sectors is the People's Identity Card issued to residents by the Ministry of Public Security (MPS). Reliance on this card proves to be a challenge as it is paper-based and issued at the provincial level, with no mechanism to ensure its uniqueness at the national level. As a result, service providers may ultimately find this practice costly due to inconsistent and duplicate identities. The paper-based identity card also results in a greater risk of identity theft.

There is a need for the development of a more robust and effective national identity system. This could entail a national-level unique identity creation process based on an EISDF. Such a system is currently under implementation by GoV.

There is also a demand for a national eID for Vietnam residents for Internet-use purposes. This will encourage the use of eGovernment, foster innovation in public and private eServices, and strengthen cybersecurity. The eID will enable residents to request and receive services and benefits from public and private sector agencies anywhere, anytime, and using any device without the need to be physically present for identity authentication purposes.

The proposed vision for the EISDF would include services such as authentication, seeding, eKYC, eSignature, ePayment, and mobile ID. The eID could support different types of standardized tokens based on: (i) "what the user has" such as mobile/OTP/biometrics/digital certificate; (ii) "what the user knows" such as a PIN; and (iii) "who the user is" such as fingerprints and iris images.

The implementation strategy for the EISDF would entail the setting up of a shared, centralized IT infrastructure and common services platform called the eID Service Delivery Platform (EISDP). The EISDP will be used for delivering eID services and common applications to service providers in order to uniquely identify residents. The key components of this centrally hosted platform are a common public portal as the online one-stop shop for all eID services, and common applications such as CRIDS, Management Information System (MIS), Decision Support System (DSS), Fraud Analytics, and ISCA/ISPA registration.

The IT infrastructure consisting of hardware and software could be deployed in data centers to run the applications and eID services. The physical infrastructure would include the Electronic Identity Authority of Vietnam (EIDAV) data center, the EIDAV disaster recovery data center (geographically separate from the EIDAV data center) and the NID system's data center. The safety and security systems include an end-to-end IT network, hardware and software security systems, and physical infrastructure with multiple-level safeguards designed to limit entry to authorized personnel using biometric data.

Each ISPA could set up a data center with the required IT infrastructure, software applications and secure network connectivity to the EIDAV data center to access eID services. Each ISCA could also set up a data center for hosting its online service delivery applications and Point of Sales (PoS) terminals where the resident could go to avail of services. The ISCA sets up the required IT network to connect its outlets to its data center, and then to the ISPA data center to forward its eID service request to the EISDP, before receiving the response the same way back.

The institutional framework includes operating model recommendations such as the creation of a separate agency, EIDAV, operating under a responsible ministry for eID, and as the owner and overseer of the EISDF and eID services. The responsible ministry would could delegate the responsibility of designing, implementing and managing the operations to EIDAV,, that will serve as the managed identification service provider (MISP). The public or private sector agencies wishing to use eID services in their delivery process could register as an ISCA. The ISCA could be enabled by an ISPA to access the services via the latter's network. Only an ISPA, public or private, may register with EIDAV for direct access to eID information to ensure high-level security for the centralized database. The service provider would be responsible for seeding the NIN into its own database; it is also responsible for the digitization and centralization of its database. EIDAV could provide eID tools and guidance to support the service provider in the seeding process. The four main operating functions for mobile ID service could be SIM provisioning, certification/user activation, usage, and termination.

The institutional recommendations touch on defining and allocating key roles to the elements of the organizational structure. EIDAV, operating under a responsible ministry for eID, could have the key role as the owner and overseer of the implementation and operational management of the EISDF and eID services. An MISP could be responsible for implementing the EISDF on behalf of EIDAV. An ISPA could be a public or private sector agency tasked with establishing a secure connectivity with EIDAV data center to transmit eID authentication requests on behalf of an ISCA, and then receive response back from eID authentication servers to ensure high-level security. The ISCA could be a public or private service-providing agency seeking to use eID services, and the eID-holder could be a resident who has been issued an eID by EIDAV. The key players in the delivery of mobile ID service, apart from those described above, could be the registration authority (RA), such as an MNO responsible for the provisioning of specialized SIM to the residents; a trusted service provider (TSP) that is also a mobile operator, but responsible for forwarding the mobile ID service request response from EIDAV to the mobile phone of the resident; and a certification authority (CA) responsible for the issuance and validation of certificates and signed data in response to the TSP service request.

The policy recommendations consist of updating or creating a new IDA to establish the national guidelines for the issuance of the NIN, ensuring that the eID has the same legal value as the NID card, updating the ESA to use the EISDF eID services for the delivery of eSignatures, and establishing that the eSignature has the same legal value as that of the handwritten kind.

For the eKYC response to be treated as a valid legal equivalent of a paper-based document, the relevant policies in the government may need to be updated. The service providers in both the public and private sectors could update their KYC norms to include the NIN/eID, and accept the

eKYC response as the valid KYC. The existing national open standards policy to promote interoperability could be updated to include demographic and biometric attributes for the eID profile of the resident in the metadata and data standards, and open standards for biometric data such as fingerprint images, fingerprint minutiae and iris images. A PDPA may need to be enacted to regulate the use of personal information by public authorities and private entities.

The proposed communication strategy for building awareness and promoting the adoption of the framework among key stakeholders includes setting up a public-facing portal, online and classroom trainings, capacity-building programs targeted at residents and officials/operators, promotions and incentive programs, technical documentation targeted at software professionals and technical decision makers who may be interested in availing of eID services.

The implementation of the EISDF may be done in two phases: the pilot and complete rollout. The pilot phase will see the establishment of the EISDF; and the responsibility of establishing EIDAV could be delegated to the responsible ministry. This will entail setting up the EIDAV data center and migrating the residents' data from the MPS's current pilot project to the CRIDS. It could also include the implementation of the following functions: eID authentication, eKYC, eID seeding, and mobile ID. There could be two ISCAs and one ISPA. For mobile ID, EIDAV could delegate the design and implementation to either Viettel or the Vietnam Post and Telecommunications Group (VNPT) that could take up the role of the RA and TSP.

The elevated budget estimate for the design and implementation of the pilot project and the complete rollout is for guidance only. It provides for the possible magnitude of investment required for the EISDF's design and implementation. The total investment for the pilot phase design, implementation and operations management for one year (without the implementation of mobile IDs) is estimated at USD 54 million. That includes the setup and implementation of the IT and institutional infrastructures for the centralized EIDAV, one ISPA and two ISCAs. Each ISCA could have one service delivery outlet in the urban district of Hanoi. The ISPA selected for the pilot may be Viettel or VNPT; and the ISCA may be the Vietnam Social Security (VSS) or the Bank of Vietnam (BoV). The RA and TSP could be Viettel or VNPT. The demographic and biometric data to be stored in EIDAV's CRIDS could be imported from the database with resident data captured for its current national identity system pilot. It is estimated that the pilot-captured data covers at least for one million residents. The budget estimate for the pilot is based on the delivery of 100,000 mobile IDs. The total investment for the complete rollout in five years of operations is estimated at USD 192 million. This estimate would include augmentation to the capacity of the IT and institutional infrastructures set up during the pilot. Also to be added are one more ISPA and about 20 more ISCAs with expected outlets of 124 (one per province and one per 10 districts) each. Ten additional RAs would be set up with 100 outlets for each RA, and two additional TSPs.

Also included in the cost are the capacity-building efforts, and setup of the framework standards and government policies that would be required for the implementation of the EISDF and the eID. The total budget for the design and the implementation of the two phases without the implementation of optional mobile ID is estimated at USD 246 million.

The budget estimates for the implementation of the optional mobile IDs in the pilot phase is an additional USD 4 million. This would include the delivery of 100,000 mobile IDs, one RA and one TSP in the pilot phase. The budget estimates for the implementation of the optional mobile IDs in the rollout phase is USD 61 million. This would include the delivery of 90 million mobile IDs, two RAs, one TSP and 124 RA service delivery outlets each. The eID and eID services could not be viewed as a standalone project. Rather the recommendations for eID and eID services will require a strong national ID foundation, especially in the areas of legislation, policies and standards, for a successful implementation.

This document could serve as the foundation for developing a detailed EISDF vision and implementation plan. The effective implementation of the EISDF would require a detailed breakdown of its high-level architecture into its technical components, taking into consideration the detailed as-is status of the IT infrastructure. A detailed implementation plan would also require policy and organizational structures, an operating model, infrastructure resources, and a phased rollout of the components.

1.0 Introduction

1.1 Purpose

This study proposes the vision and implementation recommendations for the Electronic Identity-based Service Delivery Framework (EISDF) in Vietnam. It also delineates the roles to be played by the diverse stakeholders (private, public, development community, etc.) in the field. The study recommends various relevant and innovative Electronic Identity (eID) services that can be implemented to transform and enhance the accountability and efficiency of service delivery across sectors. These recommendations are based on the stocktaking of international experiences and identified possibilities based on the country assessment. Special emphasis is placed on eID systems that operate on mobile phones, and on those that have the potential of being scaled up by both the public and private sectors in Vietnam.

1.2 Background and Rationale

Evidence shows that national eID service delivery systems offer a variety of benefits to individuals, businesses and governments. The expansion of national identity systems to eID using digital and biometric technologies can widen the scope of formal identification systems that is a prerequisite to development. Clearly, the inability to authenticate one's self inhibits an individual's access to basic rights and services from the public and private sectors.

The eID is considered a key enabler of innovation in the public and private sectors as they facilitate greater electronic authentication; it also facilitates improved value services that require a high level of security assurance. The use of eID has economic benefits in terms of reducing costs and increasing productivity in the public sector, as well as fostering usability of online services. Increased trust or assurance with regard to identities online – even bi-directional trust between parties transacting or communicating online – gives all participants an all-around edge.

The eID systems can help reduce identity fraud and enable individuals to avail of services more securely in a variety of contexts as in mobile banking and mobile applications for health care. Because identity theft is becoming a substantial challenge, governments from various parts of the world are putting in place eID-based service delivery systems. Such systems facilitate the delivery of benefits to those entitled, e.g., the poorest of the poor (those eligible to receive social benefits, disaster relief aid, etc., as in Kenya or Pakistan) and older people (for instance, pensioners in Nigeria). They also make possible the delivery of services like conditional cash transfers (for educational purposes like in India and Tanzania).

The private sector's role in deploying eID-based service delivery infrastructure could be critical because it can potentially ensure the financial viability and sustainability of the project. A number of countries, such as Belgium, Estonia and India, have successfully deployed eID systems based on Public-Private Partnership (PPP) models.

Most of the government ministries and private sector organizations in Vietnam today face the challenge of not having a unique identity designation for every resident. This could be due to the lack of a centrally generated national system of uniquely identifying a resident. The current national identity card is issued at the commune level; therefore, the identification number issued to the resident is not unique across the country.

Given this context, the Government of Vietnam (GoV) has expressed interest in exploring the deployment a full-fledged Electronic Identity-based Service Delivery Framework (EISDF). GoV is already piloting a new national identity system. In addition, the GoV is putting in place the necessary prerequisites for its deployment: a Public Key Infrastructure (PKI) and the issuance of compulsory national identity cards. The GoV is also planning to develop a National eAuthentication Framework (NAF) that will create the much-needed enabling environment for users to access government services and social benefits using eID. Going forward, the GoV is keen to leverage these infrastructures to maximize public investment and strengthen eGovernment and public service delivery to Vietnamese citizens, especially the poorest.

Given this background, the study aims to provide the vision and implementation strategy for eID-based service delivery in Vietnam. The study also pays special attention to innovative identity services to enhance the accountability and efficiency of service delivery. It will showcase such systems, and offer options for sharing risks, investments and benefits through PPP.

2.0 Methodology

The methodology of this study is based on a three-step approach, consisting of the following activities.

1. Review international eID-based service delivery experiences. This is necessary in order to determine the key factors that affect the implementation and adoption of eID, and to identify best practices applicable to Vietnam based on common eID concepts, technical and institutional aspects, and policies.

2. Define the vision for eID in Vietnam based on the lessons learned from international experiences.

3. Propose recommendations on the eID vision and implementation strategy based on the analysis of the current availability of information technology (IT) infrastructure and institutional framework in Vietnam.

The study's mode of research is described below.

1. Gather secondary data through desktop and field research in collaboration with the relevant stakeholders.

2. Gather information about international best practices through desktop research, particularly information related to international eID-based service delivery.

3. Conduct extensive in-country consultations with key stakeholders to gather their understanding and suggestions for implementation. This includes gathering information on the current national identity system, related information and communication technology initiatives, the enabling environment and infrastructure.

4. Collect inputs from key stakeholders, collaborate with relevant players in related activities, and promote the findings among relevant institutions such as the various ministries – notably the Ministry of Public Security, Ministry of Information and Communications, Ministry of Labor, Invalids and Social Affairs, Ministry of Education and Training, Ministry of Justice, Ministry of Home Affairs, Ministry of Health, and Ministry of Agriculture and Rural Development). Other players include the Authority of IT Applications (AITA), the State Bank of Vietnam, private banks, major telecommunications companies, and the Vietnam Government Certification Authority.

3.0 Lessons Learned from International Experiences

The Government of Vietnam (GoV) has various options to implement Electronic Identity (eID) services. Some of the key findings in terms of the common concepts, as well as technical and institutional aspects, that could impact implementation are described below based on experiences of the countries studied; namely India, Estonia and Belgium. Annex 5 provides detailed description of the respective experiences of these countries.

Common Concepts. Some of the common concepts in eID services learned from the experiences of India, Estonia and Belgium are discussed below.

1. **National Identity System Extended to Include Electronic Identity.** The NID system of a country could be extended to support eID that is verifiable online. The key benefit is the availability of mobile identity (ID) which enables service providers to authenticate individuals as the same and unique person, anywhere and anytime. It also supports removal of duplicate and fake identities thereby enabling higher scalability of services, allowing service agencies to use multiple channels for service delivery, reducing beneficiary harassment and rent-seeking due to reduced dependency on manual processes, supporting more efficient service delivery, providing an electronic audit trial, and reducing cost and risk of identity theft.
    a. The NID of a resident could be extended to include a unique eID profile which comprises a unique NIN linked to a resident's demographic and biometric data that is accessible online.
    b. The creation of a national eID profile with the NIN would be a centralized process with biometric deduplication at the national level to enable a unique identification acceptable to all service providers in the public and private sectors as legal Proof of Identity (PoI). There would be an infrastructure for the creation of the NID system and the delivery of eID services.
    c. The NIN and eID would prove the identity of an individual, but not the citizenship of a resident (e.g., India case).
    d. The NIN would identify a resident and provide means to clearly establish the identity to public and private agencies across the country. The three key characteristics of the NIN would be permanency (it remains the same during the entire resident's lifetime), uniqueness (no two residents may have the same NIN) and global usage (the same identifier can be used across applications and domains).

2. **Electronic Identity Authentication.** The purpose of eID authentication is to enable eID-holders to prove their identity digitally and online; and for service providers to be able to confirm the resident's identity claim to facilitate service delivery and access to benefits.
    a. The NIN and eID authentication process would be used by service providers to establish presence and proof of service delivery, and Know-Your-Customer (KYC) credential. It would also serve as a unifier of resident-centric information.
    b. The eID authentication enables beneficiary confirmation to ensure that services are being delivered to the right people. It would also supports attendance tracking in cases where wages are linked to actual number of days a beneficiary reports for the program.
    c. The eID authentication supports identity and address verification for establishing KYC credential which is a key requirement for enrolling or opening an account for a new customer. The use of the eID authentication would substantially reduce the cost of the KYC process. It would also be used as general proof of identity for standard security-related requirements in such places as airports, hotels, and other establishments; and as identity proof in school examinations. It would also be used for demographic data and address verification in service delivery databases which would help in database cleansing and management.

3. **Seeding of the National Identity Number.** In order for service providers to leverage eID assistance in delivering their product, they would have to first capture the unique NIN of their customers, beneficiaries, and subscribers (CBS). Once this is obtained, the service providers will then map and store it with their own unique identifier (e.g., customer or beneficiary number) in their respective databases. The process by which the NINs of the CBS are included in the database of a service provide is referred to as eID seeding. The seeding process would necessarily be preceded by digitization and centralization of information in the database of the service provider, and would support both the top-down and organic methods.
    a. The top-down method would use existing personal data of the resident from a previous enrollment process and would not require direct contact with the resident. However, the organic method would require the service provider to contact the resident, or vice-versa, for the seeding process to take place. The completion of the seeding process would be followed by demographic or biometric authentication, especially when no direct update of the service delivery database is enabled.

b. The seeding process would be designed to handle common challenges of service delivery databases. This includes incomplete data or repeated information across different data sources or languages.
c. The owner-government agency would provide a centralized seeding platform and seeding utilities that can be used by the service providers to perform the process accurately, faster and seamlessly. This would be critical for a faster adoption of eID-enabled service delivery.

4. **Providing Support Groups and Artifacts.** The owner-government agency would build support groups and a set of artifacts to help the service providers to adopt and implement the eID service delivery process. The support groups would include the application support team, empanelled consultants, and software vendors to help the service providers build the necessary processes and applications. The support documents for guidance on leveraging and integrating eID into the service provider solutions would include applications onboarding and readiness, the authentication framework, operating model and guidelines, criteria, checklists and activity templates for becoming an Identity Service Consumer Agency (ISCA) or an Identity Service Provider Agency (ISPA), and eID seeding to embed the NIN.

5. **Terminal Devices.** Terminal devices would be employed by ISCAs (both public and private) to provide services to residents. Examples include micro-ATM devices, PoS devices and terminals, ATMs and Access Security devices. These devices would host the applications of the ISCA and support the mechanism to capture biometrics of residents for eID authentication purposes. Any additional features of these terminal devices would depend on specific needs of services offered by the ISCAs. These devices would comply with specifications issued by the government to protect all the demographic and biometric information provided by the residents.

6. **Electronic Know-Your-Customer Process.** The eKYC process verifies the identity of a customer. The service providers would perform the process electronically with explicit authorization of the resident. This would allow instant and paperless service delivery to residents. The government could implement the eKYC process by using the same infrastructure and operating model set up for eID authentication.
    a. In the eKYC process, residents would authorize the government through eID authentication using either biometrics or One-Time Password (OTP) to provide to service providers their demographic data, along with their photograph, digitally

signed and encrypted. This would help the service providers to perform a paperless and realtime KYC process.

b. The eKYC process would enable service providers to make instant delivery to residents that, otherwise, may take a number of days for activation pending verification of related documents.
c. The use of the eKYC process would avoid the cost of repeated KYC processing, the cost of paper handling and storage, and the risk of forged proof of identity and proof of address documents.

7. **Electronic Payment Service.** The government could implement the eID-based electronic payment mechanism (ePayment) to promote transparency, accountability, efficiency and correct targeting in the payment of government program benefits such as social security pension, health benefits, etc., to the intended benefits.
    a. The ePayment would also facilitate seamless transfers of all welfare scheme payments to a beneficiary's eID-enabled Bank Account (eBA). The eBA can be viewed as a regular bank account which is identifiable through the beneficiary's electronic ID.
    b. At the time of enrollment for eID, residents would provide their existing bank account details or request for the opening of a new bank account that would be attached to their NIN for all welfare scheme payments.
    c. The ePB would have a database housing a repository of residents' NIN and their corresponding eBA. This database would be used for social security and entitlement payments from various government agencies.
    d. The solution to financial inclusion would contain the combination of the NIN as a payment address and the eKYC function for instant account creation using the eID-enabled payments infrastructure. The pilot phase should address key issues with regards to the account creation process and procedures, and \assess the implications of using the NIN as an account identifier for the national payment system.
    e. Using the NIN as the payment address, the money is sent to any resident, irrespective of whether they have a bank account or not. If the receiver has an eBA, the money would be transferred into it. If the receiver does not have an eBA, an instant account would be created, on the basis of the NIN, with a debit freeze. Money transferred would be credited to the instant account. The instant account would be activated during the first withdrawal on the basis of the eKYC function.

8. **Official Email Address of Residents.** The government could provide an official email address to each resident. The email address would be used for official government communications, but it could also be used for private communications. The government-provided email address would act as a relay, and residents could specify an email account at the time of enrollment where messages may be delivered. All email addresses could be publicly listed on the government's national registry of certification service providers.

9. **Secure Electronic Document Service.** The government could provide secure eDocument service to enable safe transport of electronic files in an unsafe environment, i.e., the Internet. The service would offer the functionality to encrypt and decrypt eDocuments using the biometrics or digital certificate mapped to the eID profile of the resident. For further details, refer to the Estonia experience in Annex 5.

10. **Mobile ID Services.** The government could provide mobile ID service to registered eID-holders which would be used for eAuthentication and digital signing with a mobile phone. In this scenario, the mobile phone with SIM (refers to cards, software or other subscriber identification mechanisms) functions simultaneously as the identity card and the card reader.
    a. When using mobile ID service, the resident would get a specialized SIM that enables the service. This would be obtained by signing a service contract with a designated national mobile operator.
    b. The mobile ID may be used anywhere in the world where there is mobile coverage. There would be no need to install the software on the computer for it to work. The software would be installed on the SIM of the mobile phone. It may be used on the latest mobile phones. As smart phone technology becomes more widespread, having the mobile ID option would become increasingly handy, allowing the user to vote, for instance, via a phone's web browser.

Technical Aspect. Some of the technical learnings in the implementation of eID-based service delivery derived from the study of international experiences detailed in Annex 5 are listed below.

1. **Defining Unique and Secure National Electronic Identity.**
    a. **Uniqueness as Crucial Attribute.** The national eID profile of the resident would include the unique NIN linked to the demographic and biometric data stored in the Central Resident eID Data Store (CRIDS).

b. **Use of Intelligence is Unwise.** Loading intelligence into identity numbers would make them susceptible to fraud and theft. Therefore, the NIN would be a unique random number assigned to the resident and may not contain any intelligence.

c. **Data Collection through Nationwide Enrollment.** The first step in the issuance of a national eID would be the enrollment process where a resident's demographic and biometric information may be collected. The uniqueness of the data provided would be established through a process called deduplication. After deduplication, the NIN would be issued and a letter would be sent to the resident with the information details.

d. **Biometric Deduplication for Uniqueness.** Ensuring uniqueness means assigning one NIN to each person, and one person has only one unique identity number. A resident profile would undergo the rigorous demographic and biometric deduplication process with 99.99 percent accuracy before being assigned a unique identity number. Demographic data alone cannot guarantee uniqueness. However, unique identity may be possible by linking demographic attributes with biometric attributes like fingerprints and iris images from the individual.

2. **Leveraging CRIDS in Electronic Identity Authentication.**

a. The eID authentication process would be exposed as stateless web service over hyper-text transmission protocol secure (HTTPS). The usage of open data format in extensible markup language (XML) and widely used protocol such as hyper-text transmission protocol (HTTP) would allow easy adoption and deployment of eID services.

b. The eID authentication process would work by taking the NIN along with eID-holder's personal identity data as the input and, in turn, sending that input to the CRIDS for matching, following which the CRIDS verifies the correctness on the basis of a 1:1 match with the eID-holder's identity information. The service either confirms the proof of identity, or verifies the information provided by the resident. To protect the resident's privacy, the service responds only with a "yes/no"; no personal identity information is given as part of the response.

c. The eID authentication process would be made available to the residents to prove their identity online anywhere, anytime and in multiple modes. It would support single-factor and multi-factor authentication. The NIN — along with attributes which could be demographic, OTP, digital certificate, or single/multiple biometrics (fingerprints and/or iris images) — may be used to provide single-factor authentication. As an alternative, these attributes would be used in combination

(multi-factor) to achieve the required authentication needs. The NIN, on its own, may not be used a factor for authentication.

d. The eID authentication process would support multiple types of authentication depending on the input type (demographic, OTP, digital certificate, biometric, or multi-factor). All types of eID authentication requests would take the NIN as one of the input in order to reduce the authentication to a 1:1 match in the CRIDS.

e. The eID authentication process would support the federated authentication model and would be designed with a view to strengthening the service providers' existing authentication systems, rather than replacing the existing one. While the federated model would not mandate the existence – or use – of the service providers' own authentication (if a service provider so wishes, the eID authentication may be used by itself), they would be encouraged to use the eID authentication in conjunction with their own local authentication to render the overall system stronger and more reliable. This could be called the federated model of eID authentication.

f. The eID authentication process would contain security and privacy features such as "yes/no" response, digitally signed request/response, response code, response timestamp and self-verifiability of response, encryption and tamper-proofing. For further details on the security and privacy features of the eID authentication process, refer to the India experience in Annex 5.

g. The eID authentication process would support buffering of data at multiple end-points to enable service delivery in case of intermittent non-availability of network connectivity.

3. **Biometric Data Standards and Devices**

a. **Biometric Device Specifications.** The terminal device used in the biometric-based authentication process would have the capability to capture the fingerprints and iris images of residents. The government could define the biometric device specifications[1] based on open standards so that the related information captured with the device would ensure high-quality data and result in greater accuracy.

b. **Biometric Data Standards.** To meet the huge demand for biometric capture devices needed in eID authentication, it may be necessary to source the devices from multiple vendors specializing in biometric authentication. However, this would be

[1] Biometric Devices Specifications for Aadhaar Authentication – http://stqc.gov.in/sites/upload_files/stqc/files/New%20Revision%20_May_%201%20STQC%20UIDAI%20BDCS-03-08%20UIDAI%20Biometric%20Device%20Specifications%20_Authentication_.pdf

possible only if there is interoperability among the devices produced and sold by various vendors for data capture and matching. The designated government body could define the biometric data standards based on the open standards for fingerprint images, fingerprint minutiae, iris images and facial photos to achieve interoperability. The ISO 19794 series of biometric standards for fingerprint, facial and iris recognition set by the International Standards Organization (ISO) are the most widely accepted, and best embody previous experiences of the US and Europe with biometrics.

c. **Biometric Specifications.** The biometric Software Development Kit (SDK) Application Programming Interface (API) specifications would provide a single unified interface across multiple modalities (face, fingerprint, and iris) for SDK developers of biometric device vendors to expose their functionality to various modules of the Electronic Identity Services Delivery Platform (EISDP). This would enable vendor neutrality as the use of standard APIs and open standards would eliminate proprietary and vendor-specific features. It would also promote interoperability by using standard interfaces, common data format definitions and protocols across the components that expose similar functionality. The open API would also allow best-of-breed algorithms to be used for special purposes. The API exposes quality check, segmentation, sequencing, extraction and matching functionalities. The specifications would be published on the government public portal.

d. **"Best Finger Detection" Technology.** The EISDP would expose the "best finger detection" as a stateless web service. This would be called by the service providers' application to detect a resident's finger providing the most accurate among successful matching results. The resident would then use the best finger to ensure a better success rate in biometric eID authentication. The chances of getting a match may vary due to differences in quality across all fingers. This variation may also be present due to the manner in which the resident normally interacts with a typical fingerprint scanner, and different fingers may inherently have varying amounts of identifying information depending on the size of the finger and the commonness of the pattern it carries. Hence, the detection of the best finger for biometric eID authentication would improve the accuracy of the results.

4. **Reliable and Trustworthy Electronic Identity IT Infrastructure with in-House Technical Support and in-Country Proven Technology.** The government could build a reliable and trustworthy eID infrastructure assisted by fulltime technical support. The technical

solution would be based on already proven technology provided by local software or technology vendors. The solution would be scalable, flexible, and standards-based for expansion to other services, as well as forward-looking to enable cross-border use.

5. **Domestic in-House Technical Capacity in Electronic Identity IT Infrastructure and Services.** The government could develop in-country technical capacity that would be self-sufficient in designing and implementing the eID IT infrastructure and services. This is preferable to relying on foreign software or technology vendors to provide and guarantee support for a critical piece of national infrastructure. A reliance on non-local vendors would have a detrimental impact on the country's day-to-day functioning going forward. Because of these considerations, a bespoke software model could be developed. In case the government decides to use the shrink-wrapped solution from external vendors, then it could build in-house capabilities to implement and manage the solution.

6. **Designing Electronic Identity for Easier Integration into Services of Providers.** The government could design the implementation of the eID services in such a way that it enables integration with the existing and planned primary service delivery systems of providers. This will allow functionalities such as eSignature, electronic authentication and document encryption. The government could implement the following measures to meet the integration requirements.
    a. **Employment of Standardized Workflows in the Service Delivery Process.** As an example, standard workflow for eSignature using a common document format would be employed. For further details, refer to the Estonia eSignature implementation described in Annex 5.
    b. **Centrally Issued Unique National Identification Number.** A centrally hosted database of the NIN issued to residents would be implemented. There would be a reliable and trustworthy eID infrastructure to enable the delivery of identity services. For further details on the centralized eID database and IT infrastructure, refer to the India experience described in Annex 5.
    c. **Central Single Point of Access to Public Services.** The eID authentication would be used as a secure token for the various services where access would be provided by a central single point of entry: the eCitizen portal.

7. **Designing Mobile ID Services to Promote Adoption of Electronic Identity Services.** In Estonia, the adoption of eID improved with the implementation of mobile ID services since the penetration of mobile phones in the country was more than 100 percent. The

improvement was brought about by the ease of use of the mobile phone as an authentication device, as compared to a smart card reader attached to the PC. For further details on the mobile ID implementation experience in Estonia, refer to Annex 5. Some of the technical design lessons learned from Estonia's implementation of mobile ID services are mentioned below.

a. Mobile authentication and mobile signing methods would accept the NIN, and personal identification number (PIN) and phone number as input parameters. Using a mobile number as the only input parameter may result in security issues since it is public information. Therefore, including a PIN and the NIN would improve security.
b. The technical design of the mobile ID would be based on the implementation of the Wireless Public Key Infrastructure (wPKI), e.g., a wPKI specification[2] in which the mobile phone operates as a smart card reader with display. The communication between the personal computer (PC) and the mobile phone would be through the mobile signing/authentication function and gateway of the Global System for Mobile Communications (GSM) operator.
c. The mobile gateway would use a standard technology such as Over-The-Air[3] (OTA) to communicate and run the applications on the SIM of the mobile phone without being physically connected to the card.
d. The signing/authentication function would send the signing/authentication request (wPKI request[4]) to the back-end system of the MNO using the Internet Protocol (IP) network which, in turn, sends the request to the mobile gateway. The gateway would forward the request to the resident's mobile phone by Short Message Service (SMS).
e. The mobile phone would support the necessary technical features in order to use it for mobile ID functions. For instance, Estonia has published the technical specifications for the mobile phone to enable mobile ID services. The

[2] wPKI Specification - http://www.signature.lt/KK/wPKI-specification.pdf

[3] Over-The-Air Technology - http://www.gemalto.com/techno/ota/

[4] wPKI Mobile Transactions - http://wpki.eu/doku/lib/exe/fetch.php/wiki:baltic_wpki_standard_draft-0.3.pdf

specifications include support for the GSM Phase 2+ standard[5], the SIM application toolkit[6] with OTA updates, and compliance with GSM standards[7].

8. **ESignature and Digital Certificate Authentication.**
    a. The eSignature architecture would be based on the universal open standards for giving, processing and verifying eSignatures. It may be able to connect to any new or existing piece of software. The components of the system would include a stand-alone client program, a web portal and a web service based on Simple Object Access Protocol (SOAP) enabling easy integration of the functionality of digital signing, signature verification and authentication with other information systems.
    b. Like Estonia, the government could choose a communication model using standardized workflows and common document format such as the XML Advanced Electronic Signatures Standard (XAdES). The XAdES defines a format that structurally enables storage of signed data, signature and security attributes associated with the eSignature; therefore, it would accommodate a common understanding among systems.
    c. The Gov could define digital certificates and smart card standards based on open standards to promote interoperability. For further details on the international experiences of leveraging open and widely used standards for digital certificates and smart cards, refer to Annex 5.
    d. The government could provide software that may be installed on residents' Internet-connected device (laptop, desktop, etc.) to enable them to use their ID card electronically to access public and private eServices, digitally sign documents and encrypt documents for safe transfer. The software would be collectively referred to as ID-software. The government could provide residents the instructions on its public website for installing ID-software on the device. For further details on the ID-software, refer to the Estonia experience in Annex 5.
    e. Some of the commonly provided software as part of the framework could include:

---

[5] GSM 11.11 Digital Cellular Telecommunications system (Phase 2+); Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface - http://www.etsi.org/deliver/etsi_gts/11/1111/05.03.00_60/gsmts_1111v050300p.pdf

[6] SIM Application Toolkit - http://www.gemalto.com/techno/stk/

[7] GSM 11.14 Digital Cellular Telecommunications system (Phase 2+); Specification of the SIM Application Toolkit for Subscriber Identity Module - Mobile Equipment (SIM-ME) interface - http://www.etsi.org/deliver/etsi_g3ts/11/1114/05.04.00_60/gsmts_1114v050400p.pdf

i. Software libraries for developers who may be interested in integrating the digital certificate authentication and signing capabilities in their software.
ii. Service such as the online certificate status protocol (OCSP) server for realtime and long-term validity of certificate. For further details, refer to the Estonia experience in Annex 5.

9. **One-stop Common eGovernment Services Portal.** The government could design a common eGovernment services portal for delivering all eServices from its various ministries and departments with Single Sign-On (SSO) capabilities using eID authentication.

Institutional Aspect. Some of the institutional learnings, including the organizational structure and operating models, taken from the study of international experiences as detailed in Annex 5 are listed below.

Organizational Structure

1. **Separate Government Organization as the Overall Regulator and Overseer of eID Services.** For any service agency, establishing both the identity and the service entitlement of the beneficiary is necessary. Though the individual identity would be unique and independent of the type of service being sought, entitlement is quite specific to the service being availed and it has to be established by each service agency separately. Hence, as in the three countries studied (India, Estonia and Belgium), instead of assigning the roles and responsibilities of eID services to an existing ministry, a new government organization could be created as the overall regulator and overseer of the eID services. For further details, refer to Annex 5.

2. **Cross-ministerial Apex Committee as Decision Makers for eID Services and Related Issues.** An apex committee at the highest level of government, headed by the president/prime minister, could be constituted. Members could be ministers from key ministries such as finance, law, information and communication, labor and employment, etc., who will have the function of managing all issues relating to the eID system, including its organization, plans, policies, programs, schemes, funding and methodology to be adopted for achieving its objectives. However the apex body should have sufficient technical capacity and operational control for it to be feasible. The apex committee should also participate with the software development user groups as well as the international development agencies to maintain openness of standards while installing best practices around privacy and protection of the residents' data.

3. **Scalable PPP-based Organizational Structure to Deliver Highly Secure and Quality eID Services.** The need for scalability requirements to meet the exponential growth in the demand for eID services could be met by designing a scalable organizational structure based on the PPP model. In this model, the government could define roles in the ecosystem that would be outsourced to the private sector. The organization for delivering the service would be small to begin with, but may be scaled out as the demand for the service increases.
    a. The need for high security in the management of Personal Identity Data (PID) in the CRIDS may be achieved by limiting access to the data center to only a few authorized organizations that play the role of ISPA.
    b. The mobile ID would be implemented using PPP between the government agency responsible for eID and the MNOs. The government agency could delegate the responsibility of supplying mobile ID SIMs to the MNOs. The user registration and mobile ID activation would be performed by the Registration Authority (RA) which would take the request for user registration and service activation from the resident. The role of the RA would be performed by the MNOs working alongside the public security department of the government. The request for the generation of a new certificate would be delegated to the Certification Authority (CA) of the Certificate Service Provider (CSP).
    c. Biometrics or digital certificate-based eID services such as eID authentication would be set on a PPP organizational structure in order to ensure that the services are scalable and meet the service-level agreement (SLA) as defined by the government. The government could delegate the role of certification center to the government agency defined in the ESignature Act (ESA), which would in turn hire the private service providers to implement and deliver the service on its behalf. The certification center would be responsible for managing the operations of services such as lightweight directory access protocol (LDAP), OCSP, and other certificate-related processes, end-user distribution channel through its parent retail outlets, development and maintenance of the ID-software and installation packages, instruction manuals and video instructions published on the government public portal, and call centers.
    d. In order to delivery smart card-based biometrics/digital certificate-enabled eID services, the government could outsource the functionality of card personalization to the empanelled and certified private sector vendors. The vendor would be responsible for both the physical and electronic personalization of the card. The

vendor would receive the card application from the government agency to manufacture, print and engrave the personal data on the card, generating the keys on the chip and embedding the certificates on the card.

e. The ESA would define the roles and responsibilities involved in the processing of eSignatures. Some of the roles could be assigned to CSPs that would certify residents identifiable by name and PIN. The CSPs would be legal entities fulfilling specific legal requirements, while timestamping service providers (TSPs) would provide the timestamp that is simply a data unit that proves that certain data existed at a certain moment.

4. **Biometric Data Standards Committee.** The government could form a national-level committee to define the biometric data standards applicable to the biometric capture, extractor and matcher devices, algorithms and software. They would be based on the existing national and international standards that are widely used in the industry. The committee would have members from the government, academia and industry experts; the standards would be established in consultation with the other government departments and service providers in the private sectors.

5. **eID Services, IT Infrastructure and Services Owned and Managed by IT Ministry.** The government could have a ministry/department responsible for IT-related policies and for delivering IT services to the government departments implementing eGovernance. This department would be responsible for providing technical support and nationwide-shared IT infrastructure and services that can be used by the government agency responsible for eID service delivery.

6. **Privacy Commission.** A privacy commission could be created reporting directly to the highest authority (the Parliament or the President's office) to ensure that all privacy rules pertaining to identity data and their usage are respected at all times.

Operating Model

1. **Fresh Enrollment of Residents for eID Services for High Quality eID Data.** The quality of the personal data in the databases of service providers is lacking and fraught with problems of fraud and duplicate/ghost beneficiaries. To prevent this from seeping into the eID database, the personal data – both demographic and biometric – would be collected and verified using the enrollment process. This would ensure that the data collected is clean from the start of the program.

2. **Introducer System in Inclusive eID Services.** The EISDF system would be inclusive and be made available to all residents, including those who do not have any form of identification document. There could be an "introducer system" for residents who do not have any form of identification, and eID would be their first form of identification. The introducer is a person who stands as the guarantor for the residents' personal demographic data to be fed into the eID system. It is noted that such system could be fraught with issues, and will need to be tight monitoring by civil society and have a clear grievance feedback loop local stakeholders.

3. **Secure and PPP-based Scalable eID Service Delivery Operating Model.** The operating model for delivering eID services using the EISDP would be scalable and based on the PPP model.
    a. The operating model would ensure the security of the CRIDS by having only a limited number of registered ISPAs to have direct connectivity to the eID services via the web.
    b. Any agency that would like to avail of eID services offered by the EISDP would need to sign up as an ISCA and enter into an agreement with the owner-government agency. To do so, the ISCA would need to go through an ISPA.
    c. The ISPA could establish secure connectivity to the eID services on the EISDP to transmit requests on behalf of ISCAs, and then receive response back from services.
    d. The ISPAs could build and maintain their secure connectivity to the EISDP in compliance with the standards and specifications set by the owner-government agency.
    e. There could be a registration process for engaging the players (ISPA, ISCA, etc.) that will be delivering eID services to the government and private organizations. The process would be simple, but at the same time it would include the necessary checks and balances to ensure that the agencies selected are capable of delivering the services. There would be a clearly defined step-by-step process for applying as an ISPA or ISCA, and it could include the list of supporting documents required of each of them as published on the public portal.

4. **Technical Awareness and Adoption.** There could be a public-facing portal for building technical awareness and for providing technical support to the user-agencies in both public and private sectors. It would publish technical documentations such as standards

and API specifications on the portal used by software professionals who are interested in incorporating eID services into their applications.

5. **Biometric Device or UID Certification for eID-enabled Applications.** There could be a certification process for biometric devices to ensure their compliance with specifications defined by the owner-government agency. The responsibility of implementing the certification process would be delegated to the department in the Ministry of Information Communications (MIC) that is responsible for delivering quality assurance services in the area of electronics and IT in the country's network of laboratories and centers. It could maintain a list of certified vendors' biometric devices. The vendors who may wish to have their biometric device certified will have to follow the certification process defined by the department. The process would be published on the public portal by the owner-government agency. Alternatively the devices could use India's UID certification standards, as it could reduce cost, and improve overall security and efficiency.

6. **PPP-based Scalable and Secure Mobile-ID Service Operating Model.**
    a. **Secure Login.** As in Estonia, a typical scenario for mobile ID-enabled eID authentication used for logging into a secure site, e.g., a bank account of the resident, could be:
        i. The resident clicks the "Log in with mobile ID" option on a supported website.
        ii. The resident is prompted to enter his/her mobile number and PIN.
        iii. The website displays a unique verification code.
        iv. The phone beeps and displays a screen indicating that a connection is being made.
        v. The phone screen displays the eID authentication service name and verification code.
        vi. If the service name is correct and the verification code corresponds to the displayed number on the page in the computer, then it is safe to press "Accept".
        vii. The user is prompted to enter a mobile ID PIN on the phone.
        viii. The screen on the phone disappears and the website is automatically reloaded with a logged in screen.
    b. **Mobile ID Provisioning.** The national mobile operators in the country could issue the mobile ID through their local stores. The resident could go to the nearest mobile operator to get a mobile ID SIM. The service provider would forward the

application to the MNO and inform the resident where to pick the new SIM. The resident would be required to have his/her identity card with valid certificates for getting the mobile ID and would have to sign a contract (mobile ID subscription agreement) to complete the transaction. The government could delegate the responsibility of issuing the mobile ID to the national mobile operators. The MNO identifies the user using the identity card and on successful authentication, hands over the new SIM to the resident. As part of the provisioning, the SIM would be attached to a unique secure signature creation device (SSCD) for the resident, and the SSCD can later be used for issuing a qualified certificate. The SSCD certificate would be declared active for a particular SIM and made available to all the TSPs. The MNO would provide a unique code to the resident for activation of the qualified certificate.

c. **User Registration/Certificate Activation.** The resident would activate the service on the handset with the new specialized SIM. To activate the mobile ID service or to apply for certificates, the resident would have to go to the website of the public security department, the RA. The resident would have to fill an online application form and enter the ID card into the card reader and follow the instructions. The purpose of the certificate activation process would be to create and activate a qualified certificate. The resident would issue a request to activate the qualified certificate using the mobile phone with the new SIM. The RA would initiate signing by responding to the resident's mobile device to sign the personal data. The resident would verify the data, and then sign it by inputting the device certificate activation code. The RA would now receive the personal data signed. The RA would attach additional data, including the device certificate, before forwarding the request for certification activation to a CA. The CA would create and activate a qualified certificate and publish it.

d. **Usage.** A service provider would request service, such as eID authentication, from a TSP and would use a GSM subscriber number and/or personal identification code to identify the resident. The TSP would generate the signature request and send it to the resident's mobile phone. The resident would sign the request by entering assigned PIN. The TSP would now receive the signature data. The TSP would check the validity of the signature data, as well as the validity of the certificate. The service provider would then receive the eID-related services from the TSP.

e. **Termination.** It may be possible for the resident to stop using the mobile ID for several reasons, among them: the resident may not be using the service, lost/compromised the SSCD, the qualified certificate expired, or the resident may

have violated the user-CA agreement. In case of certificate revocation, the RA would inform the CA about it and the CA would immediately revoke the certificate. At this point, the Certificate Revocation List (CRL) may be updated. In case of SIM blocking due to loss or SIM damage, the device certificate would be taken out of the list of valid SSCD available to all TSPs.

f. **Mobile ID Fees.** The mobile operator may charge the resident fees for the mobile ID service. The charge would include a one-time subscription fee, as well monthly fees. If the mobile ID would used outside the country, each mobile ID transaction would be charged at the cost of sending one text message based on the package price list.

7. **Readily Available ID-software and Devices to Drive Adoption.** In order to drive the adoption of eSignatures within the region, the compatible software and technology would be made available quickly to the parties looking to incorporate eSignatures into their applications.

8. **Round-the-clock Call Center and Online Services to Prevent eID Fraud.** To prevent eID fraud, the government could set up a call center operating 24/7 year-round and provide DocStop and CheckDoc services. DocStop would help avoid the risk of fraudulent use of eID documents, as well the financial consequences. DocStop would enable the resident to block the identity card and eID profile immediately in case related information is lost, stolen or compromised. The resident would have to call the toll-free DocStop number to report the incident. The service is available 24/7 year-round. The CheckDoc would enable the resident to verify in realtime the validity of the eID documents; it would also identify the stolen, lost, expired, invalid or never-used eID documents. To use the service, the resident or the user-organization would have to register by filling in a registration form. The website may be accessed by using the username and password provided on successful registration.

Policies

1. **Know Your Customer.** Service providers in both the public and private sectors such as those in banking, insurance, capital markets, telecom, LPG, railways, etc., may update their KYC norms to include eID as the valid KYC.

2. **Biometric Data Standard Policy.** The government could define a policy at the country level to standardize the use of biometric data for purposes of identification and authentication of residents.

3. **ESignature Act.** The government could pass a EESA to ensure that the eSignature of the resident issued by the designated government agency is valid certificate and has legal binding, making it equal to paper-based handwritten signature. The handwritten and eSignatures would be made equivalent in both the public and private sector by this Act. The EESA would also state that public service departments must accept digitally signed documents. The EESA would ensure that each eSignature uniquely identifies the signatory, binds the individual to the signed data, and guarantees that the signed data cannot be tampered with retrospectively without invalidating the signature itself.

4. **Rules and Regulations for Certificate Service Providers.** One of the core components of the ESA could be the establishment of rules and regulations with regard to CSPs that would issue digital certificates to users and manage related security services. The ESA would mandate stringent financial and procedural requirements to ensure that CSPs are set up and managed properly to perform their function to the highest possible standard.

5. **Rules and Regulations for Timestamp Service Providers.** The ESA would also regulate timestamping by the TSPs. These service providers would adhere to similar laws and regulations as those applied to CSPs. The timestamp is simply a piece of data that attests to the occurrence of an event at a specific time. The ESA would ensure that the timestamped data are not tampered with or amended without invalidating the timestamp itself.

6. **Personal Data Protection Act.** The PDPA regulates the use of personal data and databases by public authorities and private entities. The Act would mandate a data protection inspection department within the government to oversee that the requirements of the Act are being met; it would also enforce compliance, if necessary. The strategy for the protection of the identity card would be to keep to a minimum the private data on the card. Instead, the data would be kept in highly secure databases at authorized centers. A person would use the card as the key (authorization method) to accessing his/her personal information in the database. Requests by third parties (e.g., representatives of authorities) for private data would be logged, and logs would be made available online to the individual upon request (via the citizen's portal).

7. **Identity Documents Act.** The government could pass, or update if existing, an Identity Documents Act (IDA) affecting related documents to establish national guidelines for the creation of the NIN, and the issuance of an identity card and an eID for the residents of the country.
    a. The IDA would grant equal value to the eID as compared to the current paper-based identity documents for all legal purposes.
    b. The IDA would decide the purpose of the card and the NIN in terms of proof of citizenship. In India, the unique ID number (UID) is used as the proof of identity only, and does not confer citizenship. For further details, refer to the India experience in Annex 5.
    c. The IDA would state that the deduplicated and processed residents demographic and biometric data used for the personalization of the card would also be entered into the national population register pursuant to the Population Register Act.

4.0 Current Identity Usage and Service Delivery Issues Faced in Vietnam

An understanding of the current identity systems and identity-related service delivery issues faced by the residents and service providers in the public and private sectors in Vietnam are described below. This understanding was developed based on discussions with various stakeholders in Vietnam and secondary online desktop research.

4.1 Understanding of Current Identity Systems in Vietnam

People's Identity Card: Common Proof of Identity Document in Vietnam

Figure 4.1: People's Identity Card

The Ministry of Public Security (MPS) issues the People's Identity Card (ID card) and an identity number to all the residents of Vietnam. Service providers use it as the Proof of Identity (PoI) document to establish the identity of a resident. The ID card is a paper-based card issued to all residents above the age of 14 by the MPS department at the provincial level. The card bears the

resident's name, address, age, height, weight, date of issue, and one fingerprint; it is valid for ten years. Roughly 98 percent of the Vietnam population owns this card.

Current Identity Creation and Authentication Process during Service Delivery in Vietnam

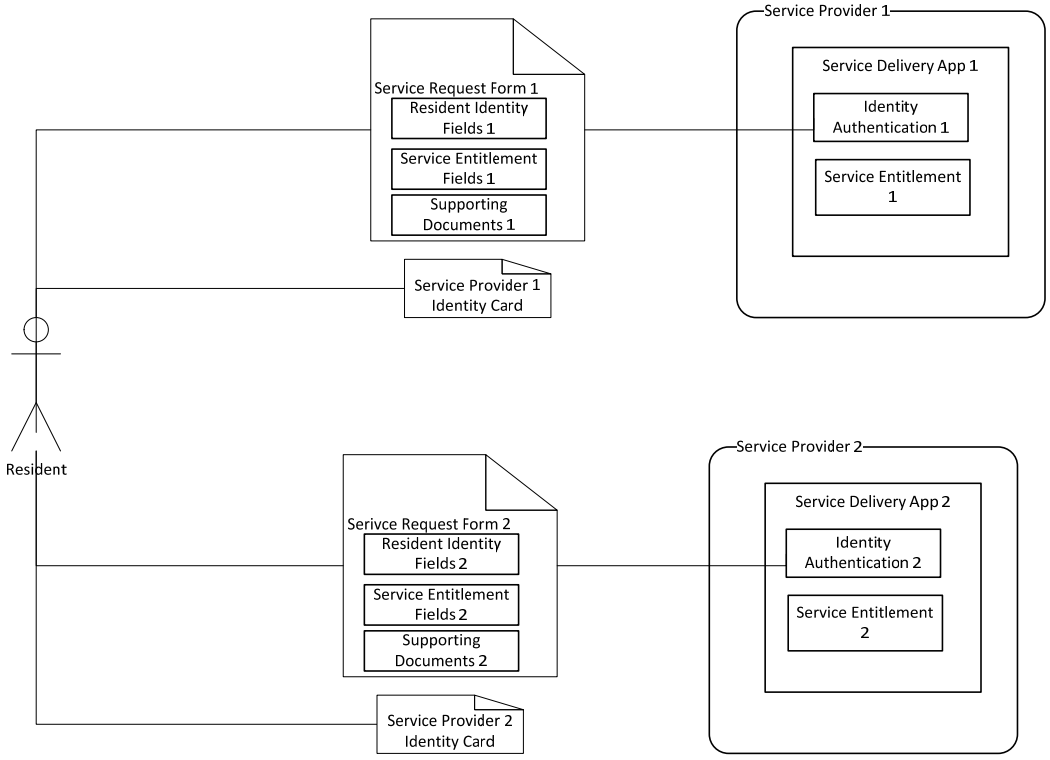


Figure 4.2: Current Identity Authentication Process for Service Delivery

In Vietnam, as in other countries, both public and private service agencies across the country typically require PoI before providing services to individual residents. For any agency, establishing both identity and entitlement of the beneficiary is necessary before offering any service to a resident, be it opening a bank account, withdrawing or depositing money, getting a tax code, receiving pension, or for travel. Individual identity may be unique and independent of services availed, but entitlement is very specific to the service desired; therefore, they have to be established separately. For instance, the issuance of a health insurance card involves individual identity (name, address) verification and health insurance entitlement identification.

Identity establishment typically involves two steps: identity creation and identity authentication. Identity creation is the mechanism of defining an individual's identity by providing identity token(s) to the person in some form (physical and/or electronic). This is typically a one-time activity. Identity authentication is a process of verifying "who an individual claims to be" by

checking the identity tokens assigned to the individual. This can be manual, electronic or a combination of both.

The service providers in both the public and private sectors typically follow their own process of identity creation, in addition to the service entitlement identification. To illustrate, the Vietnam Social Security (VSS) maintains a separate database of beneficiaries and their service entitlement identification for each of the welfare programs such as social and health insurance. A separate identity token for each of the programs are provided to the resident for identity authentication and entitlement verification.

Each service provider in Vietnam uses the ID card and other valid PoI documents such as a passport for identity establishment to generate a new service provider-specific identity card. The same identity card is used to establish service entitlement. The resident presents the service provider-specific identity card for authentication and entitlement at the time of the service delivery.

VSS. The VSS is in the process of centralizing its beneficiary databases from different programs, namely the social and health insurance which are available at present at the local level. Currently, the identification of the unique citizen across the program databases is a challenge as the IT systems and the databases are distributed with no common data standards for storing the citizens' basic information. Moreover, each database stores a separate identity system for the identification of the beneficiaries. The identification number on social and health insurance books are not consistent. There is a need for a unique identification number to be assigned to the citizens that they can use throughout their life. The VSS is waiting for the GoV to issue the national identity number (NIN) to citizens so that it may be better able to manage the social and health insurance programs.

Ministry of Labor, Invalids and Social Affairs. The Bureau of Employment under the Ministry of Labor, Invalids and Social Affairs (MoLISA) currently has to maintain two separate and disjointed databases for the supply and demand sides of the labor market due to different data fields used in the identification of the beneficiaries in the databases. The data for the demand side of the database is collected primarily from government agencies, government-owned enterprises and private businesses. The data fields used for the identification of the citizens in this database is based on the ID card or passport. The supply side of the databases uses the household book for the identification of the beneficiaries. The beneficiary is given a unique code using the geographical location codes from the government of the permanent address of the beneficiary, namely region code, province code, district code, commune code, household number and family member number. The ministry is currently executing a pilot in two districts for capturing the

supply side of the database using the ID card as the primary identification document so that it can be connected to the demand side of the databases. The ministry also has to update the databases annually to maintain the accuracy of the information – a time-consuming and resource-intensive process. The ministry would be able to avoid the necessary annual update and consolidate the databases automatically with the availability of a unique identification system for citizens. This system could also be used by the private sector and other government agencies for identification of their employees and the citizens in general. The ministry captures the data of beneficiaries from age ten and up in the labor market database. The ministry wishes to recommend that the government lower the minimum age for requiring the national identity number to ten years old. Currently, the proposal is to commence the identity card issuance at 14 years of age.

Ministry of Education and Training. The Ministry of Education and Training (MoET) is designing a centralized Education Management Information System (EMIS) for all schools in Vietnam to streamline the management of its operations. The ministry provides free Internet connection to all schools in the country and is in the process of developing the electronic databases of students and teachers across the country. The electronic database of the 20 million students in the country could be ready in three years. The MoET expressed the need for a unique identification of citizens which would help to accurately identify students and teachers across the schools. Currently, the ministry experiences difficulty in identifying students who moved from one school to another over the years. There are similar challenges with the identification of teachers and their training requirements.

Ministry of Health. The Ministry of Health (MoH) is working on a number of government programs which provides citizens benefits such as health insurance, free HIV medicines, etc., based on their identification. They have been unsuccessful for the last ten years in trying to build a unique patient identity system in which each patient would have one identification number for use in different hospitals and in the delivery of other health care services. This unique patient identity could be used by the patient throughout his/her life for identification purposes and for maintaining an Electronic Health Record (EHR). The ministry is keen to leverage the national identification system and the unique identity number in its system for the verification of patients. The MoH expressed their concern over the lack of awareness of the benefits of the National Identity (NID) and Electronic Identity (eID) systems among the citizens. Hence, there is a need for awareness programs on the benefits of the NID to citizens, and on the use the computer and other devices in the effective delivery of health care.

State Bank of Vietnam. Officials of the State Bank of Vietnam (SBV) expressed their concern over the problem of not being able to verify the identity of a person uniquely in the issuance

eSignatures. On the other hand, they have already issued eSignatures to 7,000 employees of SBV and other commercial banks. Primarily, the eSignatures are used for Internet bank payments, and signing financial results and government reports. Different PoI documents are used for the verification of the identity of a citizen, namely ID card, passport, driver's license, etc. Having a single NID with a unique number could solve the current issues of identity theft and duplication.

Vietnam Post and Telecommunications Group and Viettel Group. The two largest telecommunication providers in Vietnam, the Vietnam Post and Telecommunications Group (VNPT) and the Viettel Group, each have a customer base of about 50 million customers. Both groups have expressed the need for a unique identification system for the verification of the identity of the citizens at the time of registration of new customers. Currently, they provide various online value-added services on the computer and mobile phones such as eBanking, mBanking, utility bill payments, etc. They are also planning to have a new SIM with eSignatures for the electronic filing of tax returns, ePayment and mobile banking. They agreed that the mobile-based ID is feasible from the technical capability perspective; however, there is a need for legal measures for the enforcement of the issuance and the usage of the new eID.

Vietcom Bank. Like the other institutions that have been mentioned in this chapter, the Vietcom Bank also faces the challenges of verifying the identity of citizens at the time of registration of a new customer in their system. This is due to having to use more than one PoI for verification. It has had cases where the individual has opened two different bank accounts with two different identities using two different PoI. For this reason, it has also been unable to get an accurate credit history of citizens from the Credit Information Center (CIC). The bank's officials have expressed the need for the NID which would enable them to uniquely identify the citizens at the time of registration. They could also expect the government to provide the necessary guidelines and technical support in the integration of their systems into the new eID system, and to ensure that both the old ID card and new eID are valid during the transition period.

4.2 Key Identity Issues Faced during Service Delivery in Vietnam

The current approach to identity creation and identity authentication mechanism has resulted in the following issues.

Lack of a Unique Resident Identification

The ID card currently in use is issued to the resident at the local province level with a locally generated identification number scheme, and there are issues with resident identification number synchronization between the national and provincial levels. Hence, the same identity number

could be issued to more than one resident across provinces and it could be difficult to uniquely identify a resident by using the ID card alone. It is noted that the GoV recognizes the following issues and is proactively conducting pilots and seeking legislative changes to address them.

High Cost, Inconsistent and Duplicate Service Provider-specific Identity Creation and Authentication Process

The service providers in both the public and private sectors typically follow their own process in the customer/beneficiary identity creation. This is in addition to service entitlement identification at the time of service delivery as per their needs, with limited or no interoperability as most of the identity tokens are accepted for specific purposes and at specific locations only. The current identity system can work only in assisted mode since most of the identification tokens provided by the service agencies are physical tokens based on "what you have". This results in a higher setup cost for the authentication mechanism of each service provider. Moreover, this process gives limited scalability and cause extreme inconvenience to the residents.

The service providers' identity creation process is different from one another in terms of the personal information captured, to the extent that verification and validation of that information results in the creation of multiple identities for the same resident. For instance, the VSS maintains a separate database of beneficiaries and their service entitlement identification for each of their welfare programs (social insurance, health insurance, etc.). A separate identity token, such as a card, is issued for each of the programs. This results in leakages of welfare benefits due to the creation of a large number of duplicate and fake identities within the same benefit program. Service agencies are unable to correlate the different benefits given to a resident through various programs, as they are unable to even verify the correct entitlement. This challenge potentially lowers the impact of welfare programs.

Paper-based Identity Card Leads to Higher Risk of Identity Thefts

With a paper-based ID card that is issued at creation process, there is a higher risk of identity theft and misuse of photocopies when submitted as PoI. It is easy to forge physical documents and difficult to identify fakes and copies. Also, such documents cannot be used to verify that the person carrying the token is indeed the person it identifies, except when it also contains a photo.

Furthermore, the current ID card is subject to misuse since there is no authentic audit trail and instead relies on an exhaustive manual audit mechanism.

5.0 Vision for Electronic Identity Service Delivery Framework (EISDF)

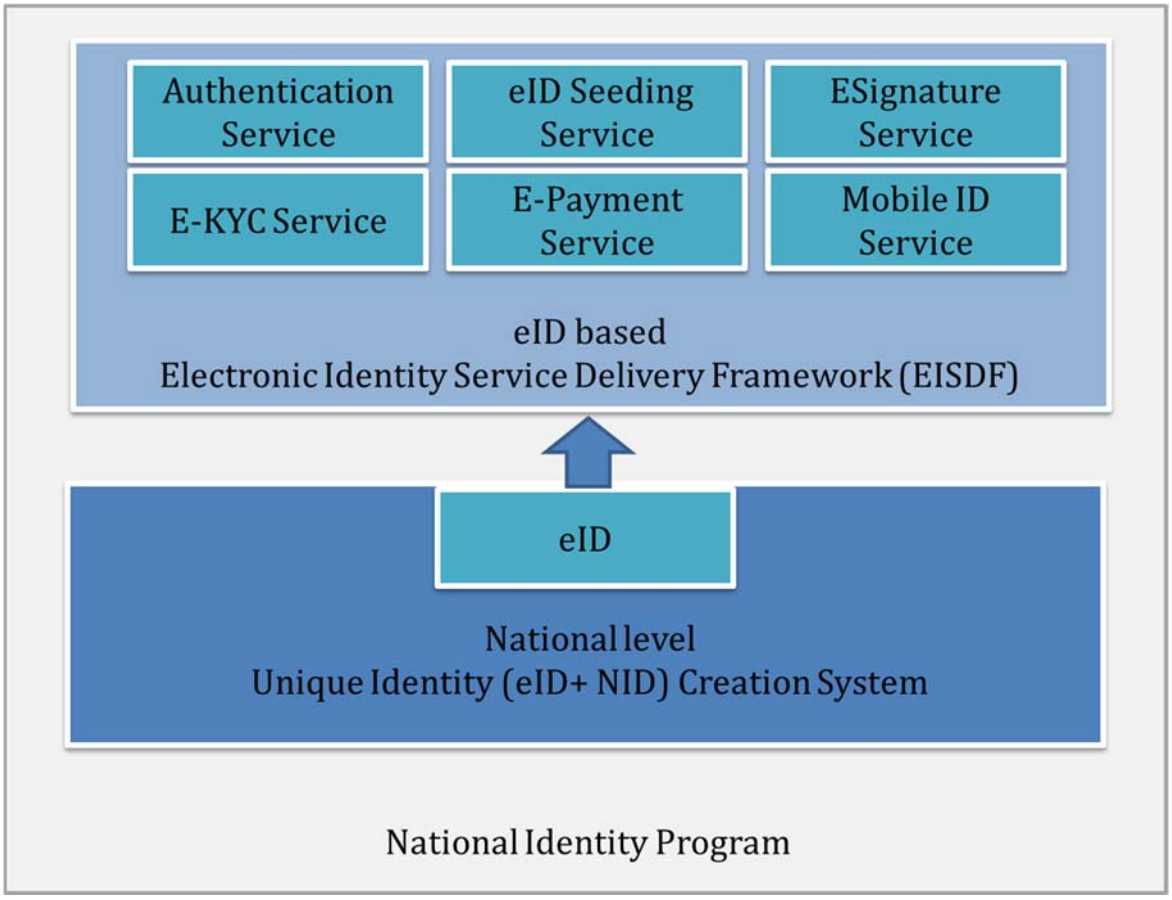


Figure 5.1: Electronic Identity Service Delivery Framework (EISDF)

In order to eliminate the issues currently facing service providers with regard to unique Customer/Beneficiary/Subscriber (CBS) identification and identity authentication, there may be a need for the development of a more robust and effective national identity system (NID) that includes the creation on the national level of a unique Electronic Identity (eID) and an eID services referred to as EISDF (Figure 5.1). The NID is being implemented by GoV. Such a system put in place will help achieve the vision of eGovernment and foster innovation in public and private eServices as well as strengthen cybersecurity. The eID would enable the resident to request and receive services from public and private sector providers anywhere, anytime, and by using any device. The focus of this chapter is to develop the vision for the EISDF.

5.1 High-level Description of EISDF

Services Offered. Some of the key services that may be delivered with the implementation of the EISDF are explained below.

1. **Electronic Identity Authentication Service**. The EISDF would facilitate the delivery of a national-level electronic-based service for the unique identification and identity authentication of residents physically or online. It would be used by service providers in the public and private sectors for delivering eID-enabled services using eID-enabled applications to their CBS.

2. **Electronic Identity Seeding Service.** The EISDF would provide eID seeding service, which enables the use of eID authentication by mapping the CBS profile to its unique National Identity Number (NIN) generated at the national level on registration.

3. **ESignature Service**. The EISDF would put into effect the use of eSignatures by residents on eDocuments in transactions with the public and private sectors. This would enable paperless eService workflows and do away with the need for physical signatures.

4. **Electronic Know-Your-Customer Service.** The EISDF would provide a centralized Electronic Know-Your-Customer (eKYC) process by which a service provider is able to identity its CBS electronically with the explicit authorization of the latter. The eKYC, being eID-based, would furnish an instant, non-repudiable Proof of Identity (PoI) and Proof of Address (PoA), along with date of birth and gender. In addition, it would also yield the resident's mobile number and email address to the service provider, which further streamlines the process of service delivery.

5. **Electronic Payment (ePayment) Service**. The EISDF would provide a centralized eID-based ePayment service through the Electronic Identity Service Delivery Platform (EISDP). With ePayment, government agencies would be able to make fund transfers of public program benefits such as social pension, health benefits, scholarships, etc., to the intended beneficiaries. While the emphasis in the report is on Government-to-Citizen payments, if the electronic payment service is made available to the business and citizen communities, it could be used for Business-to-Citizen, Citizen-to-Business and Citizen-to-Citizen payments.

6. **Mobile ID.** The EISDF would provide a centralized mobile ID service in collaboration with mobile network operators to verify the resident's identification through their mobile phones. Having the mobile ID as an identification mechanism should also facilitate the growth of mobile applications and adoption in Vietnam.

EISDF Key Concepts. Some of the key concepts for enabling the seamless delivery of the eID services are described below.

1. **Centralized National-level Identity Service Provider**. The envisioned EISDF would be owned, designed and implemented by a centralized government-owned national-level identity service provider.

2. **Electronic Identity-enabled Applications and Service Delivery.** Service delivery applications that may use eID functions to identify and authenticate the resident would be referred to as "eID-enabled applications". The use of eID-enabled applications may be broadly referred to as "eID-enabled service delivery".

3. **Centralized National-level Identity Creation Process**. The EISDF would be based on a central identity creation system operated by a national government agency which issues the eID. A centralized process for identity creation ensures uniqueness of the eID. Hence, the service providers using the EISDF for identity authentication of their CBS do not need to recreate a separate process for its purposes. This would prevent the generation of multiple identities for the same resident by multiple service providers.

   This mechanism would eliminate the need for duplication of effort in identity creation by the service providers, and result in a reduction of the overall cost of identification.

   The framework could also leverage advancement in technology to enable providers to deliver a higher quality of service to the residents and empower them to prove their identity anywhere, anytime, and in multiple modes using the global and irrevocable eID.

4. **Identity that is Digital, Online-verifiable and Interoperable**. Going digital and online has always proven to increase access, convenience and transparency to the common man. Given that Vietnam has good Internet penetration[8] with fiber optic cables laid all the way to the commune level and wireless broadband connectivity at the village level with more

[8] Report on Internet Statistics of Vietnam - http://www.thongkeinternet.vn/jsp/trangchu/index.jsp

than 100 percent mobile penetration[9], there is an increasing demand from the CBS for eServices in both the government and private sector organizations. The eServices would require a digital and online-verifiable eID for delivery. The EISDF could also leverage advancement in technologies with the use of the eID which is digital, online-verifiable and standard-based interoperable for unique identification of residents.

5. **Identity Based on NIN, Demographic Attributes, and Biometrics.** The EISDF would leverage the use of the eID as defined by the identity creation process of the new NID system. The unique eID would be defined in terms of a person's demographic attributes (name, gender, age, address, etc.), biometrics (fingerprints, iris images) and the central government-issued NIN. Demographic data alone may not guarantee uniqueness; however, they would be linked to the biometric attributes of the individual to create a unique identity for NIN generation.

6. **Global and Irrevocable NIN.** The NIN identifies the residents and would give them the means to clearly establish their identity to public and private agencies across the country. The NIN would have three key characteristics:
   a. Permanence: It remains the same throughout the lifetime of a resident.
   b. Uniqueness: One resident has one identity number, and no two residents throughout the country have the same identity number.
   c. Globalness: The same identifier can be used across applications and domains from different service providers in the country.

7. **NIN Uniqueness through Biometric Deduplication**. The NIN would be issued by GoV during the initiation process called enrollment where a resident's demographic and biometric information are collected and the uniqueness of the provided data is established through a process called deduplication. The deduplication process would include running the demographic and biometric information captured during enrollment through the rigorous 1:1 mapping of the two sets of data to yield 99.99 percent accuracy before assigning a unique identity number to the resident. Post deduplication, the NIN may be issued and a letter containing the details sent to the resident.

---

[9] Mobile-cellular subscriptions - http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2012/Mobile_cellular_2000-2011.xls

The digital and online-verifiable eID could reduce the risk of resident identity theft and remove the issues of photocopied fake documents. It is easy to forge paper-based identity documents compared to the digital-based identity which is verifiable online.

The eID would be issued using the Personal Identity Data (PID) based on an individual's paired demographic and biometric information following the national policy of the government to ensure interoperability.

8. **Standardized Identity Supported by Tokens**. The EISDF would support standardized identity tokens of different types depending on the identity authentication and eSignature requirements of the service providers or their specific programs. The EISDF would support three different types of identity tokens: a personal identification number (PIN), or "what the user knows"; a mobile/One-Time Password (OTP)/digital certification, or "what the user has"; and fingerprints or iris images, or "who the user is". Identity tokens are described in detail in Annex 1. The eID of the resident would be assigned multiple identity tokens to be used, as appropriate, for authentication and eSignature based on the business need of the service being rendered.

Common Security and Privacy Considerations. The eID functions, as envisaged, would become available online across various domains and applications on a daily basis. Any online service may come under various kinds of attacks, including organized large-scale ones. This means that the delivery of secure eServices is of utmost importance. The design of the eID would include security and privacy measures at different levels to ensure high-level protection. They are described below.

Security Considerations

1. **Security of Resident Data Captured during Service Request.** The eID system would ensure the security of the personal identity data (PID block) captured on the front-end devices and applications through several means.
    a. **Encryption and Tamper-proofing.** The EIDSF would encrypt the data on the capture device before transmitting it over the network. The encrypted data would not be stored unless it is for buffered authentication for a short period of time and it would be deleted after transmission. Biometric and OTP data captured for the purposes of authentication would not be stored in the database on a permanent basis. The service would also support Hash-based Message Authentication Code (HMAC) to ensure that the PID block is not tampered in transit.

b. **Trusted Service Delivery Ecosystem.** The EIDSF would provide a mechanism for the registration and authentication of the terminal device, operator and other participants to form the trusted service delivery ecosystem. The digitally signed service delivery application on the terminal device would be used to identify the trusted devices and applications. The operator would be authenticated in the case of operator-assisted devices.

c. **Digitally Signed Service Request and Response.** In addition to the encryption of data, the registered provider digitally signs the service request and the service response is signed by the owner-government agency to establish trust and non-repudiation mechanism between the provider and the agency. The source of the application programming interface (API) call is heavily authenticated to ensure no malicious calls are processed. Digital signing of the response by the government agency would ensure that the integrity of the response is maintained and that the provider can trust the fact that the response, indeed, came from the right authority. This feature would allow applications to move eID verification fully online thereby avoiding paper processing and reducing the overall cost.

d. **Response Timestamp.** The eID service response to a request would have a timestamp to allow applications to verify "when" the service was delivered or the resident authentication was done. Applications would also use it for audit purposes. This can be useful in filtering the time range of when a particular NIN was issued during the authentication process.

e. **Audit and Certification Mechanism.** The EISDF would provide the mechanism for data and transactions audit and certification. The metadata and the responses would be stored for audit purposes for over a period of time for a minimum of six months. There could be standard audit and certification processes for application devices and overall networks across the ecosystem. Every service request would generate a unique response code that can be used for audit and troubleshooting purposes. This code would uniquely distinguish every transaction across the system, quite similar to the unique authorization code issued for every credit card transaction.

f. **Fraud Analytics.** The EISDF would avail of the Fraud Analytics software, a detection tool suite that identifies suspicious claims at the onset.

g. **Anti-Virus Software.** Software to prevent malware/virus attacks would be put in place, along with other network security controls and end-point authentication schemes.

2. **Security of End-to-end Network.** The eID service delivery would use a protected network for transmission of data using a secure channel such as the secure sockets layer (SSL) and a secure leased line or similar private lines as a defense against network attacks which result in denial of service (DoS). The service design would also ensure high availability and redundancy in case some parts of the network are compromised or unavailable. Service providers and their partners (agents, application providers, etc.) would put appropriate network security in place to guarantee their systems are protected from attacks.

3. **Securing Service End-points/CRIDS.** If centralized EISDF is exposed over a public network such as the Internet to partners, it is expected to come under DoS/Distributed DoS (DDoS) attacks. Since many applications in the country could heavily depend on functions such as eID authentication, it is strategically important not expose them over any public network like the Internet, and not create a "single point" of attack that can potentially affect multiple services. There are means to fully protect the eID from unauthorized external systems' direct network attack that could result in DoS and data theft. They are explained below.
    a. **Identity Service Provider Agency.** The EISDF service would be kept in the secure zone and exposed through multiple network end-points. The design would include the creation of authorized organizations like Identity Service Provider Agencies (ISPAs), and exposing authentication service solely through their secure private connections using leased lines. This is strategic in ensuring multiple end-points always exist to provide authentication service in a secure, and always available, fashion.
    b. **License Key Usage.** The EISDF would support the concept of license key similar to that issued in software licensing: a pattern of numbers and/or letters provided to license users. It ensures that only authorized service provider can access the authentication service. It provides a mechanism to enforce specific feature usage, expiry, etc. It also allows the service providers to extend the service API to their partner-agencies and to trust their requests.

4. **Standards-based Security Management.** The EISDF would implement standards-based security management; which includes information security management, potential security controls and control mechanisms, the Plan-Do-Check-Act (PDCA) process, the information security management system (ISMS), and implementation and risk assessments. The eID authentication function would support standards such as the ISO

27001[i] for information security management, the ISO 27002[ii] for potential control and control mechanisms, the ISO 27003[iii] for guidance on the use of the PDCA process, the ISO 27004[iv] to establish the effectiveness of the ISMS implementation, and the ISO 27005[v] for risk assessment, etc.

Privacy Considerations

1. **"Yes/No" Response.** This feature would be applicable to the authentication function only. The eID authentication would allow applications to "verify" the identity claimed by the resident at service request while still protecting their data privacy. The eID authentication function would only respond with a "yes/no" and no personal identity information is returned as part of the response. This is one of the key strategic options to ensure resident data privacy – that there is no mechanism to "get" data of a resident through the authentication API.

   To illustrate, the authentication API involves questions and answers handled in this manner: "Resident claims his/her name is so-and-so, is this correct?". While eID authentication may respond to a "yes/no" answer, it does not provide any scheme to ask questions such as: "What is the address of the resident whose national identification number is such-and-such?"

2. **Self-Verifiability of Response.** The eID authentication and eKYC response would provide a true electronic version of identity verification and proof for verification. It would allow decoupling of the response usage from the actual service request which generates the response. The response would be used long after its generation and would be used multiple times as required. The current practice of identity verification is done by collecting "attested" copies of documents. Attesting allows the system to "trust" the fact that the copy is indeed verified against the original. At a high level, the eID authentication response would allow the service provider agencies to self-verify the following:
   - Is this authentication indeed verified by the eLD-issuing government agency? ESignature would allow this check. This is akin to checking if an authorized officer has signed.
   - Is this authentication for a given NIN?
   - Was this authentication done within the last "n" months? A timestamped response allows this. It is useful to know if the authentication proof is recent.
   - What was authenticated? "Usage flags" within "info" allows this check.
   - Was name, date of birth, etc., verified?
   - Was biometrics used?

- Was full or partial address verified?
- Is the address verified during authentication the same as what is now provided by the resident? Hash value of demographic data would be used to uniquely identify secret information.
- In the case of the pension system, residents need to annually establish the fact that they are alive. This is currently done by having residents go to an authorized officer to sign a declaration. With eID authentication, an agency would authenticate a resident independently and provide the response to the pension system. The pension application can answer the question, "Has the person with such-and-such NIN been biometrically authenticated in the last six months?", by simply verifying the extensible markup language (XML) response. Then it is determined whether that person is alive or not.
- The eID authentication response is similar to the paper-based document currently in use which says, "To whom it may concern," and which is signed by an authorized officer on a specified date with the document clearly stating that "the person with such-and-such NIN has the name and address as given below".
- The eID response would be viewed simply as an electronic version of the paper-based document and may be trusted and self-verified by a third party application.

3. **Asynchronous Service Call via Transaction ID.** The eID can be called by the service provider applications in an asynchronous mode, that is, data transmission is intermittent rather than in a steady stream. The transaction ID could be used by service providers to assign a logical business transaction identifier while integrating eID services. This feature would allow the request/response scheme to be made synchronous or asynchronous without worrying about how to correlate a request to its particular response. Whenever there is integration between two independent systems, it is critical that every transaction has a common "identifier" for correlating the request and response; it could also serve audit purposes later. For instance, when conducting a payment transaction, a bank would have to keep track of it across the flow. Service response contains the same transaction code that was in the request allowing applications to correlate a response with a particular request.

4. **Buffered Service.** The eID system supports "Buffered Service" in which the PID of multiple eID-holders are collected and buffered at the service request device, then transmitted at a later time. The buffered service process, therefore, varies slightly from that of the normal case until the service requests are transmitted from the service request device.

From this point, the model and process are similar to the normal scenario: the buffered set of service requests are checked, structural validation of data is performed and forwarded to the service request processing server. Upon receiving the service result for each request, the service provider application forwards the same to the service request device that has placed the requests. Although the service request device may transmit multiple requests at the same time, each request would be treated as a separate transaction in the server and each request would have its own auth code. It is the responsibility of the service provider to ensure that the service request devices being used are capable of managing buffered service (including the capability to store multiple requests, transmit them at the same time, and receive and store the results of multiple requests). There would be an upper limit for the time duration that requests can be buffered. This duration may be determined by specifications defined by the owner-government agency. Since buffered service is provided only for supporting occasional connectivity issues on the field, buffering of requests would be done only on service request devices, and not on the servers of service providers.

Common Identity Service Usages. Service providers could use the eID system provided by the EISDF mainly for the following three broad usage types:

1. **Establishing Know-Your-Customer Credentials**
    a. **KYC for various services.** Identity and address verification would be a key requirement for the service providers to enroll a new CBS or to open a new account for an individual. Examples are issuance of a new tax code, telephone connection, bank account or Internet service account for an online business. The service provider in all such cases would be able to verify applicant identity and address using eID authentication. This is expected to substantially reduce the cost of the KYC process to service providers.
    b. **General Proof of Identity.** The PoI is a standard security-related requirement, e.g., for entry to the airport, and to qualify for various examinations in hospitals or schools where a large number of cases of impersonation are reported every year. Various Internet, social-networking and eCommerce websites could also use eID authentication to verify customers and subscribers whenever it is required to establish the true identity of the person doing a transaction.
    c. **Demographic Data and Address Verification.** The demographic data of the CBS in the databases of service providers could also be verified; this process would help in the database cleansing and management to weed out duplicate and ghost identities.

2. **Establishing Presence and Proof of Delivery**
    a. **Beneficiary Identity Verification.** Various social sector programs, where beneficiary identity needs to be verified before delivery of the service, are expected to be the most common users of the eID authentication service. Examples of its use include subsidized food and kerosene deliveries to below poverty line beneficiaries, health service delivery to health insurance beneficiaries, job applications registration by beneficiaries, etc. Identity verification would ensure that services are delivered to the right beneficiaries.
    b. **Attendance Tracking.** Another key purpose of eID authentication would be in establishing the presence of the beneficiary of the programs at the site for attendance tracking. For example, student and teacher attendance tracking for education-related activities, and labor attendance tracking for employment-related programs where outlay is linked to actual number of days the beneficiary reports for the program.
    c. **Financial Transactions.** Banks would authenticate the customer using the eID and other bank-related identity information (account number, user ID, along with password/OTP) before enabling financial transactions such as fund transfers and fund withdrawals.

3. **Unifying Resident-centric Information.** The (NIN) would be used as the common identifier to link related databases. The application for linking these databases would be for:
    a. A 360-degree view of the resident across social welfare programs, namely education loan assistance programs, subsidized health programs for newborn children and pregnant women, old age pension, etc. Such views could be used to improve the effectiveness of the government programs and to ensure benefits reach the targeted individuals.
    b. Healthcare and patient records database at the local, regional and national level.
    c. Credit bureaus for customer rating information.
    d. National employment and skills database, and tracking of individuals through the lifecycle.
    e. Large entities such as banks and insurance companies that need to implement a single-customer view across services.

5.2 Electronic Identity Services Detailed Description

The section below describes eID services and their specific features.

5.2.1 eID Authentication Service

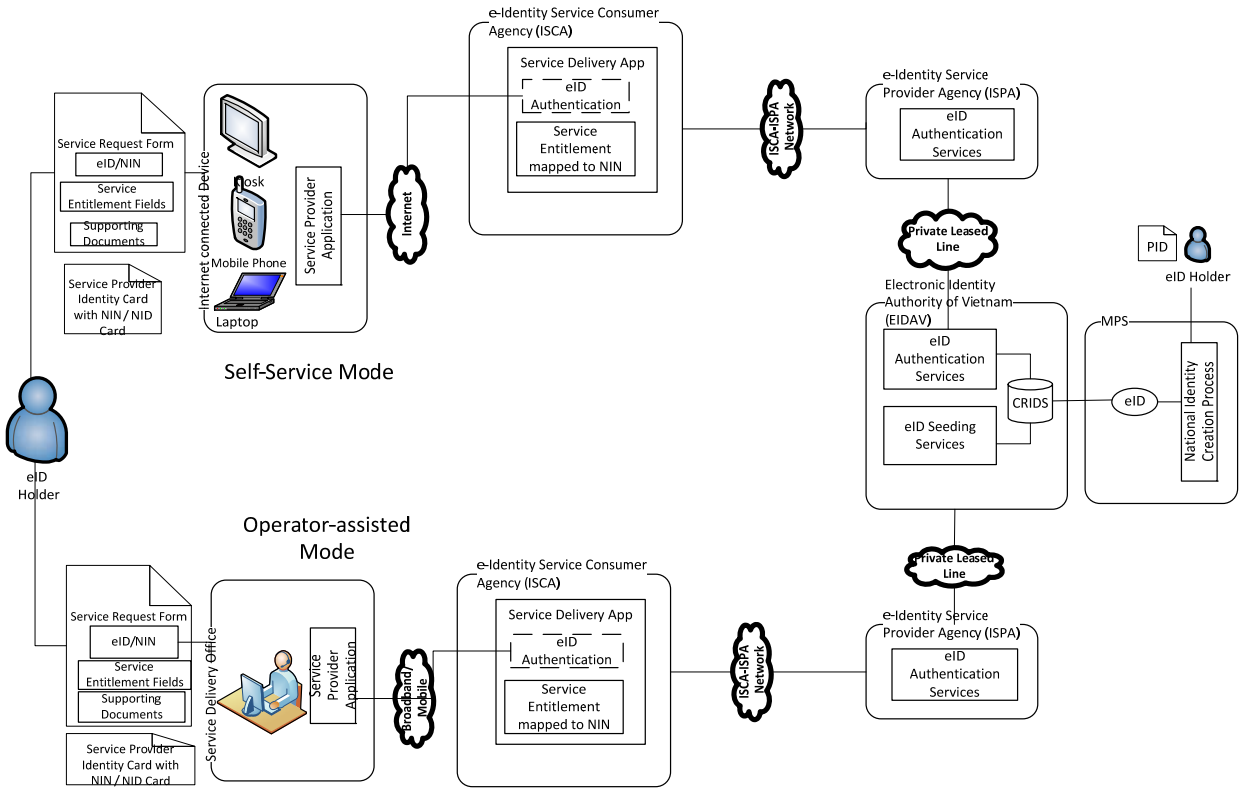


Figure 5.2: Functional View of the Electronic Identity Service Delivery Framework

The EISDF would provide eID authentication as the highly scalable, secure and available national online platform for the verification of the eID of a resident. The NIN and eID profile of the resident would be verifiable online using the demographic and biometric attributes over mobile, landline and broadband networks.

The eID authentication would be used by holders to prove their identity digitally and online, and for service providers in both public and private sectors to confirm the residents' identity claim in order to supply services and give access to benefits to their CBS. The service providers would be able to deliver different types of eID authentication to their CBS in both the self-service mode using mobile, kiosks or Internet-connected devices, and the operator-assisted mode using the point of sales (POS) terminal at designated locations as shown in Figure 5.2. The supported scenarios are detailed in Annex 1.

The eID authentication is based on the prerequisite that residents could be uniquely identified using the NIN assigned to them. The service could take the NIN along with the eID-holders' PID as the input which, in turn, verifies the correctness of the data provided on the basis of a match. The service would send a "yes/no" response to either confirm the PoI or verify the information provided by the resident.

Electronic Identity Authentication Service Types. Since the eID is meant to empower residents to prove their identity anytime, anywhere and in multiple modes, the proposed authentication service would support multiple types of authentication.

Support for Single-factor and Multi-factor Authentication. The eID system would support single-factor and multi-factor authentications. The NIN, by itself, would not be a factor for authentication. All authentication types would require the NIN for every request to reduce transaction to a 1:1 match. The NIN along with demographic attributes or single/multiple biometrics would be used to provide single-factor authentication, and these attributes could be used in combination to provide a multi-factor authentication to achieve the required authentication needs.

eID Authentication Service Classification Based on Type of Authentication Attributes. The authentication types would be classified based on the attributes used and could support the following types that can be used by the service providers depending on their business needs:

> **Type 1: Demographic** authentication would use any single/combination of the demographic attributes such as name, address, date of birth, gender, mobile number and email address. It would be used on a periodic basis to check validity of the credentials, or for cleaning up the service provider database by removing duplicates. Service providers can also use the demographic authentication for identifying CBS prior to any transaction.
>
> **Type 2: OTP** authentication would use a single-use password. It would be delivered to a mobile or email address on request initiated by the resident or an application. It would be used for authenticating residents for Internet and mobile transactions as well as in cases where deployment of biometric technology is difficult or not practical. The OTP feature would enable the authentication to be further strengthened by verifying the possession of the mobile by the resident. The eID authentication would be supported by biometrics and/or OTP. While the biometrics provide one factor (who you are), OTP provides an additional factor (what you have). Service provider applications would use OTP as what-you-have factor to provide single-factor authentication, or along with biometrics as who-you-are factor for achieving two-factor authentication. In a nutshell, the OTP

authentication request would be initiated by the resident using Short Message Service (SMS)/Unstructured Supplementary Service Data (USSD) portals; it can also be initiated by the service providers' application on behalf of the resident using OTP API. Notice that OTP authentication is always delivered to the resident's mobile or email, and the application is expected to capture that during authentication so that OTP would be validated along with authentication.

Type 3: Digital certificate or biometrics authentication would use eSignature issued to the eID-holder by the designated authority in Vietnam. The service provider would issue a smart card with digital certificate/biometrics, or use the mobile ID to authenticate the resident. It could be used for authenticating residents for Internet and mobile transactions and in cases where deployment of biometric technology is difficult or not practical and the business scenario requires higher security assurance level.

Type 4: Biometric authentication would use fingerprints and/or iris images. It would require the resident to be present to provide fingerprint/iris image capture on a device. Biometric authentication would be required in scenarios such as KYC, financial transactions, and attendance tracking. The biometric matching feature supports one or more fingerprint matching using either fingerprint minutiae resolution (FMR) or fingerprint image resolution (FIR), and iris matching using iris image resolution (IIR).

Type 5: Multi-factor authentication would use fingerprints and/or iris images, and/or digital certificate/biometrics, and/or mobile/OTP. It could be required in cases where there is a need for greater assurance.

Electronic Identity Authentication Type Based on Assurance Needs. The service provider would select the authentication type such as single-factor or multi-factor depending on the level of assurance required by them of their CBS. The selection criteria would depend on the risk, impact, implementation cost and volume of authentications. These are described in detail in Annex 1.

Authentication Assurance Increases with Biometric Attributes. Demographic authentication (Type 1) is based on demographic attributes and does not guarantee "proof of presence"; hence, it is associated with a lower level of assurance when compared to authentication based on biometric attributes, digital certificate and OTP. The OTP authentication (Type 2) or digital certification authentication (Type 3) is based on the OTP attribute or the digital certificate, respectively, and the PIN which guarantees "proof of presence" of the mobile/email registered by the resident or the availability of the digital certificate and the PIN. This process is associated with a higher level of assurance when compared to demographic authentication type. However, since the

mobile/email registered by the resident or the certificate and the PIN on the smart card or the mobile phone can be shared with family members or friends, it does not guarantee "proof of presence" and is, therefore, associated with a lower level of assurance when compared to authentication based on biometric attributes. Biometric authentication indicates presence of that individual; therefore, it provides the highest level of assurance. The assurance potentially increases as different biometric modalities such as fingerprints and iris images are introduced into the process.

Supports Federated Authentication Model. Most current authentication systems of service providers in Vietnam may be described as "local" (i.e., created, managed and/or valid for a few services, situations or entities) and "revocable" (wherein an existing identity factor would be revoked and reissued as a result of expiry, compromise or other valid reasons). Such revocable, local authentication systems come with a set of strengths and limitations. The EISDF, on the other hand, may be described as "global" (because of it is created and managed by a single national entity and it is applicable across situations, service providers and services) and "non-revocable" (because the eID factors such as fingerprints and iris images cannot usually be revoked or replaced). Global, non-revocable/permanent authentication systems come with their own set of strengths and limitations.

In the federated authentication model, the global/irrevocable eID authentication co-exists with and strengthens the local/revocable authentication. It is expected that such a federated approach would result in authentication systems that are stronger and more reliable than those that are based only on either the global/irrevocable model or the local/revocable model.

Hence, the EISDF could be designed with a view to strengthening the service providers' existing authentication systems, rather than replacing them. While the federated model would not mandate the existence or use of a service provider's own authentication (if a service provider so wishes, it could use only the EISDF by itself), it may be encouraged to use the EISDF in conjunction with its own local system to render the overall system stronger and more reliable.

The proposed authentication service in the case of multi-factor authentication could support the federated authentication model in which the service provider can use both factors from the proposed eID system, or one factor from the proposed eID system plus a second factor from another entity including that of the service provider itself. For example, a bank could choose a combination of biometrics and OTP as authentication factors from the proposed eID system, while another bank could opt for biometric authentication from the proposed system in conjunction with an ATM card/OTP issued by the bank itself.

5.2.2 Electronic Know-Your-Customer Service

A fundamental building block of service delivery is the eKYC process; which establishes a resident's identity along with the address and other basic information such as date of birth and gender. Typically, this KYC information is combined with other information to determine eligibility – be it for scholarship, loan, social security pension, mobile connection, etc.

The EISDF would provide a centralized eKYC service as part of the EISDP; through which the KYC process can be performed electronically with explicit authorization by the resident. The eID-based eKYC service would provide an instant, electronic, non-repudiable PoI and PoA along with date of birth and gender. In addition, it would provide the resident's mobile number and email address which further helps streamline the process.

The service provider could use the eKYC function primarily for performing the KYC process during the registration of a new customer or beneficiary, or for linking the resident profile stored its database with the NIN/eID database. The service would be accessible only to authorized service providers using the secure network of the ISPA. The EISDF could provide a mechanism for registering service providers to use the eKYC function.

The eKYC process could be performed at an agent's location using biometric authentication as well as remotely using an OTP on a website or mobile connection. As part of the eKYC process, the residents could authorize the owner-government agency – through eID authentication using biometrics/digital certificate/OTP – to provide their demographic data, along with their photograph, digitally signed and encrypted to service providers.

The owner-government agency could publish the eKYC API specifications on their public portal. The authorized service provider could invoke the eKYC function using the eKYC front-end application. The application could capture the NIN along with the biometric/digital certificate/OTP of the resident to form the eKYC XML by encapsulating the PID block, encrypting the XML, affixing the eSignature and sending it to the eKYC system using the secured private network of the ISPA. The eKYC system would authenticate the resident. If the authentication is successful, it would respond back with a digitally signed and encrypted demographic data and photograph in XML format. The demographic data and photograph, in response, are encrypted with the public key of the service provider.

Some of the key features of the service could be:

1. **Paperless.** The service would be fully electronic and document management may be eliminated.

2. **Consent-based.** The KYC data would only be provided upon authorization by the resident through eID authentication, thus protecting resident privacy.

3. **Eliminates Document Forgery.** Elimination of photocopies of various documents that are currently stored in the premises of various service providers reduces the risk of identity fraud and protects resident identity. In addition, since the eKYC data is provided directly by the owner-government agency, there is no risk of forged documents.

4. **Non-repudiable.** The use of resident authentication for authorization, the affixing of a eSignature by the service provider originating the eKYC request, and the affixing of a eSignature by the owner-government agency when providing the eKYC data would make the entire transaction non-repudiable by all parties involved.

5. **Low-cost.** Elimination of paper verification, movement and storage could reduce the cost of the KYC process to a fraction of what it is today.

6. **Instantaneous.** The service could be fully automated, and KYC data would be furnished in realtime, without any manual intervention.

7. **Machine Readable.** Digitally signed electronic KYC data provided by the owner-government agency would be machine readable, making it possible for the service provider to directly store it as customer record in its database for purposes of service, audit, etc., without human intervention, thus making the process low-cost and error-free.

8. **Secure and Compliant with IT Policy.** Both end-points of the data transfer are made secure through the use of encryption and eSignature following the national IT security policy, thus making the eKYC document legally equivalent to a paper-based document. In addition, the use of encryption and eSignature would ensure that no unauthorized parties in the middle can tamper or steal the data.

5.2.3 Electronic Identity Seeding Service

The EISDF would provide eID seeding service which is a process by which the NIN of a resident is included in the database of service providers to enable eID authentication. The process allows the service provider to map the CBS profile to the NIN. The objective is not to replace the unique identifier currently employed by service providers, but to seamlessly enable eID authentication using the NIN without impacting any other interface that the service providers maintain for their customers.

This could help to weed out duplicates and fake identities in the database of service providers and reduce the leakages of welfare benefits. This could also enable the service providers to correlate different benefits of various programs using the unique NID-mapped profiles of the CBS. The practice could result in proper delivery of entitlements and a greater impact of welfare programs. The repeated need for KYC checks during service delivery would be avoided by seeding NIN in the databases of service providers.

Service providers would be responsible for seeding their databases with the NIN/eID information. The EISDF would provide them the necessary tools, expertise, best practices, and consulting advisory on request for the implementation of the seeding process. Some of the tools which would be provided include seeding utilities and a centralized National eID Seeding Platform (NESP); they are detailed in Annex 1. The eID seeding process would be a combination of several sub-processes, and no one solution may apply to all cases. Therefore, it is essential that every seeding process is thoroughly analyzed and planned before proceeding with the actual seeding.

The eID seeding process would necessarily be preceded by data digitization and centralization in the service provider database. The EISDF would support top-down and organic methods of seeding. In the case of the top-down method, the service provider would use the already available database of the residents to compare with the profile of the residents in the service delivery database; it would not contact the residents for the seeding process. However, in the case of the organic method, the service provider would contact the resident, or vice-versa, for updating of the NIN in its database. After the completion of top-down seeding and organic seeding where no direct update of the database is enabled, the next step is to conduct a demographic authentication of the data in the service delivery database. This is to ensure that the seeding process has been done correctly.

5.2.4 Electronic Payment Service

In order to promote transparency, accountability, efficiency and correct targeting in the benefits delivery of government programs such as social pension, health care, scholarships, etc., the EISDF could provide a payment mechanism called National eID-based Electronic Payment Service (NEPS). The NEPS would leverage eID authentication and the eID-Enabled Bank Account (eBA) for routing the money to any resident on the basis of an eID. The NEPS would provide a centralized national eID Payment Bridge (ePB) which would maintain the repository of the NIN/eID and the corresponding eBA mapping for all the eID-holders in Vietnam. The residents could provide their primary bank account details for receiving the government benefits at the time of NID enrollment for the eBA. In case a resident has not provided bank account information at the time of enrollment, an instant account could be created on the basis of the NIN/eID and serve as the eBA

for the resident with a debit freeze. Money transferred would be credited to the instant account that could be activated during the first withdrawal on the basis of eKYC.

The eID owner-government agency, along with other relevant government and private stakeholders, could appoint a government agency to be responsible for implementing and managing the NEPS.

Government departments would have to register with the NEPS as users of its service in the disbursal of government benefits payment through registered sponsor banks. Sponsor banks" are banks (both commercial and government owned) in Vietnam who may provide their service to the government departments in the disbursal of government benefits to the residents of the Vietnam. The bank would have to register with NEPS as the sponsor bank in order to provide their services to the government departments. Both the public and private sector banks could register with the NEPS as a sponsor banking institution to cater to user-agencies registered with the NEPS. A user-agency could submit an ePB file with the NIN/eID of a beneficiary, the user-agency identifier, the welfare scheme reference number, and the amount to be paid to the beneficiary's bank in a pre-defined format to the sponsor bank. ePB file is pre-defined formatted file that is generated by the government agency which captures the payment details for all the beneficiaries in the given welfare schemes. This file is sent to the sponsor bank IT system electronically. The sponsor bank validates the data and attaches the Bank identification number (BIN) in the ePB file and submits it to the NEPS system.

The sponsor bank could add its NEPS-issued Bank Identification Number (BIN) to the ePB file and upload it onto the NEPS server. The NEPS processes the uploaded file, prepares the beneficiary bank file and generates a settlement file. The destination bank would then download the incoming file for credit processing after the settlement file has been processed. Using the credit file, the destination bank could use their Core Banking System (CBS) to credit the funds to the bank account of the beneficiary.

The beneficiary bank would provide the mobile-based or web-based application used by the beneficiaries to withdraw funds, check their account balance, and allow for the initiation of electronic payments. The issue of how the propose application allows for fund withdrawal could also be examine in a pilot phase. The application would authenticate a beneficiary by using the eID before enabling the beneficiary to access the account for any transaction. For the resident who does not have access to a mobile-based or web-based application, he/she may walk to a bank branch to perform the transaction. The resident also may use the micro-ATM with the Banking Correspondent (BC) nearby to perform the same transaction to avoid travel time and effort involved in having to go to a bank branch that is inconveniently located.

This could promote the use of the formal banking system and electronic payment for financial transactions by residents of Vietnam. It could also enable a faster channel for receiving all welfare payments without middlemen, and promote ease of accessing bank accounts at anytime and anywhere.

For government departments, the use of eID as the primary key could eliminate ghost and fake beneficiaries and lead to better targeting. It could also reduce the time and cost of payment processing and provide electronic audit trail and end-to-end visibility of all payments to improve the transparency and accountability within departments.

For banks, use of the eID system could help in having a unique identification of their customers, encourage electronic payments and, thus, reduce cash management costs. It would enhance the reach to customers in remote areas using the BC and micro-ATM model, and enable greater customer acquisitions.

It would be worth noting several considerations with the above proposed concept:

- It assumes that one person has only one bank account;
- The person has to go to the ID authority in case there is a change in bank account number;
- If a bank is not involved in the sending side, then the ID authority has to start dealing with funds; and
- If a person's Id number is not tagged with an account number.

While this approach might work in the context of Vietnam, there are other alternatives that could be considered. For example, the agency responsible for the benefit payments can simply maintain the ID and the bank account number. If there is a concern on ownership of bank account number, the agency can validate the name, etc. with the ID agency and also with the bank. This way a recipient deals with the agency has a direct on-going relationship.

5.2.5 ESignature Service

The EISDF could provide a centralized eSignature service as part of the EISDP for the resident to be able to digitally sign eDocuments, thereby enabling an end-to-end eService by providers in Vietnam. The service would provide a universal system for giving, processing and verifying eSignatures. It can be connected to any new or existing service delivery application using the common standardized workflows in the form of the common document format applicable to each service independent of the service provider. The service would use a digital certificate issued to the resident by the competent government agency of the Vietnam. The digital certificate would be issued to the resident at the time of enrollment in the eID system, or the resident would

request for the digital certificate separately after the issuance of the eID. The issuance of the digital certificate would require the availability of the NIN.

The EISDF could provide software for use by residents in signing the eDocuments. The software would include base and intermediate libraries, client utility, web services and end-user applications. The client utility can be installed on the residents' Internet-connected desktop/laptop/smart phone and used to sign eDocuments with the eID card or the mobile ID, check the validity of eSignatures, and open and save documents inside the signature container. The client utility can be made available to anybody to download for free from the EISDF public portal. The portal could also provide the instructions for the installation of the software by the residents on their device. The working of the client utility using the desktop or Internet browser is detailed in Annex 1.

5.2.6 Mobile ID Service

The EISDF would provide mobile ID service for digital signing of eDocuments and for authentication of eID-holders. The mobile ID allows residents to use their mobile phone as a form of secure eID for authentication and eSignature. Like the ID card, it could be used in accessing secure eServices and digitally signing documents, but with the advantage of not requiring a card reader. The eSignatures and its associated digital certificate could be issued to residents who needs such a service, as massive implementation for all residents is likely not feasible from a process and management perspective.

Qualified eSignatures are advanced eSignatures that are based on a qualified certificate and which are created by a Secure-Signature-Creation Device (SSCD). Usually, the latter implies the use of a specific smart card. As an off-the-shelf personal computer (PC) or notebook would not contain a reader for the simple use of a smart card – the procedure required before the card can actually be used – it can be quite time-consuming and costly to have to install one. In the case of mobile ID, there is no need for installation of any card reader and no complicated installations are required for its use. It can be used anywhere in the world where there is mobile coverage.

The International Telecommunication Union (ITU) has ranked Vietnam at the eighth position in the world in terms of mobile subscription density. Therefore, the mobile ID could be a good option for faster adoption of the use of eID. As smart phone technology becomes more widespread, having the mobile ID option would become increasingly handy, allowing further adoption of eID for use in mobile applications. This could also help the top mobile network operators (MNOs) in Vietnam to increase their revenue per subscriber without adding new virtual subscribers.

The system would be based on a specialized mobile ID SIM, which the resident should request from the mobile phone operator. The two certificates along with their private keys could be stored on the mobile SIM with a small application for authentication and signing.

The government could delegate the responsibility of issuing the mobile ID to the national mobile operators, namely Viettel, Mobiphone, Vinaphone, etc., through their local stores. Residents would go to their nearest mobile operator with their ID card with valid certificates for issuance of the mobile ID. The resident simply signs a contract (mobile ID subscription agreement) with the mobile operator to get the mobile ID, and activates the service on the handset with the new specialized SIM. To activate the mobile ID service or to apply for the certificates, the resident would go to the website of the EISDF to submit an application online.

The mobile operator could charge the resident for the mobile ID service. The charges would include a one-time subscription fee and monthly fees. If the mobile ID is used outside of Vietnam, each mobile ID transaction could be charged at the cost of sending one text message as specified on the package price list.

The mobile ID could be used by the residents for logging in to secure sites; for instance, a bank account:

1. The resident would click the "Log in with mobile ID" option on a supported website.

2. The resident would be prompted to enter his/her mobile number and personal identification code.

3. The website would display a unique verification code online.

4. The phone would beep and display a screen indicating that a connection is being made.

5. The phone screen would display the authentication service name and verification code.

6. If the service name is correct and the verification code corresponds to the displayed number on the page on the computer screen, then it would be safe to press "Accept".

7. The user would be prompted to enter a mobile ID PIN on the phone

8. The screen on the phone would disappear and the website is automatically reloaded with a logged in screen.

6.0 Implementation Strategy Recommendations

The implementation strategy for the vision of the Electronic Identity Service Delivery Framework (EISDF) could include the high-level technical architecture options for the development of state-of-the-art, highly scalable and secure Electronic Identity (eID) service delivery IT infrastructure and platform. This will support an institutional and legal framework including an organizational model, an operating model and the identification of national policies needed for the governance and regulation of such a framework. It could also include the communication strategy to develop awareness and provide tools to key stakeholders to promote the adoption of the framework in Vietnam. The section below describes some of the implementation strategy recommendations related to the eID framework, technical options, communication strategy, institutional and policy framework for the EISDF. It is to be noted that the proposed implementation strategy recommendations will depend heavily on the foundation set by the National ID program.

6.1 Technical Recommendations

1. **Electronic Identity Service Delivery Platform (EISDP).** The shared centralized IT infrastructure and common services platform could be designed and implemented using common standard mechanisms and open standards-based technologies for facilitating eID-related processes performed by service providers in the government and private sector organizations. Service providers could delegate the common eID-related processes such as unique identification and identity authentication of their customers/beneficiaries/subscribers (CBS) online to the EISDP, instead of recreating their own mechanism for identification and authentication. This could remove the duplicate efforts of identity creation and in turn could reduce the overall cost of the service delivery process. This could also enable standardized and interoperable identity and identity authentication process for the residents across all service providers in Vietnam.

2. **Key Technical Components of EISDP.**
    a. **Public Portal.** The EISDP could provide a common public portal for sharing public information related to identity services for the residents, technical content, development and testing environment for software developers to help them develop eID-enabled software applications, and service management and monitoring applications for various stakeholders accessible over the Internet and intranet. The portal could provide user registration and authentication capabilities

for accessing the protected content on the portal. For further description and technical details about the public portal, refer to Annex 4.

b. **Electronic Identity Services and Common Applications.** Some of the eID functions and common applications required by service providers in the unique identification and identity authentication of residents could be hosted on the EISDP, rather than repeatedly hosted by service providers. The common eID functions and applications that could be hosted on the EISDP are:
    i. The eID system and eID authentication, electronic Know-Your-Customer (eKYC) application, eID seeding, ePayment, eSignature and mobile ID services.
    ii. Common applications: Management Information System (MIS), Decision Support System (DSS), Fraud Analytics, registration and management applications of Identity Service Provider Agencies (ISPAs) and Identity Service Consumer Agencies (ISCAs), and application and IT infrastructure management systems.
    iii. The Centralized Resident Identity Data Store (CRIDS)/EISDP could host an updated version of the centralized and highly secure database of the eID (NIN + demographic and biometric data) of the residents.
c. **IT Infrastructure (hardware and software).** The EISDP could support the IT infrastructure recommendations as described below. For the detailed description, refer to Annex 5.
    i. The eID services could generally be exposed as stateless web services.
    ii. Both the eID services and common applications could be hosted on two separate scalable, highly available virtualized web farm with clustered virtual web servers within the centralized data center.
    iii. The IT infrastructure could support server virtualization and capabilities for the management of virtualized and physical IT infrastructure environment.
    iv. The Electronic Identity Authority of Vietnam (EIDAV) data centers would not have direct access to the public network. It would only be accessed by the registered ISPA using dual redundant private leased line connectivity between the ISPA and EIDAV's data centers.
    v. Adequate security measures could be designed to prevent any malicious access outside of the private network by hosting web farms in a secure zone of the network infrastructure protected by firewall, and the separate isolated network with the redundant switches.

vi. The data could be stored on the servers and storage devices in the data zone that is separated from the secure zone using the firewall. The data storage system could be designed to be highly available and scalable.

vii. The disaster recovery center could have the same configuration and capabilities as that of the production data center, and operate in the active-active mode.

viii. The portal and development environment servers could be accessible over the Internet and could be completely isolated from the servers and the network of the secure and data zones in the De-Militarized Zone (DMZ). The servers for the public portal and development environments could be hosted on a different segment of the network completely separated from the servers in the secure and the data zones.

ix. The residents' eID data in the CRIDS could be populated and updated on a regular basis using a centralized national-level identity creation process. Instead of recreating the identity creation process, the CRIDS could be populated by reusing the resident database created by GoV for issuing the national identity system (NID) card and the national identity number (NIN) to the residents of Vietnam.

x. Given that the NID card and the NIN would be issued at the national level, there could be a single process for identity creation and verification of the identity; hence, the problem of multiple identities for the same resident could be solved. The NID card could be used as the centrally issued national identity token to identify the residents uniquely and the NIN could be used as the unique identifier for the eID of the resident in the envisioned EISDF.

xi. There could be a periodic transfer of the new residents' data from the NID system to EIDAV as and when new residents are enrolled, until all the residents have been issued the NIN and NID card. A secure operational model for transferring updates, such as address change, to the resident data stored in the CRIDS and the NID resident database on an ongoing basis could be designed.

d. **Physical Infrastructure.** The EISDF could include the implementation of the physical infrastructure such as the data centers at various locations based on the topology and implementation requirements for the EISDF. The EISDP's physical infrastructure that could be part of the overall physical infrastructure of the EISDF. The figure below describes the possible topology of the physical infrastructure to be established for the implementation of the overall EISDF.

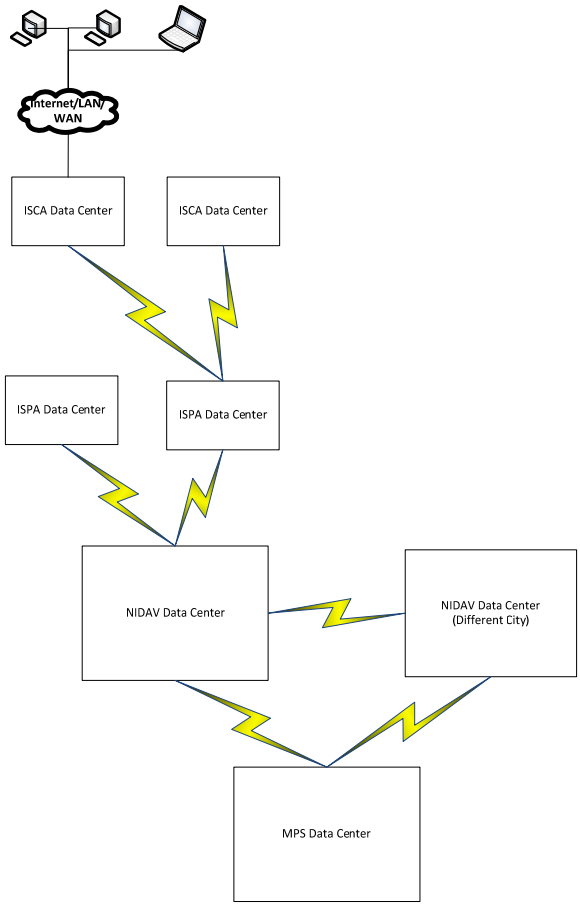


Figure 6.6 – EISDF Physical Infrastructure Topology

EISDP physical infrastructure could include the following components and for further details on each of the component, refer to Annex 4.

i. **EIDAV Data Center.** The EISDP could be hosted at the national-level centralized data center, namely the EIDAV data center. Since all the EISDF eID services could be hosted at this data center and the eID services could be used by the mission-critical applications of the government and the private sector organizations, this data center could be designated as a national critical infrastructure.

ii. **EIDAV Disaster Recovery Center.** The disaster recovery center could be built in a different geographical location, such as a different city in a different seismic zone from EIDAV data center. The disaster recovery center could provide the failover support for eID services, applications and IT infrastructure of EIDAV data center. It could work in the active-active mode and could host the eID services and applications to provide load balancing

and fault tolerance solution to EIDAV center; it could also fall back to the EIDAV center in case of any failures.

iii. **NID Data Center.** The NID data center could host the national identity information database, and the latter could be used to populate the citizen database in the EIDAV data center for identity services delivery.

e. **Safety and Security Systems.** EISDP could provide the common security functions and be hosted on the platform. Some of these functions could include end-to-end security of the network using the standard network security practices at multiple levels such as the usage of encrypted channels, IP filtering, authentication of systems and devices, creation of security zones, network protection through firewalls and the Network Intrusion Protection System (NIPS), auditing, etc. The physical security infrastructure could have a multiple level of security system for entry of authorized personnel, biometric-based access, etc.

f. **Operations Management.** The operations monitoring and management system could include technical, institutional and policy-level solutions across the physical and technology infrastructure, identity services and applications, and the information delivery interfaces of the EISDP.

3. **ISPA Data Center.** The ISPAs could be government or private agencies that could establish a secure private network between their data center and the EIDAV data center compliant with EISDF standards and specifications. The ISPAs offer their EISDF-compliant network connectivity as a service through their data center to ISCAs and transmit the latter's identity service requests to the EISDP. Some of the technical recommendations for the ISPA data center are described below and for further details, refer to Annex 4.

   a. Only the ISPA data center may send identity service requests to the EIDAV data center. The ISPA data center could be the critical infrastructure in the delivery of the eID services; hence, the design of the data center could include a disaster recovery solution with a remote data backup support.

   b. The EISDF could publish on their public portal the process for any government or private agency to register as an ISPA. The portal could also publish the detailed technical guidelines for setting up and operating an ISPA data center.

   c. ISPA applications and their respective databases could be hosted on the highly scalable and fault-tolerant virtualized servers. The data center could also include the required hardware and software for security, data backup, monitoring and management of the data center.

4. **ISCA Data Center.** The ISCAs could host their service delivery applications in the ISCA data center and integrate them with the eID services for unique identification and identity authentication of their CBS. The ISCA data center could connect with the Point of Sales (PoS) terminals and with the designated ISPA data center. Some of the technical recommendations for the ISCA data center are described below and for further details, refer to Annex 4.
    a. The ISCA could host their web-based service delivery applications in their data center, and client-based applications on their PoS terminal; which could send their eID service request to the ISCA data center that forwards it to the ISPA data center via a secure network.
    b. The ISCA applications and their respective databases could be hosted on the highly scalable and fault-tolerant virtualized servers. The data center could also include the required hardware and software for security, data backup, monitoring and management of the data center.
    c. The EISDF could publish the ISCA registration process and the detailed technical guidelines for setting up the ISCA data center on EIDAV's public portal.
    d. The ISCA would have to update their service delivery applications and PoS applications to integrate with the EISDF eID service Application Programming Interface (API) calls following the technical guidelines provided by the EISDF in order to ensure a secure and fail-proof delivery of services.
    e. The PoS applications could be centralized web-based or rich client-based applications connected to EIDAV-compliant biometric devices such as fingerprint capture, iris scan, and photo camera devices used to collect the biometric data of the resident.

5. **Electronic Identity Authentication Services.** Some of the technical recommendations for the implementation of the eID authentication services are listed below, and for further details, refer to Annex 4.
    a. The eID authentication service could provide several ways in which residents can authenticate themselves using the system and could support "demographic authentication" and/or "biometric authentication" and/or digital certificate/OTP.
    b. The eID authentication service could be exposed as stateless web service using the open data format in extensible markup language (XML), widely used protocol such as hyper-text transfer protocol (HTTP) and open standards-based technologies. These could enable easy adoption and deployment of eID

authentication services. For further details on the open standards recommendation, refer to Annex 4.

c. To support strong end-to-end security, only registered ISPAs and ISCAs could be allowed to use the service using the unique registration code and license keys to enable non-repudiation and message integrity. To avoid request tampering and man-in-the-middle attacks, encryption of data could happen at the time of resident data collection on the capture device, and no data have to be stored in the devices or log files.
d. The EISDP, ISCA and ISPA could maintain audit records for all the authentication request metadata along with the response to enable issue resolution, audits and business intelligence.
e. The servers of the EISDP, ISCAs and ISPAs could support buffering of authentication requests and responses to support occasional lack of network connectivity among ISCA, ISPA and EISDP data centers.
f. The eID authentication service could take the NIN along with the eID-holder's personal identity data (PID) as the input which, in turn, submits the data to the CRIDS for matching, following which the CRIDS verifies the correctness of the data provided on the basis of a 1:1 match with the eID-holder's identity information available with it. The service would respond with a "yes/no" response to either confirm the Proof of Identiy (PoI) or verify the information provided by the resident.
g. In all forms of eID authentication service types, the NIN could be submitted along with the single/multiple authentication factors so that authentication is reduced to a 1:1 match.
h. The implementation of demographic authentication could include the matching of the basic demographic attributes of the resident, such as name, address, gender, etc., captured as part of the service request input data with the PID data stored in the CRIDS. The demographic data fields and the matching design are further described in Annex 4.
i. The biometric authentication service type could allow service provider applications to verify if the resident is "who he/she claims to be". Several applications may require physical, in-person verification to ensure only the right resident is being served and right beneficiaries are being authenticated for service delivery. The implementation of biometric authentication service could include fingerprint and/or iris matching. The biometric data captured by the input device should comply with open standards to promote interoperability and avoid vendor lock-in situation. For further details, refer to Annex 4.

j. The One-Time Password (OTP) authentication service could enable the resident to initiate the OTP authentication request by using Short Message Service (SMS)/Unstructured Supplementary Service Data (USSD) portals or it can be initiated by the service provider application on behalf of the resident using OTP API. The OTP authentication could always be delivered on the resident's mobile/email, and the application could capture that during authentication so that the OTP can also be validated along with authentication.

k. The digital certificate/biometrics authentication service could enable the resident to insert their NID card into the card reader attached to the Internet-connected desktop for authenticating on the service provider application. The service provider application would read the digital certificate/biometrics on the card and initiate a call to the web service for authentication using the digital certificate/biometrics exposed as the API from the eID authentication service.

l. The digital certificate/biometrics authentication could also be initiated using the mobile ID. The resident would be able to select the mobile ID option for authentication on the service providers' website. The resident could enter his/her mobile number and NIN on the website. The application, in turn, calls the eID authentication service API for mobile ID which could respond by providing the unique code on the website. It could also connect with the mobile phone and invoke the eID authentication application on the mobile phone and display the same unique code.

m. The authentication service design could be extensible and support different tokens such as the mobile phone, Near Field Communication (NFC) token, smart card, etc., today and in the future. This could be useful in adding second factor ("what resident has") for a self-service transaction from the resident.

n. The authentication response could be used as the digital PoI and proof of address (PoA) at a later point in time by adding the meta-information of the PID details in the authentication request to the authentication response.

6. **Electronic Know-your-customer Service.** Some of the technical recommendations for the implementation of the eKYC service are listed below:

   a. The eKYC service could enable the KYC process to be performed electronically with explicit authorization by resident. The eID-based eKYC service could provide an instant, electronic, non-repudiable PoI and PoA along with date of birth and gender.

b. The technical architecture and security designs could be the same as that of the eID authentication service.
c. The service could be made available only to registered ISCAs and ISPAs; and is performed at an agent location using biometric authentication, as well as remotely using an OTP on a website or mobile connection.
d. Residents could authorize the ISCA through eID authentication using biometrics/digital certificate/OTP to provide their demographic data along with their photograph digitally signed and encrypted to service providers.
e. The eKYC service response could be an encrypted and digitally signed XML containing demographic data along with the photograph of the resident. It could be used as the eKYC document by the service provider, for delivering services to the citizen.

7. **ESignature service.** When a legal document is signed, all parties involved in the signed activity act on a set of basic assumptions regarding the signature:

- The signer intended to sign the document.
- The signer is who the person claims to be and is authorized to sign the document.
- The signature is that of the signer and is unique to the signer.
- The signature binds the signer to whatever the document states.
- The document will not be changed once the parties have signed it.
- A signature on one document is not transferrable to another document.
- The signer cannot later deny or repudiate the signature in an attempt to invalidate his or her relationship to the document.

The Need for eSignatures

An eSignature is the electronic equivalent of a handwritten signature. eSignatures have appealed to governments and businesses around the world due to the following reasons:

- Accelerate transactions — The requirement for handwritten signatures often result in lengthy delay in a transaction. eSignatures make possible long-distance transactions, in which parties are in different time zones or in different countries. In addition, digital signatures greatly reduces the amount of travel for in-person meetings, the cost of courier service, and the number of days and salaried hours needed to complete transactions.
- Reduce the amount of paper — Many public and private agencies and organizations still seek "the paperless office" because of the desire to cut down on the time, staffing, and storage space required to handle paper-based transactions.

eSignatures are divided into two separate categories — (1) digital signatures and (2) electronic signatures, which is distinguished primarily by the presence or absence of Public-Key Cryptography (PKC).

Digital Signatures

The term digital signature refers to the encryption and decryption technology used as the foundation for a variety of security implementations. Based on public and private key cryptography, digital signatures are used in secure messaging, public key infrastructure, virtual private networks, and electronic signatures.

Contrary to what the name might suggest, a digital signature *alone* is not a type of electronic signature. Rather, digital signature encryption could be used by electronic signature applications to secure the data and verify the authenticity of a signed record. Further, a digital signature *alone does not* capture a person's intent to sign a document and be legally bound to an agreement or contract.

Electronic Signatures

An electronic signature employs digital technology to bind a signature to an electronic document. In its most-secure solutions offered by service providers, the signature is bound to the document in such a way that neither the document nor the signature can be altered without invalidating the document.

An electronic signature is, like its paper equivalent, a legal concept. According to the U.S Electronic Signatures in Global and National Commerce Act, an e-signature is an "electronic sound, symbol, or process attached to, or associated with, a contract or other record and adopted by a person with the intent to sign a record." A digital signature, on the other hand, refers to the encryption / decryption technology on which an electronic signature solution is built. A digital signature alone is not a type of electronic signature. Rather, digital signature encryption secures the data associated with a signed document and helps verify the authenticity of a signed record. Used alone, it cannot capture a person's intent to sign a document or be legally bound to an agreement or contract.

eSigning Process

1. **Channel:** The resident fills out an application form on the organization's website, visits a retail branch, contacts a representative or the call center.

2. **Access**: The resident is provided with a link to the e-signing process from within the application process itself, or an email containing the link is sent to the resident inviting him / her to the e-signing session.

3. **Authentication**: The resident enters his / her personal information or credentials, and is brought into the e-signing session. For in-branch signing, the resident presents his / her credentials in paper format.

4. **Consent**: The resident is presented with the E-SIGN Consent form, as required by law. If he / she does not consent to the use of electronic signatures, the resident is provided with the ability to sign the documents using pen and paper.

5. **Presentation**: The resident is presented with all required documents and legal disclosures on-screen. The documents can also be printed and presented in paper format for in-person signing sessions.

6. **Affirmation**: The resident indicates his / her acceptance of legal disclosures and signs and initials documents by clicking on a button on-screen, or by hand-scripting his / her signature on a signature capture pad, iPad or other mobile device.

7. **Delivery**: The resident is provided a secure, tamper-proof copy of the e-signed documents in electronic format, or in paper format.

8. **Mobile ID Service.** Some of the technical recommendations for the implementation of the mobile ID service are listed below and for further details, refer to Annex 4.
    a. The mobile ID service could be based on SIM enabled by Wireless Public Key Infrastructure (wPKI) and supported by standard protection profile. The SIM could be procured through secure environment and supported mobile phones.
    b. The SIM could have Secure-Signature-Creation Device (SSCD) module, with two key pair; one for authentication, and the other for signing/non-repudiation purposes.
    c. The mobile ID service could be hosted on the EISDP as stateless web service and the service provider would have to integrate it into their service delivery application. The service delivery application could be hosted on the ISCA data center and could, in turn, call the mobile ID service hosted at the EIDAV data center with the NIN, mobile number and PIN.

d. In turn, the service validates the mobile number provided as the input with the mobile number stored in the CRIDS for the resident. After successful validation, it would call the Trusted Service Provider (TSP) web service hosted in the TSP data center over the secured Internet connection with the mobile number, verification code and PIN.
e. In response, the TSP service could generate the verification code and send it to the ISCA website. It could also generate the signature request with the verification code, mobile number and PIN and sends it to the resident's mobile phone using Over-The-Air (OTA) and SMS gateway of the TSP over the wireless network in SMS form.
f. The specialized OTA SMS activates the identity verification application on the SIM card. It could display the verification code which is the same as that displayed on the computer of the resident. The resident validates the verification code displayed on the mobile device with the one displayed on the computer and then signs the request by entering the PIN.
g. On successful authentication, the resident logs in to the secure website.
h. The mobile ID service would require SIM provisioning, user registration, certificate activation and termination of the service. Further technical details related to these operations are detailed in Annex 4.

9. **Electronic Identity Seeding Service.** Some of the technical recommendations for the implementation of the eID seeding service are listed below.
    a. A **seeding utility** would be a desktop client utility for seeding the NIN in the resident profile stored in the database of the service provider. The ISCA could download the utility from EIDAV's portal and install it on its server as the executable. The utility provides the capability for data extraction, consolidation, normalization and matching, and connects to different data sources to pull the relevant PID from the reference databases. It could also pull the data from the relevant data tables in the database of the service provider. For further details on the functioning of the utility, refer to Annex 4.
    b. The **National Electronic Seeding Platform** (NESP) could be a web application hosted on EIDAV's public portal. Residents and authorized users ("seeders") of the service providers login to submit the seeding request and verify the request ("verifiers"). The NESP would access the resident data stored in the CRIDS using the web services, and the resident data in the service enablement database using the web services or by setting the service enablement database in the NESP. The web

service for accessing the resident data in the service enablement database could be hosted on the ISCA server in the ISCA data center. The other option is to replicate the service enablement database into the database server in the EIDAV data center as part of the NESP. The NESP could also provide the mechanism to call the eID authentication service hosted on the EISDP for performing the demographic and biometric authentication for seeding validation.

6.2 Institutional Recommendations

Some of the institutional recommendations related to the operating models and organizational structure that would be required for the implementation of the EISDF from the technical and operating perspectives are listed below.

6.2.1 Operating Model

Electronic Identity Authentication Service

The eID authentication service could be used by the service providers across Vietnam. It would be governed by a highly scalable operating model based on Public-Private Partnership (PPP) to meet the demands of the service providers today and in the future. Some of the operating model recommendations for eID Authentication Service are:

1. The eID authentication service could be a delivered as part of the EISDF to all service providers in Vietnam. Hence, it would be managed and owned by a responsible, national-level ministry for delivering eID services such as eID authentication to service providers and not be responsible for any service entitlement. The responsible ministry could set up an agency, EIDAV, for such a purpose.

2. The responsible ministry would delegate to EIDAV as Managed Identification Service Provider (MISP) the responsibility to design and implement the eID authentication service and host it in the EIDAV data center as part of the EISDP. EIDAV could hire a solution integrator (SI) vendor to implement the service using tender. It could also implement the registration process for the eID authentication service on the public portal of EIDAV.

3. The public or private service providers wishing to utilize eID services such as eID authentication to enable its services could sign up as an ISCA and enter into an agreement with EIDAV.

4. The ISCA, in turn, could engage with a public or private ISPA. In order to ensure high security of the centralized store of the resident database that is on the EISDP, only a limited number of qualified ISPAs could be allowed to connect directly to the servers in the centralized EIDAV data centers.

5. The ISPA could establish secure connectivity to the eID services servers in the EIDAV data center to transmit service requests such as eID authentication on behalf of ISCAs and receive response back.

6. EIDAV could provide standards and specifications that the ISPAs have to comply with to build and maintain their secure connectivity to the services in the EIDAV data center.

7. The ISCA could have the option to connect to EIDAV's servers by itself or through an existing ISPA.

8. Furthermore, the service provider wishing to use eID services such as authentication could be given the option to choose to become an ISCA, or it may access eID services through an existing ISCA. In the latter case, it could become a sub-ISCA of the existing ISCA which it engages.

eKYC Service

Some of the operating model recommendations for eKYC service are described below.

1. Like the eID authentication service, the eKYC service could be managed and owned by EIDAV.

2. The service provider wishing to utilize the eKYC service to enable its services would sign up as an ISCA with access to the eKYC service, and enter into an agreement with EIDAV.

3. The ISCA, in turn, would engage with the ISPA to route the service request and receive response back from the eKYC service hosted in the EIDAV data center through the secure network of the ISPA.

4. The eKYC service could be performed at an agent location using biometric authentication as well as remotely using an OTP on a website or mobile connection. As part of the eKYC process, the resident would authorize the owner-government agency through eID

authentication using biometrics/digital certificate/OTP to provide their demographic data along with their photograph digitally signed and encrypted to the service provider.

5. The resident could go to the ISCA and, with the help of an operator or using an Internet-connected device, access the application to input data for the eKYC service request. The response is received in encrypted XML that is used as the eKYC document by the service provider in the service delivery to the citizen.

6. The resident may keep the eKYC response for later use when requesting service from the registered service providers in Vietnam.

Electronic Identity Seeding Service

Some of the operating model recommendations for eID seeding service are described below.

1. Service providers using eID services in their service delivery process would be responsible for seeding the eID/NIN in their service enablement database for unique identification of their CBS.

2. The implementation strategy for NIN/eID seeding in the service enablement database of service providers would be a combination of several sub-strategies and no one solution may apply to all cases. Therefore, it would be essential that every seeding process is thoroughly analyzed and planned before proceeding with actual seeding.

3. As the prerequisite to eID seeding, service providers could prepare their service enablement database by performing data digitization and data centralization on it. If a service provider already has its service enablement database digitized and centralized, then there is no action required from the eID seeding perspective. For detailed description of data digitization and centralization, refer to Annex 4.

4. Based on data availability and other requirements, the service provider could choose between the top-down approach and the organic strategy for NIN seeding in their service enablement database. For detailed description of eID seeding strategies, refer to Annex 4.

5. In the case of the top-down approach, the service provider could use the offline seeding utility or the eID Seeding Platform (eSP) for the NIN seeding in one batch. In the case of organic seeding, the service provider could use the eSP for seeders to send the seeding request and for the residents to respond; the residents could also come forward voluntarily.

6. The service providers would have to register with EIDAV to use the offline seeding utility and register online on EIDAV's public portal as the seeders and verifiers to use the eSP platform.

7. The service provider could register as the ISCA on the public portal of EIDAV to perform the demographic authentication of its CBS profile in its database using the eID authentication service to validate the seeding process. In cases where demographic authentication fails, the service provider could investigate the reasons for failure. Some of the reasons could be:
    a. The NIN was seeded into an incorrect record. This could potentially happen in cases of partial or fuzzy match.
    b. The resident updated his/her PID in the Central Identities Data Repository (CIDR) due to marriage, change of address, update of incorrect information, etc.
    c. There was an incomplete KYR+ form or incorrect data captured during enrollment (e.g., incorrect health insurance card number).

8. Biometric authentication could be enabled for operator-assisted touch-points where a direct update of service delivery database takes place.

9. The eID seeding services could be designed to address some of the common challenges during the seeding process. For common seeding challenges and their resolutions, refer to Annex 4.

Mobile ID Service

Mobile ID service could be governed by a highly scalable PPP-based operating model with four main operating procedures; namely SIM provisioning, certificate activation, usage and termination. The operating procedures are operated by entities that are defined in the organizational structure for mobile ID services later in the document. The recommendations on the operating procedures are defined below,

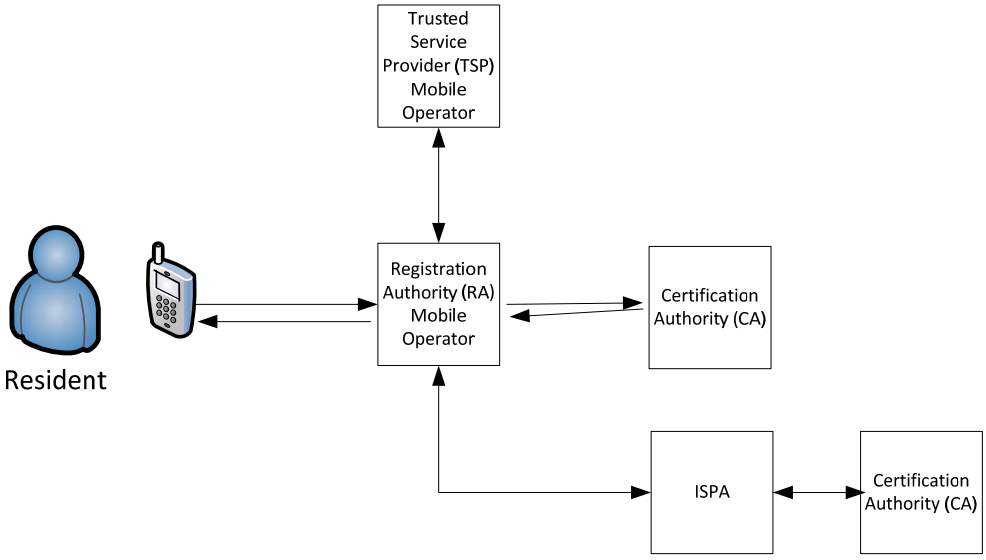


Figure 6.1: Operating Model for Mobile ID Service – SIM Provisioning/Certificate Activation

1. **SIM Provisioning**
    a. The resident wishing to use mobile ID service may go to the nearest outlet of a mobile operator that is registered with EIDAV as the approved registration authority (RA).
    b. The RA could provision the specialized SIMs with SSCD function that has the capability to issue a qualified digital certificate/biometrics for authentication and signing purposes.
    c. The RA could verify the identity of the resident by his/her NIN and biometrics using the eID authentication service. The RA could be registered as the ISCA with EIDAV to submit the eID authentication service request to the registered ISPA.
    d. On successful eID verification, the RA would issue the specialized SIM along with the secret activation code to the resident in a face-to-face procedure.
    e. The RA would declare the SSCD's device certificate active for that particular SIM and that information is made available for all TSPs.

2. **User Registration/Certificate Activation**
    a. The resident using his/her mobile phone would initiate the SIM activation application stored on the SIM. The resident would send a request to have the qualified certificate activated.
    b. The RA would respond to the request by initiating action on the resident's mobile device to sign the PID. The PID would include the NIN along with other demographic details.

c. The resident would verify the data and sign it by inputting their device certificate activation code.
d. The RA would receive the signed PID and add supplementary data including the device certificate, then forward the request for certificate activation to a certification authority (CA). The RA also sends the service request to EIDAV via a registered ISPA to update the resident's identity record with the mobile number.
e. The CA would create and activate a qualified certificate, and make it available to all TSPs and EIDAV.
f. The resident would be notified of the operation status and given the opportunity to change the pin.

3. **Usage**

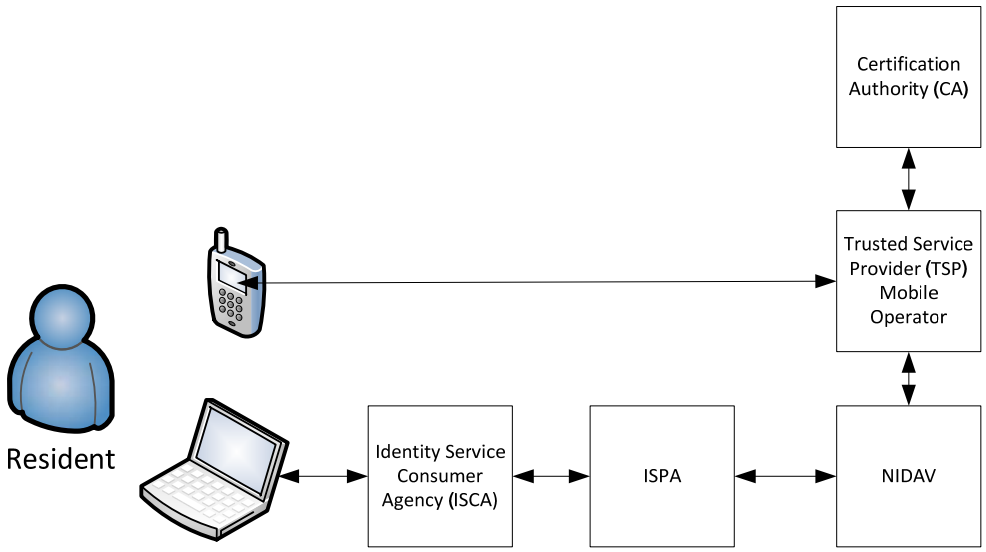


Figure 6.2: Mobile ID Service Usage Operating Model

a. The resident would use the mobile ID for eID authentication on a secure site, e.g., online banking.
b. The resident would access the secure website of the ISCA. The supported website would have the option to click the "Log in with mobile ID" button.
c. The resident would be prompted to enter his/her NIN, registered mobile number and PIN.
d. The ISCA system would call the EISDF mobile ID web service with the identity service request giving the NIN, mobile number and PIN via the ISPA to the TSP.

e. EIDAV's mobile ID service would validate the mobile number provided with the stored mobile number for the given NIN and forward the service request to the TSP along with the mobile number, verification code and PIN. The service would generate the verification code and send it to the ISCA website.
f. The TSP would generate the signature request with the verification code, mobile number and PIN and send it to the resident's mobile phone.
g. The resident would check the verification code on his/her mobile phone with the one on the website and sign the request by entering the PIN.
h. The TSP would receive the signature data and send it to the CA to validate the signature data and the certificate.
i. The TSP would forward the response received from the CA to the ISCA via EIDAV and the ISPA.
j. On successful authentication, the resident logs into the secure website.

4. **Termination**
   a. The resident could stop using the mobile ID service in several ways:
      i. The resident informs the RA of his/her wish stop using the service.
      ii. The resident informs the RA of lost/compromised SSCD.
      iii. The qualified certificate expires.
      iv. The RA finds out that the user has violated the user-CA agreement, or other laws governing mobile ID service.
   b. In cases of certificate revocation, the RA will inform the CA of certificate revocation. Then the CA immediately revokes the certificate and circulates the updated certificate revocation list (CRL) to all TSPs.
   c. In case of SIM blocking due to loss or SIM damage, the device certificate would be taken out of the list of valid SSCDs available to all TSPs.

6.2.2 Organizational Structure

The section below provides recommendations on the key roles in the organizational structure to operate and manage the EISDF eID services. For detailed description on the roles and responsibilities, refer to Annex 4.

1. **Electronic Identity Authentication Service: Key Roles**
   a. **Electronic Identity Authority of Vietnam.** EIDAV could be created with the mandate of generating the eID and providing EISDF-based eID services such as eID authentication to eligible service providers in the public and private sectors. This will enable business functions that require establishing the identity of CBS as well

as employees. EIDAV could be the overall regulator and overseer of the EISDF eID services ecosystem. It could also own and manage, either by itself or through an agency, the CRIDS that contains the NIN and the corresponding PID. EIDAV could manage the CRIDS and the eID authentication server through an MISP.

b. **Managed Identification Service Provider.** The MISP could be the entity that offers eID services such as authentication on behalf of EIDAV. EIDAV could hire one or more MISP depending on the service request volume. EIDAV would have the responsibility of implementation and operating the technical architecture of the EISDP as the MISP in the pilot phase.

c. **Identity Service Provider Agency.** The ISPA could be government or private agencies that establish secure connectivity with the EIDAV data center in compliance with the standards and specifications set by EIDAV to transmit eID authentication request on behalf of ISCAs and receive response back from eID authentication servers. Only agencies contracted with EIDAV as ISPAs may send service requests related to eID authentication; no other entity can directly communicate with the identity services. An ISPA would be bound to EIDAV through a formal legal contract. The ISPAs could offer their EIDAV-compliant network connectivity as a service to one or more ISCA and may transmit the ISCAs' authentication requests to the EIDAV authentication server. Possible of ISPAs are:

    i. A government department such as an MIC telecom department could become an ISPA and establish a secure EIDAV-compliant leased line connectivity to the eID authentication servers; through which several ministries/departments in the country could channel their authentication requests.

    ii. A telecom carrier such as Viettel Group or VNPT could obtain EIDAV's approval and establish a secure connection with EIDAV and offer ISPA services to ISCAs.

    iii. A nationalized bank such as the Bank of Vietnam (BoV) could establish a secure EIDAV-compliant connectivity to eID authentication servers and offer authentication services and, possibly, value-added services to itself and other smaller banks.

d. **Identity Service Consumer Agency.** The ISCA could be any government or private agency that seeks to use eID services such as authentication to enable one or more of its services. An ISCA could have the option of connecting to the authentication server by itself (in which case it needs to get an approval from EIDAV to become an ISPA), or through an existing ISPA for transmitting its service requests. An ISCA

could also send a service request from other entities that are "sub-ISCAs". The ISCA could act as the aggregator offering authentication services to sub-ISCAs and offer value-added services such as multi-party authentication, MIS reports and authorization to the sub-ISCA. An ISCA would have to enter into a formal contract with EIDAV in order to access EISDF eID services. Potential ISCAs could be:

i. The Vietnam Social Services (VSS) which seeks to authenticate a target resident before issuing one of its benefits.
ii. A bank which seeks to authenticate its customers before allowing them a financial transaction such as withdrawal or transfer of funds.
iii. The administration department of a high-security zone that seeks to authenticate individuals seeking entry into the premises.
iv. A social networking or eCommerce website that seeks to authenticate customers or subscribers during the registration process.

e. **Sub-ISCA.** Any legal entity registered in Vietnam desiring to use the EISDF eID services could become an ISCA, or it could access identity service through an existing ISCA. In the latter case, it could become a sub-ISCA of its chosen ISCA. The sub-ISCA would not have a direct contractual relationship with EIDAV. Only the ISCA is contracted to EIDAV and would be responsible for all service requests flowing through it, including those originating from its sub-ISCAs. The following are some possible sub-ISCA:

i. A government department at the provincial level could become an ISCA; and ministry branches/departments in the region could access the eID services as sub-ISCAs.
ii. A small business like a local bank which does not want to directly engage in a formal contract with EIDAV, but still needs to use identity services, may choose to become a sub-ISCA of an ISCA.
iii. Several entities could combine under a single ISCA for business reasons, e.g., several hotels could access eID authentication as sub-ISCAs of a hotel association that becomes an ISCA.

f. **Authentication Devices.** These could be electronic devices that form a critical link in the eID authentication service. These devices would collect PID from eID-holders, prepare the information for transmission, transmit the packets for authentication and receive the results. They could be either operator-assisted or self-operated. Examples of eID authentication devices include desktops, laptops, kiosks, handheld mobile devices, etc., that are, if required, connected to biometric

devices for capturing fingerprints and iris images. They could be operated by an ISCA/sub-ISCA or its agents.

g. **Electronic Identity-holders.** A holder of an eID-based identity is any eligible individual who has enrolled with and obtained a unique NIN and NID card. In the context of eID authentication, eID-holders are usually associated with ISCAs/sub-ISCAs as CBS or employees, and in this capacity seek access to ISCA/sub-ISCA services. In order for them to gain access, their eID is authenticated using their PID in the database. Depending on the authentication type sought by the ISCA/sub-ISCA, the eID-holders would provide their demographic and/or biometric information.

2. **eKYC Service: Key Roles**

   a. **Electronic Identity Authority of Vietnam.** As in the eID authentication service, EIDAV could be the overall regulator and overseer of the eKYC service and supporting ecosystem. EIDAV could determine the operating and engagement model for the eKYC service and define the eligibility criteria for the MISP and ISCAs. EIDAV could also determine standards and specifications that could be adhered to by all those participating in the eKYC ecosystem (including ISPA, ISCA and sub-ISCA).

   b. **Managed Identification Service Provider.** The MISP could offer eKYC service on behalf of EIDAV. The MISP's main areas of responsibility could include eKYC transaction operations (i.e., receive authentication request, execute a match of PID received by calling eID authentication service and transmitting the result), network operations, data center operations, availability of eKYC service, service-level agreement (SLA) with ISCA, if any, and monitoring operations and performance metrics.

   c. **Identity Service Provider Agency.** The eKYC service should only be accessible through the secure network of the ISPA.

   d. **Identity Service Consumer Agency.** The ISCA could be any agency that seeks to use eKYC service to enable its services. An ISCA could use eKYC service to enable one or more of its services. It could enter into a formal contract with EIDAV in order to access EIDAV eKYC service. The ISCA could ensure that the eKYC request originating at the service request device is compliant with the standards and specifications prescribed by EIDAV and complete before transmitting the request to its ISPA. For further details, refer to Annex 4.

e. **Sub-ISCA.** Any legal entity registered in Vietnam wishing to use eKYC service to enable its services could become an ISCA, or access eKYC service through an existing ISCA. In the latter case, it becomes a sub-ISCA of the ISCA it partners with.

f. **Electronic Identity Service Devices.** The eID device for eKYC service could be the same as that used for eID authentication, and have the capability to capture the inputs required for eKYC service. It could be operator-assisted or self-operated. Examples of eID service devices include desktops, laptops, kiosks, handheld mobile devices, etc., that are, if required, connected to biometric devices for capturing fingerprints and/or iris images. These could be operated by an ISCA/sub-ISCA or its agents.

g. **Electronic Identity-holders.** In the context of eKYC service, eID-holders would usually be the CBS or employees associated with ISCAs or sub-ISCAs, and in this capacity seek access to ISCAs/sub-ISCA services. In order for them to gain access to the services, they need to provide their KYC data for registration in eKYC service. It would be the responsibility of eID-holders to provide consent to the performance of eKYC service.

3. **Mobile ID Service: Key Roles**

a. **Registration Authority.** The RA would typically be the nationalized mobile operator such as Viettel, Mobiphone, Vinaphone, etc., responsible for the provisioning of the specialized SIM with SSCD functionality to residents at their service outlets across the country. A mobile operator would have to register with EIDAV to become an RA. The mobile network operator (MNO) could work with the national ID project in the provisioning of specialized SIM.

b. **Trusted Service Provider.** The TSP could also be the MNO responsible for forwarding the mobile ID service request from EIDAV to the mobile phone of the resident over the mobile network. It could also be responsible for sending the signed data from the mobile phone to the CA and responding back to EIDAV with the authentication response. Mobile operators would have to register with EIDAV to become an authorized TSP.

c. **Certification Authority**. The CA could be responsible for issuing the certificate; it is also responsible for the validation of the certificate and signed data in response to the TSP service request. The CA may be competent government entities, such as VGCA.

d. **Electronic Identification Authority of Vietnam.** In the case of mobile ID, EIDAV could host the service in its data center and would register and hire all the ecosystem entities in various roles for the scalable delivery of the services.
e. **Identity Service Consumer Agency.** The ISCA could be any agency that seeks to use the mobile ID service to enable its services. An ISCA can use mobile ID to enable one or more of its services.
f. **Identity Service Provider Agency.** The ISPA could be an agency that establishes secure connectivity with the mobile ID service hosted on the servers in EIDAV data center to transmit authentication requests on behalf of ISCAs and receive the response.
g. **Mobile Phone Device with Specialized SIM.** The mobile phone with specialized SIM issued by the RA could initiate the mobile ID service request on the device using the application and the private keys stored on the SIM.
h. **Resident-User.** The resident-user could be the individual who has registered with the RA to get the specialized SIM with SSCD capability and activated digital certificate/biometrics along with private key on the SIM.

6.3 Policy Recommendations

In order to ensure successful implementation of the EISDF in Vietnam, it may be supported by national policies to enable the governance structure to provide an auspicious environment. Some of the recommendations for the policy interventions are described below.

1. The GoV could update the relevant policies to enable eKYC response as the valid legal KYC document equivalent to the paper-based KYC document for service delivery by the service providers.

2. Service providers in both the government and private sector such as banking, insurance, capital markets, telecom, LPG, railways, etc., could update their KYC norms to include the NIN/eID and eKYC response as the valid KYC.

3. The GoV could define a national policy or update the existing one on data and metadata standards to include the data and metadata formats of both the demographic and biometric data fields of the resident to be stored in the centralized national eID database. There could be a national policy for KYR specifications that complies with the data and metadata standards.

4. The existing national policy on the adoption of open standards to promote interoperability could be updated to include eID data format. It could also include standards for biometric data such as fingerprint images, fingerprint minutiae, and iris images.

5. The existing national policy on the ESignature Act (EESA) could be reviewed and updated, as needed, to include requirements on the use of digital certificates or biometrics in the EISDF as defined in the technical recommendations previously discussed in this chapter. As a rule, handwritten and eSignatures could be equivalent in both the public and private sectors. The ESA could also state that public service departments could accept digitally signed documents. The ESA could ensure that each eSignature uniquely identifies the signatory, binds the individual to the signed data, and ensures that the signed data cannot be tampered with retrospectively without invalidating the signature itself.

6. The ESA could mandate stringent financial and procedural requirements to ensure that Certificate Service Providers (CSPs) and Timestamp Service Providers (TSPs) are set up and managed properly to perform their function to the highest possible standard.

7. The existing national policy on IT security could be updated to include the security requirements of the eID and the EISDF as defined in the technical and institutional recommendations previously discussed in this chapter.

8. The Personal Data Protection Act (PDPA) could regulate the use of personal data and databases containing personal information by public authorities and private entities. There could be an independent data protection inspection department outside the government; which ensures the requirements of the Act are met and enforces compliance if necessary. It will report directly to the apex body within the Prime Minister's office. Requests by third parties (e.g., representatives of authorities) for private data could be logged and the logs made available online for the individual on request via the citizen's portal.

9. The use of open standards-based technology in eGovernment implementation could be promoted with the national policy on open standards. It would include standard specifications for biometric devices, list of approved vendors of biometric devices and standard specifications for dedicated leased line for the ISPA, etc.

10. The GoV could pass an act an Identity Documents A (IDA) to establish national guidelines for the creation of the mandatory NIN, NID card and eID for the residents of the country. The law would also state that the eID may have the same legal value as that of the NID card, and decide the purpose of the card and of the number in terms of proof of citizenship. It could state that the deduplicated and processed resident demographic and biometric data used for the personalization of the card could also be entered into the national population register pursuant to the Population Register Act. There could be a legal provision in the form of a decree for transferring the resident data from the NID system to EIDAV's CRIDS for EISDF eID services on a regular basis.

11. The GoV may expedite the enrollment of residents into the new national ID program and delivery of national ID to all the residents. This may help in the faster delivery of the pilot of eID as the eID is based on the resident data collected from the national ID program.

6.4 Communication Strategy Recommendations

The communication strategy could include the steps to be taken to build awareness and promote adoption of the framework among the key stakeholders; such as service providers in public and private sectors and residents of Vietnam. Some of the recommendations for the communication strategy are described below.

1. EIDAV could set up a public-facing portal for awareness building among the stakeholders in the eID ecosystem, and to provide support to the users of the eID authentication services by publishing documentations related to technical solutions and updates.

2. There could be capacity-building programs in the form of online and classroom trainings targeted at the residents and officials/operators in the government and private sector agencies.

3. EIDAV could publish a set of technical documentations targeted at the technical stakeholders in the eID authentication ecosystem which could include the technical decision makers, technical architects and developers within EIDAV, and other service providers responsible for the design, development and maintenance of the eID authentication system.

4. EIDAV could also publish a set of technical documentations targeted at the software professionals working in the technology domain such as technical decision makers,

technical architects and developers in the government and private sector service provider agencies interested in incorporating eID authentication services into their applications. An example of technical documentation would be the eID authentication services API specifications.

5. In order to improve the adoption of the EISDF eID services by providers in the government and the private sector, EIDAV could set up the development and testing environment in the form of a publicly available URL (e.g., https://auth.eidav.gov.vn) that could be made accessible over the Internet and be used by the software developers of service provider agencies in the development of related applications.

6. In order to improve the adoption of the EISDF eID services such as eID authentication, EIDAV could provide a reference implementation of an eID authentication client library for packaging and encrypting authentication data block in different programming languages. A mechanism could be put in place to promote the development of other programming language bindings among members of the software programming community for submission to EIDAV. Developers may be able to download these libraries along with EIDAV public key, all digitally signed by EIDAV for use within their application.

7. The GoV could set up awareness campaigns among the service providers in the government and the private sector to leverage the benefits of the EISDF in their business processes.

8. Awareness campaigns, promotions and incentive programs targeted at early users, individual residents and the private sector agencies to improve the adoption of the national identity could be planned and set up. The EISDF eID services could be offered free of charge to service providers in the pilot phase to promote the adoption of the services.

6.5 Pilot Implementation Recommendations

The implementation of the EISDF in Vietnam could be done in two phases: the pilot and the complete rollout. The pilot implementation could be conducted upon the finalization of the National ID numbering format. Some of the pilot phase implementation recommendations are listed below.

1. **Electronic Identity Service Delivery Platform**

a. Formation of EIDAV: The creation of an independent department in the government for eID generation and the EISDF eID services delivery and maintenance.
b. Central Resident Identity Data Store process initialization and periodic update.
    i. Instead of recapturing the PID of residents for the CRIDS, it could be recommended to reuse the PID captured and processed for generation of the unique NIN and NID card.
    ii. There may be a legal provision in the form of a decree for transferring the resident data from the NID system to EIDAV's CRIDS for the implementation of EIDSF eID services.
    iii. The PID to be stored in the CRIDS could include the biometric and demographic data of the resident.
    iv. There could be a periodic transfer of new residents' data from the NID system to EIDAV as and when new residents are enrolled by the ministry until all the residents have been issued a NIN and the NID card.
    v. It is recommended to have a secure operational model for transferring the updates in the CRIDS and the NID resident database such as address change, etc., on an ongoing basis.
c. EIDAV would set up the EIDAV data center following the technical recommendations for the EISDP as discussed previously in this chapter.
d. EIDAV could set up the registration process for ISPAs and ISCAs on their public portal. The national telecom operators in Vietnam have the required capabilities to set up the dedicated secure connectivity to the National Identification Authority of Vietnam (NIDAV) center. The NIDAV could select the Viettel Group and/or the VNPT to take up the role of ISPA in the pilot phase.

2. Electronic Identity Authentication Service
    a. EIDAV, as the MISP, would have the responsibility of designing and implementing the eID authentication service then host it its data center on the EISDP. It could also implement the registration process for eID authentication service on the public portal of EIDAV.
    b. EIDAV could hire the SI vendor to implement the service using a tendering process.
    c. The service providers in the government departments and private sector could register with EIDAV on the public portal for eID authentication service. On approval by EIDAV, the service providers could install the eID authentication service API on their service delivery application using their point-of-delivery device following the

guidelines provided by EIDAV. Then the setting up of the hardware, software, process and network would be performed.

d. EIDAV would to update the IT policies in Vietnam to enable eID authentication service as an acceptable means of identity verification by service providers.
e. In order to promote the adoption of the service, it could be offered free of charge to service providers.
f. EIDAV could set up awareness campaigns for residents and services providers. There could be capacity-building programs in the form of online and classroom trainings targeted at the residents and officials/operators in the government and the private sector. There could be software development training programs targeted at the developer community in the service provider agencies.

3. **Electronic Identity Seeding Service**
    a. EIDAV could make available the offline seeding utility, the Electronic Seeding Platform (eSP), and the registration process on the public portal of EIDAV by delegating the operation to the chosen SI vendor selected using the tendering process.
    b. The government, along with EIDAV, could select one service provider each from the government and the private sector to pilot the implementation of the eID seeding service. Public and private entities that may be considered for the pilot could be the VSS and the VNPT or Viettel, respectively.
    c. The selected service providers could prepare the service enablement database by performing the data digitization and centralization.
    d. The selected service providers could register as ISCAs by following the registration process provided by EIDAV on its public portal.
    e. The ISCA could also register for downloading the seeding utility and for requesting access to the eSP. It could also provide the option to import the service enablement database or provide the web service details at the time of registration.
    f. The ISCA could implement the strategy chosen for seeding by setting up the programs for collecting the data. On completion of the seeding, the ISCA could perform the seeding validation using the eSP, the seeding utility, and export the updated service enablement database to their server in their data center.

4. **Electronic Know-your-customer Service**

a. EIDAV have the responsibility to design and implement the eKYC service and host it in its data center as part of the EISDP. It could also make available the registration process for eKYC service on the public portal of NIDAV.
b. EIDAV could hire the SI vendor, selected under the tendering process, for implementing the eKYC service.
c. The selected service providers could register for the eKYC service on EIDAV public portal. On approval by EIDAV, the service providers could install the eKYC service on their application following EIDAV guidelines. At this point, the setting up of the hardware, software, process and network may be performed.
d. EIDAV would update the IT policies in Vietnam to enable the eKYC response as a valid legal KYC document equivalent to the paper-based version.
e. EIDAV could work with the government departments such as the VSS, the Ministry of Labor, Invalids and Social Affairs (MoLISA), the Ministry of Environment (MoE), the Ministry of Finance (MoF) and private sector organizations such as the BoV, Viettel, etc., to update their KYC norms to include the NIN and the eKYC response as the valid KYC document.
f. In order to promote the adoption of the service, it could be offered free of charge to the service providers.

5. **Mobile Identity Service**
    a. EIDAV would have the responsibility to design and implement the mobile ID service and host it in the EIDAV data center as part of the EISDP.
    b. EIDAV could delegate the implementation and operation of mobile ID services to the national telecom operators such as Viettel and VNPT.
    c. The selected telecom operator could leverage its existing SIM manufacturers to build new mobile ID SIMs following the technical specifications provided.
    d. The telecom operator could set up the necessary infrastructure in its outlets for SIM provisioning to perform the role of mobile ID RA.
    e. The telecom operator could provide training to residents in user registration and activation of their mobile ID and also in using the mobile for eID authentication.
    f. The telecom operator could implement the process of the provisioning of digital certificate by the VGCA. The VGCA could also provision OCSP service for digital certificate validation at the time of identity authentication using the mobile ID service.
    g. The service provider wishing to use the mobile ID as the mechanism for eID authentication would need to update its existing service delivery application to use

the mobile ID service. The telecom operator could extend support to the service provider in installing the mobile ID service into its service delivery application.

h. The service providers could provide online and offline training to their end-customers to use the mobile ID for validating their identity.
i. The mobile operator could set up the necessary technical infrastructure in its data centers as described in the technical recommendations for the mobile ID service.

7.0 Budget Estimates

7.1 Estimation Basis

The budget estimate for the design and implementation of the Electronic Identity Service Delivery Framework (EISDF) includes the budget for the initial pilot project and the subsequent complete rollout of the framework in the country. The high-level budget estimate for the implementation of the vision of the framework is based on the information of the Government of Vietnam (GoV) and the proposed private sector setup. The estimates have been calculated based on the average investment index estimation method. This method leverages the budget estimates of the representative typical projects from a large number of similar projects so as to estimate the typical project investment scale based on which the investments of the project and the planned total budget estimates are calculated. The budget estimates provided here are for guidance only and may not necessarily be used for budgeting purposes. It may, however, keep the GoV and implementation agencies abreast of the possible magnitude of investment required for the design and implementation of such framework. Further due diligence would be required to arrive at the accurate estimates based on the implementation details with knowledge of the current setup and additional capabilities to be added for the implementation of the framework.

7.2 Budget Details

The budget estimates include the design, implementation and operation of the centralized infrastructure for the Electronic Identity Authority of Vietnam (EIDAV), Identity Service Provider Agencies (ISPAs) and Identity Service Consumer Agencies (ISCAs). The budget estimates for the mobile IDs, Registration Authority (RA), and Trusted Service Providers (TSPs) is also provided to implement the optional mobile ID service. The estimates include the cost of the physical infrastructure (construction of new buildings, electricity, water, and furniture) and IT infrastructure (hardware, software, networking equipment). The latter also includes design and development of software applications, and development of the standards and operational processes. In addition to the infrastructures, the cost takes in to consideration the salaries of staff and the capacity-building programs for all the stakeholders in the ecosystem. The operating cost includes the budget for running and maintaining the infrastructure and institutional setup for a period of one year for the pilot, and for five years for the complete rollout in the country.

The project could be implemented in two phases. The first phase could be the pilot phase followed by the complete rollout phase.

7.2.1 Budget Estimates for Pilot Phase without Mobile IDs

The budget estimates for the pilot phase include the setup and implementation of the IT and institutional infrastructures for the centralized EIDAV, one ISPA and two ISCAs. Each ISCA would have one service delivery outlet in the urban district of Hanoi. The ISPA selected for the pilot could be either Viettel or the Vietnam Posts and Telecommunications Group (VNPT), and the ISCA could be Viettel or the VNPT and the Vietnam Social Security (VSS). The RA and TSP could be Viettel or the VNPT. The resident demographic and biometric data to be kept in EIDAV's Centralized Resident Identity Database Store (CRIDS) would be imported from the database of the resident data captured by the Ministry of Public Security (MPS) for their national identity pilot. It is assumed that the resident data captured in this national identity pilot going on currently is at least for one million residents. The breakdown of the capital and operating budget estimates for the pilot phase is detailed in the table below.

Particulars	Capital Budget (K USD)	Operating Budget (K USD)
EIDAV Data Center (A1)	$20,966.00	$3,144.90
EIDAV Disaster Recovery Center (A2)	$16,263.00	$2,439.45
Geographical Data Backup Center (A3)	$610.00	$91.50
MPS Data Migration (A4)	$1,100.00	$165.00
EIDAV IT and Institutional Infrastructure (A=A1+A2+A3+A4)	**$38,939.00**	**$5,840.85**
ISPA Data Center (B1)	$5,554.50	$833.18
ISPA IT and Institutional Infrastructure (B=B1)	**$5,554.50**	**$833.18**
ISCA Data Center (C1)	$2,437.40	$365.61
ISCA Service Delivery Outlets (C2)	$29.18	$4.38
ISCA IT and Institutional Infrastructure (C=C1+C2)	**$2,466.58**	**$369.99**
Awareness, Trainings and Capacity Building (D)	**$100.00**	**$0.00**
National IT Standards and Policies (E)	**$100.00**	**$0.00**
Total Budget = (J = A+B+C+D+E)	**$47,160.08**	**$7,044.02**
Total (Capital + Operating Budget)	**$54,204.10**	

Table 1: Breakdown of Pilot Phase Budget Estimates

As shown in the table above, the total investment for the pilot phase is estimated at **USD 54.2 million**. It includes the capital cost of **USD 47.16 million** and the operating cost of **USD 7.04 million** for the first year.

The breakdown of the pilot phase capital budget estimate is described below.

1. **EIDAV IT and Institutional Infrastructures.** Budget estimate for the design and implementation of the centralized physical, IT and institutional infrastructures is at **USD 38.94 million**. It includes the design and implementation of the centralized EIDAV data center, the disaster recovery center and the geographical data backup center. The budget estimate for each data center includes the setup of the physical building, interiors, electricity, water and furniture; setup of IT infrastructure such as hardware, software and networking equipment; and design, development and deployment of custom and packaged applications. It also includes the cost for setting up the IT infrastructure between the NID system and the EIDAV data center for migration of the resident data to the EIDAV data center from the NID system.

2. **ISPA IT and Institutional Infrastructures.** Budget estimates for the design and implementation of the ISPA data center at Vittel/VNPT is **USD 5.56 million**. It includes the design and implementation of the ISPA data center. The budget estimate for setting up the ISPA data center includes the design, architecture and the implementation of the IT infrastructure (hardware, software and network), procurement of the IT infrastructure following the design and EIDAV's IT specifications.

   ISCA IT and Institutional Infrastructures. Budget estimates for the design and implementation of two ISCA data center and one service delivery outlet for each ISCA in Viettel/VNPT and the VSS is **USD 2.47 million**. It includes the design and implementation of the ISCA data centers and the service delivery outlets for each ISCA. The budget estimates for setting up the data center and the service delivery outlets include the design, architecture and the implementation of the IT infrastructure following the design and EIDAV IT specifications. It also include the design, development and deployment of custom point of sales (PoS) applications, customization of the existing PoS applications to integrate with EIDAV's identity services, the seeding of the NIN in the database of the existing line of business (LoB) and PoS applications.
3. **Awareness, Trainings and Capacity Building.** The budget estimates include the capacity-building trainings for all the stakeholders of the ecosystem, technical and process- related

trainings for the stakeholders, and awareness programs and online and in-person training for the residents and users of the mobile ID and other identity services of the EISDF. The budget estimate for the awareness, trainings and capacity building is at **USD 100,000.**

4. **National IT Standards and Policies.** The budget estimates for setting up the government and private sector committees for developing and ratifying the government policies and IT standards is at **USD 100,000**.

The breakdown of the pilot phase operating budget estimate is described below.

1. **EIDAV IT and Institutional Infrastructures.** Budget estimates for the operation of centralized physical, IT and institutional infrastructures for one year is **USD 5.84 million**. It includes the operation and maintenance of physical infrastructure such as monthly electricity and water, repair and cleanliness of the premises, and staff salaries. It also includes the maintenance and upgrade of hardware, software and networking equipment, salaries of IT staff in the data center, disaster recovery center, and data backup center. In addition, it includes the continuous migration and management of the data from the NID system to the EIDAV data center.

2. **ISPA IT and Institutional Infrastructures.** Budget estimates for the operation of the ISPA data centers' physical, IT and institutional infrastructures for one year is at **USD 833,180**. It includes the operation and maintenance of physical infrastructure such as monthly electricity and water, repair and cleanliness of the premises, and staff salaries. It also includes the maintenance and upgrade of hardware, software and networking equipment and salaries of IT staff in the data center.

   ISCA IT and Institutional Infrastructures. Budget estimate for the operation of the data center's and service delivery outlets' physical, IT and institutional infrastructures for one year is at **USD 369,990**. It includes the operation and maintenance of physical infrastructure such as monthly electricity and water, repair and cleanliness of the premises, and staff salaries. It also includes the maintenance and upgrade of hardware, software and networking equipment, salaries of IT staff in the data center and service delivery staff in the outlets.

7.2.2 Budget Estimates for Implementation of Optional Mobile IDs in the Pilot Phase

The budget estimates for the implementation of optional mobile ID service in the pilot phase is described below. The budget estimates are based on the roll out 10,000 mobile IDs, one RA and one TSP in the pilot phase.

The breakdown of the capital and operating budget estimates for the implementation of optional mobile ID in the pilot phase is detailed in the table below.

Particulars	Capital Budget (K USD)	Operating Budget (K USD)
RA Data Center (D1)	$2,218.70	$332.81
RA Service Delivery Outlets (D2)	$14.59	$2.19
SIM Provision (D3)	$50.00	$0.00
RA IT and Institutional Infrastructure (D=D1+D2+D3)	**$2,283.29**	**$335.00**
TSP Data Center (E1)	$1,903.70	$285.56
TSP IT and Institutional Infrastructure (E=E1)	**$1,903.70**	**$285.56**
Total Budget = (K = D+E)	**$4,186.99**	**$620.56**
Total (Capital + Operating Budget)	**$4,807.55**	

Table 2: Breakdown of Pilot Phase Budget Estimates for Mobile ID Implementation

As shown in the table above, the total investment for the implementation of optional mobile ID in the pilot phase is estimated at **USD 4.81 million**. It includes the capital cost of **USD 4.19 million** and the operating cost of **USD 620,000** for the first year.

The breakdown of the capital budget estimates for the implementation of optional mobile ID in the pilot phase capital is described below.

1. **RA IT and Institutional Infrastructures.** Budget estimates for the design and implementation of the RA data center and one service delivery outlet at Viettel/VNPT is at **USD 2.28 million**. It includes the design and implementation of the RA data center and the service delivery outlet. The budget estimates for setting up the data center and the service delivery outlet include the design, architecture and the implementation of the IT infrastructure following the design and EIDAV IT specifications. It also includes the design, development and deployment of the custom POS applications, customization of the existing POS applications for the provisioning of the mobile ID SIMs (assuming the use of SIM cards), activation of digital certificates or biometrics, and seeding of the NIN in the resident database of the service provider.

2. **TSP IT and Institutional infrastructures.** Budget estimates for the design and implementation of the TSP data center at Viettel/VNPT is at **USD 1.90 million**. The budget estimates for setting up the data center include the design, architecture and the implementation of the IT infrastructure following the design and EIDAV IT specifications.

The breakdown of the operating budget estimate for the implementation of optional mobile ID in the pilot phase is described below.

1. **RA IT and Institutional Infrastructure.** Budget estimate for the operation of the data center and service delivery outlets' physical, IT and institutional infrastructures for one year is at **USD 334,990**. It includes the operation and maintenance of physical infrastructure such as monthly electricity and water, repair and cleanliness of the premises, and staff salaries. It also includes the maintenance and upgrade of hardware, software and networking equipment, salaries of IT staff in the data center and service delivery staff in the outlets.

2. **TSP IT and Institutional Infrastructure.** Budget estimates for the operation of data centers' physical, IT and institutional infrastructures for one year is at **USD 285,560**. It includes the operation and maintenance of physical infrastructure such as monthly electricity and water, repair and cleanliness of the premises, and staff salaries. It also includes the maintenance and upgrade of hardware, software and networking equipment and salaries of IT staff in the data center.

7.2.3 Budget Estimates for Complete Rollout Phase without Mobile IDs

Particulars	Capital Budget (K USD)	Operating Budget (K USD)	Units	Total Capital Budget (M USD)	Total Operating Budget (M USD)
EIDAV Data Center (A1)	$9,160.00	$22,594.50	1	$9.16	$22.59
EIDAV Disaster Recovery Center (A2)	$9,160.00	$22,594.50	1	$9.16	$22.59
Geographical Data Backup Center (A3)	$830.00	$457.50	1	$0.83	$0.46
MPS Data Migration (A4)	$500.00	$375.00	1	$0.50	$0.38
EIDAV IT and Institutional Infrastructure (A = A1+A2+A3+A4)				**$19.65**	**$46.02**
ISPA Data Center (B1)	$5,554.50	$4,167.08	2	$11.11	$8.33
ISPA IT and Institutional Infrastructure (B = B1)				**$11.11**	**$8.33**
ISCA Data Center (C1)	$1,218.70	$914.03	20	$24.37	$18.28
ISCA Service Delivery Outlets (C2)	$14.59	$10.94	2,480	$36.18	$27.14
ISCA IT and Institutional Infrastructure (C = C1+C2)				**$60.56**	**$45.42**
Awareness, Trainings and Capacity Building (D)	**$1,000.00**		**1**	**$1.00**	**$0.00**
National IT Standards and Policies (E)	**$200.00**		**1**	**$0.20**	**$0.00**
Total Budget = (J = A+B+C+D+E)				**$92.52**	**$99.77**
Total (Capital + Operating Budget)	**$192.29**				

Table 3: Breakdown of Rollout Phase Budget Estimates

As shown in the table above, the total investment for the complete rollout phase is estimated at **USD 192.29 million**. It includes the total capital cost of **USD 92.52 million** and the total operating cost of **99.77 million** for five years.

The budget estimates for the complete rollout include the addition of the capacity to the IT and institutional infrastructures setup during the pilot phase of the centralized EIDAV. It also includes the setup and implementation of the IT and institutional infrastructures for one more ISPA apart from the one set up during the pilot phase. About 20 additional ISCAs would be set up with 124 outlets (one per province and one per 10 districts) for each ISCA for the service delivery to the residents. Ten additional RAs would be set up with 100 outlets for each RA, and two additional TSPs. In addition, it includes the budget estimates for capacity building efforts and setup of the EISDF standards and government policies that may be required for the implementation of the framework and the eID system.

The breakdown of the capital budget estimates for the complete rollout phase is detailed below:

1. **EIDAV IT and Institutional Infrastructures.** Budget estimates for extending the capacity of the centralized physical, IT and institutional infrastructures for the complete rollout of the

framework is at **USD 19.65 million**. It includes enhancing the capacity of the centralized EIDAV data center, the disaster recovery center, and the geographical data backup center. The budget estimates for each data center include additional electricity capacity, water and furniture; additional IT infrastructure such as hardware, software and networking equipment to meet the requirements for the complete rollout. It also includes the cost of design, development and deployment of custom and packaged applications and enhancement and updating of the existing applications. In addition, it includes the cost of the enhancement of the IT infrastructure between the NID system and the EIDAV data center, for migration of the resident data to the EIDAV data center.

2. **ISPA IT and Institutional Infrastructures.** Budget estimates for the design and implementation of two additional ISPA data center at Vittel/VNPT or of other provider agencies to cater the needs of all the ISCAs is at **USD 11.11 million**. It includes the design and implementation of the ISPA data center. The budget estimates for setting up the ISPA data center include the design, architecture and the implementation of the IT infrastructure (hardware, software and network), procurement of the IT infrastructure following the design and EIDAV IT specifications.

   ISCA IT and Institutional Infrastructures. Budget estimates for the design and the implementation of 20 ISCAs data center and 124 service delivery outlets (one per province and one for 10 districts each) for each ISCA is at **USD 60.56 million**. It includes the design and implementation of the ISCA data centers and the service delivery outlets for each ISCA. The budget estimates for setting up the data centers and the service delivery outlets include the design, architecture and the implementation of the IT infrastructure following the design and EIDAV IT specifications. It also includes the design, development and deployment of the custom PoS applications, customization of the existing PoS applications to integrate with EIDAV's eID services, seeding of the NIN in the database of the existing LoB and PoS applications.
3. **Awareness, Trainings and Capacity Building.** Budget estimates include the capacity building trainings for all stakeholders of the ecosystem, technical and process-related trainings for the stakeholders, and awareness programs for the residents and users of the mobile ID and other eID services of the EISDF. The budget estimates for the awareness, trainings and capacity building is at **USD 1 million**, in addition to the pilot budget for capacity building.

4. **National IT Standards and Policies.** Budget estimates for setting up the government and private sector committees for developing and ratifying the government policies and IT standards is at **USD 0.2 million**.

The breakdown of the operating budget estimates for the complete rollout phase for five years of operation is detailed in the table below.

1. **EIDAV IT and Institutional Infrastructures.** Budget estimates for the operation of the national-level centralized physical, IT and institutional infrastructures for five years is at **USD 46.02 million**. It includes the operation and maintenance of physical infrastructure such as monthly electricity and water, repair and cleanliness of the premises, and staff salaries. It also includes the maintenance and upgrade of hardware, software and networking equipment, salaries of IT staff in data center, the disaster recovery center, and the data backup center. In addition it includes the continuous data migration and management of information from the NID system to the EIDAV data center.

2. **ISPA IT and Institutional Infrastructure.** Budget estimates for the operation of centralized data centers' physical, IT and institutional infrastructures for five years for two ISPAs is at **USD 8.33 million**. It includes the operation and maintenance of physical infrastructure such as monthly electricity and water, repair and cleanliness of the premises, and staff salaries. It also includes the maintenance and upgrade of hardware, software and networking equipment and salaries of IT staff in data center.

3. **ISCA IT and Institutional Infrastructures.** Budget estimate for the operation of the data centers' and service delivery outlets' physical, IT and institutional infrastructures for five years for 20 ISCAs and their 124 service delivery outlets is at **USD 45.42 million**. It includes the operation and maintenance of physical infrastructure such as monthly electricity and water, repair and cleanliness of the premises, and staff salaries. It also includes the maintenance and upgrade of hardware, software and networking equipment, salaries of IT staff in the data center and the service delivery staff in the outlets.

7.2.4 Budget Estimates for Optional Mobile ID in the Complete Rollout Phase

The budget estimates for the implementation of optional mobile ID service as part of the complete roll out phase is described below. The budget estimates are based on the roll out of 90 million mobile IDs, two RA, 200 RA service delivery outlets and one TSP in the rollout phase.

The breakdown of the capital and operating budget estimates for the implementation of optional mobile ID in the rollout phase is detailed in the table below.

Particulars	Capital Budget (K USD)	Operating Budget (K USD)	Units	Total Capital Budget (M USD)	Total Operating Budget (M USD)
RA Data Center (D1)	$2,218.70	$1,664.03	2	$4.44	$3.33
RA Service Delivery Outlets (D2)	$14.59	$10.94	200	$2.92	$2.19
SIM Provision (D3)	$44,950.00	$0.00	1	$44.95	$0.00
RA IT and Institutional Infrastructure (D = D1+D2+D3)				**$52.31**	**$5.52**
TSP Data Center (E1)	$1,903.70	$1,427.78	1	$1.90	$1.43
TSP IT and Institutional Infrastructure (E=E1)				**$1.90**	**$1.43**
Total Budget = (K = D+E)				**$54.21**	**$6.94**
Total (Capital + Operating Budget)	**$61.15**				

Table 4: Breakdown of Rollout Phase Budget Estimates for Mobile ID Implementation

As shown in the table above, the total investment for the implementation of optional mobile ID in the complete rollout phase is estimated at USD 61.15 million. It includes the capital cost of USD 54.21 million and the operating cost of USD 6.94 million for the first five years.

The breakdown of the rollout phase capital budget estimate for the implementation of optional mobile ID is described below.

1. **RA IT and Institutional Infrastructures.** Budget estimates for the design and implementation of two new RA data centers and 100 service delivery outlet for each RA at Viettel/VNPT, or other mobile operators' data center and existing outlet is at **USD 52.31 million**. It includes the design and implementation of the RA data center and the service delivery outlets. The budget estimates for setting up the data center and the service delivery outlet include the design, architecture and the implementation of the IT infrastructure following the design and EIDAV IT specifications. It also includes the design, development and deployment of the custom PoS applications, customization of existing PoS applications for the provisioning of the mobile ID SIM cards, activation of digital certificates or biometrics, and seeding of the NIN in the resident database of the service provider. In addition, it includes the cost of 90 million mobile ID-based SIM provisioning in addition to the 100,000 envisioned for the pilot phase.

2. **TSP IT and Institutional Infrastructure.** Budget estimates for the design and implementation of one additional TSP data centers at Viettel/VNPT, or of other mobile operator is ate **USD 1.90 million**. The budget estimates for setting up the data center could include the design, architecture and implementation of the IT infrastructure following the design and EIDAV IT specifications.

The breakdown of the rollout phase operating budget estimate for the implementation of optional mobile ID is described below.

1. **RA IT and Institutional Infrastructures.** Budget estimates for the operation of the data centers' and service delivery outlets' physical, IT and institutional infrastructures for five years for two RAs and their 200 service delivery outlets is at **USD 5.52 million**. It includes the operation and maintenance of physical infrastructure such as monthly electricity and water, repair and cleanliness of the premises, and salaries of the staff. It also includes the maintenance and upgrade of hardware, software and networking equipment, salaries of IT staff in the data center and the service delivery staff in the outlets.

2. **TSP IT and Institutional Infrastructures.** Budget estimate for the operation of the data centers' physical, IT and institutional infrastructures for five years for one TSP is at **USD 1.43 million**. It includes the operation and maintenance of physical infrastructures such as monthly electricity and water, repair and cleanliness of the premises, and staff salaries. It also includes the maintenance and upgrade of hardware, software and networking equipment, and salaries of IT staff in the data center.

7.2.5 Total Budget Estimate without Mobile ID

	Capital Budget (M USD)	Operting Budget (M USD)	Total Budget (M USD)
Pilot Phase with 1 year of Operation (A)	$ 47.16	$ 7.04	**$ 54.20**
Complete Rollout Phase with 5 years of Operation (B)	$ 92.52	$ 99.77	**$192.29**
Total Budget (C=A+B)	**$139.68**	**$ 106.81**	**$246.49**

Table 5: Total Budget for EISDF Implementation

As shown in the table above, the total budget estimated for the pilot phase with one year of operation is at **USD 54.20 million**, and the total budget estimated for the complete rollout phase with five years of operation is at **USD 192.29 million**. Overall budget estimated for the implementation of the EISDF in Vietnam in two phases (pilot and rollout) is at **USD 246.49 million**.

8.0 Annexes

Annex 1

1. Types of Identity Tokens

An individual identity may be created and authenticated by providing three types of identity tokens:

What the user knows. Examples are username, password, PIN, and secret questions and answers. They may be used for electronic authentication only. They are never used for physical authentication as, once they are known to another person, they lose their value for identity verification.

What the user has. Examples are paper identity card, health insurance card, access card, ATM card, and mobile phone. For this type, authentication may be done electronically and/or manually on the form of the token. For instance, paper identity card and health insurance card may only be manually authenticated, while ATM card and access card may be electronically authenticated. These are currently the most common forms of identity token in Vietnam.

Who the user is. Examples are fingerprints, iris patterns, facial photo, body marks, and voice. For this type, authentication can be both electronic and manual. However, manual authentication is done mostly on the facial photo that is printed on an identity card.

II. Service Providers' Authentication Type Selection Criteria

The authentication type selected by the service provider may be based on the following criteria:

1. Level and type of risk, and impact on the resident in case of inaccurate authentication at the time of service delivery. Type of risk and impact on the resident include inconvenience and distress, financial loss, and breach of security and privacy.

2. Level and type of risk, and impact on the service provider in case of inaccurate authentication on the business transaction. Type of risk and impact on the service provider include financial loss, business squeeze, breath of security and privacy, and threat to national security.

3. Cost and logistics of implementing a certain type of authentication. For instance, biometrics will require investment in devices and resident presence, while OTP requires residents to have a mobile phone.

4. Volume of authentications based on number of beneficiaries and frequency of authentication required. For instance, stronger assurance level may be appropriate for KYC purpose of one-time account opening or service issuance compared to a lower assurance requirement for frequent transactions such as delivery of services.

In cases where there is higher risk of identity misuse, multi-factor authentication may be considered to eliminate occurrence of such instances.

III. Supports Self-service and Operator-assisted Service Delivery Scenarios

Scenario 1: Operator-assisted transaction using the PoS terminal at the designated service delivery location

1. In this scenario, the resident could go to the designated service delivery location (e.g., public or private) to request a service. The resident presents the NIN and the required demographic, biometric and digital personal identity data for reading by the terminal device of the service provider. In the case of digital certificate or biometrics, the terminal device would have the capability to read it from the smart card with the use of a card reader or from the mobile ID.
2. The service operator feeds the resident's identity data to the eID authentication-enabled application software that is installed on the authorized terminal device. In the case of mobile ID, the residents would authenticate themselves by providing the PIN on their mobile phone.
3. The software application packages the input parameters, encrypts, and sends them to the centralized EISDF eID authentication service over a mobile or broadband network.
4. EISDF eID authentication service returns with a "yes/no" based on the match of the input parameters.
5. Based on the response from the eID authentication service, service provider conducts the transaction accordingly.

Scenario 2: Self-service transaction using mobile, kiosk, or Internet-connected device

1. In this scenario, the resident may conduct a self-service transaction using the eID authentication service on the mobile or on an Internet-enabled device such as tablet, PC, kiosk, laptop, etc.
2. The resident inputs the transaction data on the mobile/Internet-connected device to access the mobile/Internet-enabled service delivery application of the service provider.

3. The resident provides the NIN, the necessary demographic data or digital certificate/biometrics along with OTP in addition to service provider-specific attributes (may be domain specific account number, password, PIN, etc.). In the case of digital certificate, the resident may also use the mobile ID supported by EISDF. Biometric data such as fingerprints are also possible although not yet common on the mobile or PC. However, the EISDF could provide the standard specification for the biometric device (UID or otherwise) and circulate the list of approved vendors of such device.
4. Steps 3, 4, and 5 are the same as in scenario 1 above.

Scenario 3: Testing environment for Service providers and software developers

1. Service providers may use the development and testing environment provided by the EISDF to build their software application that could use the eID authentication service.
2. The EISDF could provide a public URL (e.g., https://auth.EIDAV.gov.vn) where software developers may go to access the APIs for eID authentication services.
3. This would help in checking the installation of the eID software on the service provider devices and servers.

IV. Electronic Identity Seeding Utilities and Platform

Seeding Utility

The EISDF could provide the seeding utility to service providers to perform common activities including data extraction, consolidation, normalization and matching. The service provider would need to register in the system and sign the agreement to use the utility for only the intended purposes. Some of the features of this tool may be:

1. **Source Data Extraction.** The utility would be able to connect to different data sources to pull the relevant Personal Identity Data (PID) from the reference database. It would also pull the data from the relevant data tables in the service delivery database of the service provider.

2. **Matching and Seeding.** The utility would provide the capability in which one or more PID equivalent fields (name, date of birth, age, gender) from resident records in the service delivery database may be matched with equivalent fields in PID records from the reference database. The mapping thus created may be exported to Excel for further review and approval by a competent authority appointed by the service provider. The utilities'

functionality of match and seed would be limited only to the creation of the mapping and their export. It is expected that based on mapped data, service providers would create custom SQL scripts to update the service delivery database.

3. **Demographic Authentication.** In order to verify whether seeding has been done accurately, it is essential that the resident records in the service delivery database are authenticated demographically. The objective of demographic authentication is to check whether the NIN and PID fields are mapped correctly and are in line with the data in the CRIDS. Post demographic authentication, the authentication status may be marked as "pass/fail". In the case of "fail", error code may indicate and explain the reason for authentication failure that may be used for investigation purposes. The prerequisite to demographic authentication is service provider enrollment in the system to call the eID authentication service for demographic authentication.

Centralized eID Seeding Platform

The EISDF could provide the centralized eID Seeding Platform (eSP) as part of the Electronic Identity Service Delivery Platform (EISDP) which would enable converging various seeding channels into one central staging area. The eSP would be accessible to operators in various service delivery organizations for the verification of seeding and inclusion into their service delivery databases. It would support efficient and seamless seeding of the NIN into the service provider databases, thereby enabling faster adoption of eID-enabled service delivery in Vietnam.

The seeding requests would go to the eSP from various input channels. A seeding request is a submission of the NIN and corresponding beneficiary/subscriber/customer identifier (ID) to be linked to the service delivery system.

The eSP may be published on the public portal of EIDAV and may be accessed by the resident directly to submit the seeding request. Authorized users from service provider organizations may have login-based access to submit seeding requests ("seeders") on behalf of residents. Authorized users from service provider organizations may have login-based access to validate seeding requests ("verifiers"). Verifiers may process seeding requests by comparing the PID of the resident from the CRIDS (made available to eSP through web services) with the PID of the resident from the scheme beneficiary database (made available on eSP either through a web service or setup on the eSP database itself by the scheme administrator).

V. ESignature

eSignatures are divided into two separate categories — (1) digital signatures and (2) electronic signatures, which is distinguished primarily by the presence or absence of Public-Key Cryptography (PKC).

Digital Signatures

The term digital signature refers to the encryption and decryption technology used as the foundation for a variety of security implementations. Based on public and private key cryptography, digital signatures are used in secure messaging, public key infrastructure, virtual private networks, and electronic signatures.

Contrary to what the name might suggest, a digital signature alone is not a type of electronic signature. Rather, digital signature encryption could be used by electronic signature applications to secure the data and verify the authenticity of a signed record. Further, a digital signature alone does not capture a person's intent to sign a document and be legally bound to an agreement or contract.

The digital signature for which the most full-featured and, arguably, the most secure type of e-signature relies on Public-key cryptography to authenticate identity. Public-key cryptography involves a pair of mathematically related keys:

- The "private key," known only by the signer, can be used to sign a message that only the corresponding "public key" holder can verify.

- The public and private keys are very large, randomly generated prime numbers, and it is computationally infeasible to distinguish one from the other. By issuing and managing public and private keys, public-key infrastructure (PKI) enables very strong authentication, integrity and nonrepudiation.

- Because the crypto functions bind mathematically with a hash (a unique representation) of the document, any change negates the signature (the hash of the document being the document encoded with a one-way hash algorithm).

Further, because a Certification Authority vouches for the certificate holder, PKI can provide a higher level of assurance of signer identity and authentication. The primary risk related to a digital signature is the compromise of the private key.

In a PKC-based signature, the encrypted hash could match the message content; otherwise, the digital signature is void. Thus, a digital signature cannot be copied from one message and applied to another because it is bound to specific message content — any changes to the message could invalidate the signature. Because the signature is based on a protected private key known only to the user, the safety of the key is of critical importance. Figure 1 [10]is a graphic representation of the digital signature process. Table 1 provides an outline of the signing and encryption process.

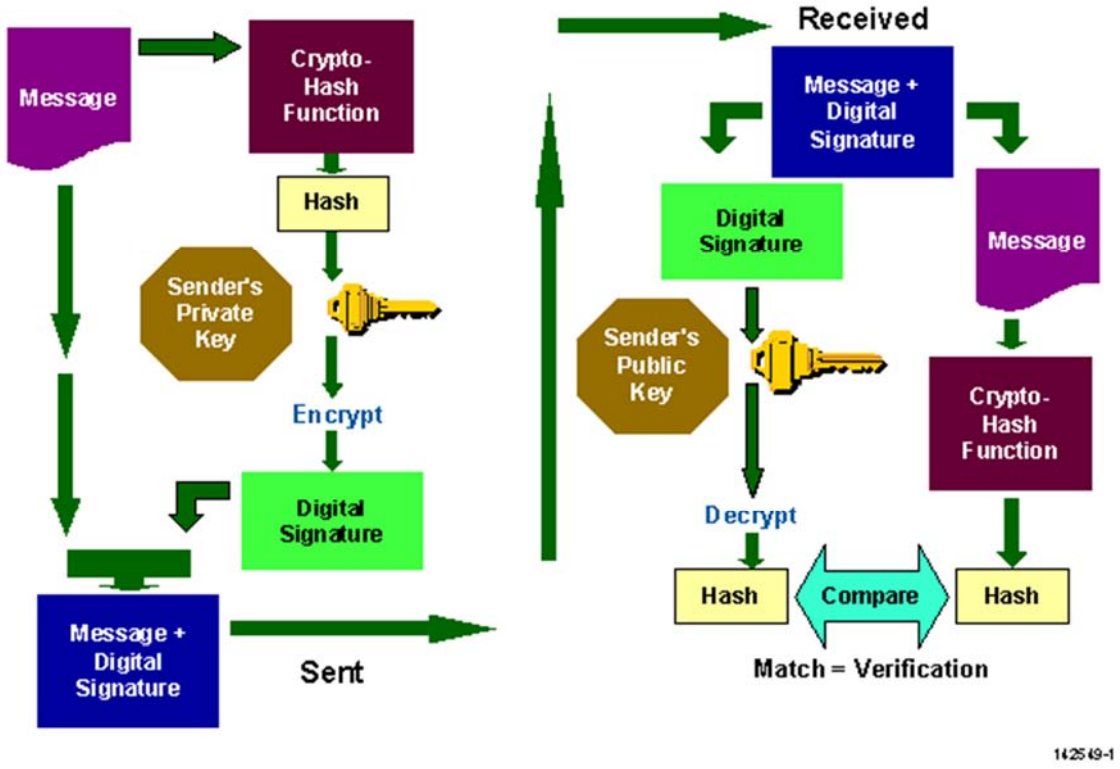


Figure 1. The digital signature process

Table 1. Signing and Encrypting a Message Using PKC	
Possession of Public and Private Keys	• At the beginning of or during the transaction, the participants could acquire one another's public keys (similar to looking up a number in a telephone book). Public keys are often stored and retrieved from directories or are included with a signed e-mail message. • At no time does the private key of either party leave the owner's possession.

[10] Source from Gartner

Sender Uses Hash Function to Create Hash or Message Digest	• A hash function is a one-way algorithm that transforms a string of characters into a shorter fixed-length value. The result of this calculation is commonly called the "hash" or "hash value."
Message Signed With Digital Signature	• The sender's private key is then used to encrypt the hash to produce the digital signature, which is appended to the message.
Message Sent	• This digitally signed message is sent "in the clear" to the recipient. Once the message has been sent, any further change to the message contents will result in the digital signature being corrupted (because any change in the message will result in hash values no longer matching).
Message Verified Through Matching	• The recipient generates the hash from the message itself using the same one-way hash function. • The encrypted hash that came with the message is decrypted using the sender's public key, and the results are compared. • If the two hashes match, the message can be treated as genuine and authentic. Nonmatching hashes can indicate impersonation, message alteration or an error in transmission. In any case, the message is considered corrupted or a forgery.
Message Encrypted (Optional)	• To ensure the confidentiality and privacy of the message content, the entire message can be encrypted using the recipient's public key.
Message Decrypted (If Applicable)	• If the sender has encrypted the entire message, the message is returned to clear text through decryption using the recipient's private key.
Time Stamping	• The digital signature can be "time stamped" to allow the transaction to be traced in the future or to verify that a transaction was conducted in a timely fashion.

An electronic signature employs digital technology to bind a signature to an electronic document. In its most-secure solutions offered by service providers, the signature is bound to the document in such a way that neither the document nor the signature can be altered without invalidating the document.

An electronic signature is, like its paper equivalent, a legal concept. According to the U.S Electronic Signatures in Global and National Commerce Act, an eSignature is an “electronic sound, symbol, or process attached to, or associated with, a contract or other record and adopted by a person with the intent to sign a record.” A digital signature, on the other hand, refers to the encryption / decryption technology on which an electronic signature solution is built. A digital signature alone is not a type of electronic signature. Rather, digital signature encryption secures the data associated with a signed document and helps verify the authenticity of a signed record. Used alone, it cannot capture a person’s intent to sign a document or be legally bound to an agreement or contract. Table 2 below details the basics of an eSignature.

Table 2. Basic Elements of an eSignature

Electronic Document An electronic document, transaction or record requiring a legal signature	
Intent to Comply The intent to agree to/comply with the content of the document or nature of the transaction	The very process of creating the e-signature is what is known legally as an "affirmative act," making clear to the signer that the signature is a legal agreement.
Mark or Representation A mark or representation unique to the signer that becomes an integral part of the document, transaction or record	This signature could clearly identify what is being signed and be attached in such a way that the signer is associated with the document. The signature could be generated from information in the secure, sole possession of the signer or in a way that is uniquely bound to the individual.

Verification Verification that the mark or representation is indeed that of the signer for nonrepudiation and to avoid fraud, forgery and impersonation	In the most-secure e-signature applications, verification is accomplished by matching the eSignature against a known piece of authentic information.

Types of eSignature — Biometric

In a biometrics-based signature, the characteristics of a fingerprint, the iris of an eye, a sound or the dynamics of a handwritten signature are encoded digitally and then stored and transmitted by computer to verify identity. These unique human characteristics can be linked to a specific person's biological information, separating the person scientifically from anyone else. The key steps in ensuring identity are similar to those for paper signatures. With biometric data, a 100 percent match is not probable. The government or the private sector could determine the acceptable parameters. If the parameters are too generous, false matches can allow access by unauthorized persons, and if the parameters are too strict, false negatives will deny legitimate users. Table 3 shows the authentication process used to verify a fingerprint signature.

Table 3. Biometric Authentication for a Fingerprint Signature	
Create Reference Template	Person's fingerprint is scanned to create reference template to be stored in a central database or token, along with other personal information.
Store in Database	Reference template is stored in central database or token, along with other personal information.
Authenticate Request	To authenticate, person places finger on reader. Reader sends digitized fingerprint (sample) to central database.
Authentication Through Matching	Sample is compared with reference template. If it matches — within a certain tolerance threshold — the person's identity is authenticated.

Signature pads or tablets are the end-user interface for some types of signature products. These portable devices have screens (similar to those on handheld computers) on which the user physically signs with a stylus or pen. While standard imaging technology permits an image such

as a pen-and-ink signature or document to be scanned and the results stored, signature pads permit the signature to be captured in a way that permits analysis of additional characteristics, such as handwriting speed and stylus pressure. For the user, these devices have the advantage of being similar to a pen-and-ink signature, which improves the acceptance of signing within the workflow and shows strong intent. The resulting signatures are verified when the stored digitized image is compared for verification.

Types of eSignature — Neither Digital nor Biometric

Most signatures in the broad electronic signature category or do not exclusively rely on cryptographic methods. In jurisdictions such as the U.S. and Canada, electronic signature law allows a wide variety of electronic signature types.

For example, if a government body or a private sector firm issues a customer an ID and password that are to be used in an electronic transaction, and the resulting records of that transaction could be signed and stored, then the affirmative act of completing the transaction using the issued ID and password can be deemed sufficient verification of the customer's identity. When this type of e-signature is used, it is highly recommended that some notice is displayed to the user indicating that by clicking on an "Agree," "Save" or "Sign" prompt, the user is acknowledging the transaction.

Additionally, the signer can be authenticated by requesting that he or she provide some information based on knowledge that the signer and the recipient share. For example, the U.S. Internal Revenue Service has successfully used a combination of a tax filer's self-selected PIN and other data elements to verify the filer's identity.

This type of signature does not guarantee that tampering with the record, will not go undetected. However, if strong user ID issuance procedures are followed, and administrative controls on the records database and archival storage procedures are maintained, the government body or the private sector firm may deem such an approach as "good enough."

Assessment on signatures

For many applications, the implementation of simple electronic signatures will be adequate. For example, a user ID and password logon could be required to access a document that is classified as non-confidential. The use of digital signatures based on PKC, while offering more attributes, may not always be needed. In fact, many organizations choose electronic signatures not for security but to reduce the paperwork and time that could be required for a conventional paper transaction.

With PKI, it's virtually impossible for a person to forge a signature because of the public/private-key relationship. Although the public key is distributed freely to anyone with whom the public-

key owner wishes to communicate securely, successful fraud could also require access to the private key. Because the private key cannot be derived from the public key, gaining access to the private key could require social engineering (tricking someone who knows the key into revealing it) or hacking (such as gaining access to the workstation that holds the private key) by unauthorized persons inside or outside the company.

PKI-based digital signature techniques do cost more than simpler electronic signature methods. The government's and resident's needs, not technology, could drive the choice as to which method is "best" for a given transaction.

VI. Client Utility for ESignature

The resident starts the client utility on his/her computer and selects the document to be signed in the application. Using the GoV-issued National Identity Data (NID) card in the ID card reader attached to the computer, the resident signs the document selected. The application reads the digital signing certificate from the ID card and creates a eSignature using the private key by providing the PIN. After the eSignature is created, the validity of the signer's certificate is obtained in the format of Online Certificate Status Protocol (OCSP) response and stored within the signed document. The EISDF may provide the OCSP service to validate the eSignature. The client application calls the OCSP web service hosted in the EISDP by providing the authentication certificate of the resident, and the hash of the eSignature. The hash of the eSignature is received back within the OCSP response. The OCSP service acts as the digital eNotary confirming signatures created locally with a smart card.

The EISDF may also provide the option to sign the document using the Internet browser on their computer by connecting to the EISDF public portal. Its functions are similar to the client program and may be used to generate and verify the eSignature. In addition, it may be used to sign the document by a number of people. It allows designating the people whose signatures are needed on the document and they can all sign it on the same portal. Every user has a directory of his/her documents which no one else sees, but where anyone can send documents to be signed by the user.

The signed document includes within the container: the original documents, the certificate used for signing, signing time, place of signature, signer role, and certificate validity information, namely, OCSP response and OCSP responder certificate. There is no need for any further external information to verify the signature validity.

The service providers can include the functionality of the eSignature into their service delivery applications using the base and intermediary libraries provided by the framework.

The framework enables long time validity of the eSignature by maintaining the log of the OCSP responses and changes in the certificate validity.

Annex 2: Demographic Data Matching Strategy and Rules

I. Name Matching Rules

Name Matching. For the name of the resident, there could be a support for "exact" and "partial" matching strategies. When using "exact" matching strategy, the name is compared for an exact match with the name stored in the CRIDS. Though comparison is case insensitive, all the words of the name should be specified in the exact same order as provided by the resident. When using "partial" matching strategy, the name is compared with that in the CRIDS based on the following rules:

1. Words from the name can appear in any order in the "name" attribute. For example, if the name is stored as "Pham Dang Nguyen", then any of the inputs – "Nguyen Pham Dang", "Pham Nguyen Dang", "Dang Pham Nguyen" or any other combinations – may result in a successful match.
2. Usage of specific titles may be allowed in the "name" attribute. These are ignored for matching purposes. Supported titles are "Mr.", "Mrs.", "Ms.", and "Dr.". No other titles are currently supported. For example, if the name is stored as "Pham Nguyen", then any of the inputs – "Dr. Pham Nguyen", "Ms. Pham Nguyen" or "Mrs. Pham Nguyen" – may result in a successful match.
3. The following special characters, if present in the "name" attribute, are ignored during matching:
    a. Period (.)
    b. Comma (,)
    c. Hyphen (-)
    d. Asterisk (*)
    e. Open and close parentheses [( )]
    f. Open and close brackets ([ ])
    g. Apostrophe (`)
    h. Single quote (')
    i. Double quote (")
    j. Forward slash (/)
    k. Backward slash (\)
    l. Hash (#)
    m. Leading, trailing, and two or more contiguous spaces are removed before matching. For example, if a resident's name is stored as "Pham Nguyen", then "Nguyen, Pham" may result in a successful match.

n. Input may not contain any additional words or initials that are not present in the database. This may result in an unsuccessful match and authentication failure. For example, if the name is stored as “Pham Nguyen”, then, “Pham Dang Nguyen” or “Pham Dang” or “Pham D Nguyen” may result in unsuccessful matches as the words “Dang” and “D” are not present in the CRIDS database.

o. When the threshold value for the partial match is other than 100 percent, then inputs can have some words omitted, or initials can be used in place of the full word. The match is considered successful as long as the input contains a minimum number of matching full words as determined by the value of threshold value for the partial match. For example, if the name is stored as “Pham Dang Nguyen”, and the threshold value is specified as 60 percent. It means that 60 percent of total words should match. In the case of “Pham Dang Nguyen”, 60 percent of three words is 1.8 that is rounded up to two.

   Thus, any of the following inputs may result in a successful match:

   i. “Pham Nguyen” matches because it has the minimum two full words
   ii. “Nguyen, Pham Dang” matches because it has the minimum two full words in any order, and the comma (,) is ignored.
   iii. “Pham D Nguyen” matches because it has the minimum two full words in any order, and “D” is the initial of “Dang”.

   The following inputs may result in an unsuccessful match:

   i. “Pham” does not match because the number of words is less than the specified minimum.
   ii. “Pham D N” does not match since the initials are not counted as full words; hence, the number of matching full words is less than the specified minimum.
   iii. “Pham S Nguyen” does not match because, while “Pham” and “Nguyen” are matching full words, “S” does not match as the initial of “Dang”.

4. The matching strategy may support both languages, i.e., English and Vietnamese. The name in Vietnamese may be a Unicode string and may use phonetic matching against the data stored in the CRIDS.

II. Address Matching Rules

1. **Address Matching.** For the address of the resident, there could be support for both “exact” and “partial” matching strategies. There is a “threshold value” defined for

"partial" matching strategy that defines the percentage of full words from the address stored in the CRIDS database that should be specified in the input data of the service request for the match to be considered successful.

2. **Normalization.** The address value in the input data for the service request and the residents' address stored in CRIDS are both normalized using the following rules before comparison. The following characters/phrases are ignored:
    a. Period (.)
    b. Comma (,)
    c. Hyphen (-)
    d. Asterisk (*)
    e. Open and close parentheses [( )]
    f. Open and close brackets ([ ])
    g. Apostrophe (`)
    h. Single quote (')
    i. Double quote (")
    j. Forward slash (/)
    k. Backward slash (\)
    l. Hash (#)
    m. Care of labels, such as "C/O", "S/O", "D/O", "W/O", "H/O"
    n. "No."
    o. Leading and trailing spaces are trimmed and multiple consecutive spaces are replaced with single space.
3. When using "exact" matching strategy, the normalized address attribute of the input data is compared for an exact match with the normalized resident's address.
4. When using "partial" matching strategy, the normalized address attribute is compared for a partial match with the normalized resident's address. Following are the rules of partial match:
    a. Words may appear in any order.
    b. Following additional normalizations are applied to both the input data address value and the address stored in CRIDS database:
    c. Commonly used words are replaced with their shortened version:
        i. "apartment" => "apt"
        ii. "street" => "st"
        iii. "road" => "rd"
        iv. "main" => "mn"
        v. "cross" => "crs"

vi. “sector” => “sec”

vii. “opposite” => “opp”

viii. “market” => “mkt”

ix. Suffixes typically used with numbers such as “st”, “nd”, “rd”, and “th” are removed. For example, 21st is converted to 21, 44th is converted to 44, etc.

5. When used with threshold value other than 100, some of the words can be omitted in the input. Match is considered successful if the minimum numbers of full words that should match, as determined by the threshold value, are present in the input. Here is a scenario where a partial matching strategy with 60 percent threshold value is applied to the following value as resident’s address: c/o Pham Dung Nguyen, Apartment #12, Trong Building, Chua Boc street, Quan Dong Da, Hanoi, Vietnam, 560055
    a. This may be the normalized address: Pham dung nguyen apt 12 trong building chua boc st quan dong da Hanoi vietnam 560055
    b. These are examples of matching and their result:
        i. “s/o Pham Dung Nguyen, Trong Building, apt #12, chua boc st, hanoi – 560055” may be normalized to “pham dung nguyen trong building apt 12 chua boc st hanoi 560055” – which results in a successful match as 12 words are matched (more than 11 words which is the rounded up 60 percent of the total, 17).
        ii. “s/o Pham Dung Nguyen, Trong Building Hanoi 560055” may be normalized to “pham dung nguyen trong building hanoi 560055” – which results in an unsuccessful match since only 8 words are matched when a minimum of 11, representing 60 percent, was requested.
6. The matching strategy for address may also support the address both in English and Vietnamese, using the phonetic matching.

Annex 3

I. Standard Address Structure Proposed

The fixed attributes of the standard address structure are defined below:

CO – "care of" person's name

House – house identifier

Street – street name

Landmark – landmark, if any

LOC – locality where resident resides

VTC – name of the village, town or city

Commune – commune name

District – district name

Province – province name

PC – postal code

II. Encoded Usage Data

Hexadecimal digits within the "Encoded Usage Data" for the India Aadhaar system is interpreted based on below rules.

1st hexadecimal digit:

Bit 3-0: Version number of encoding. It may be hexadecimal "1" (binary: 0001) for encoding specified in this document.

2nd hexadecimal digit:

Bit 3: Was "Pi->name" attribute used?

Bit 2: Was "Pi->lname" attribute used?

Bit 1: Was “Pi->gender” attribute used?

Bit 0: Was “Pi->dob” attribute used?

3rd hexadecimal digit:

Bit 3: Was “Pi->phone” attribute used?

Bit 2: Was “Pi->email” attribute used?

Bit 1: Was “Pi->age” attribute used?

Bit 0: Was “Pa->co” attribute used?

4th hexadecimal digit:

Bit 3: Was “Pa->house” attribute used?

Bit 2: Was “Pa->street” attribute used?

Bit 1: Was “Pa->lm” attribute used?

Bit 0: Was “Pa->loc” attribute used?

5th hexadecimal digit:

Bit 3: Was “Pa->vtc” attribute used

Bit 2: Was “Pa->dist” attribute used?

Bit 1: Was “Pa->state” attribute used?

Bit 0: Was “Pa->pc” attribute used?

6th hexadecimal digit:

Bit 3: Was “Pfa->av” attribute used?

Bit 2: Was “Pfa->lav” attribute used?

Bit 1: Was “FMR” used for biometric auth?

Bit 0: Was “FIR” used for biometric auth?

7th hexadecimal digit:

Bit 3: Was “IIR” used for biometric auth?

Bit 2: Was “Pv->pin” attribute used?

Bit 1: Was “Pv->otp” attribute used?

Bit 0: Was “Tkn” used?

8th hexadecimal digit:

Bit 3: Was “Pa->po” attribute used?

Bit 2: Was “Pa->subdist” attribute used?

Bit 1: Was “Pi->dobt” attribute used?

Bit 0: Unused

9th to 12th Hexadecimal digits:

Currently unused. May have value 0.

For example, if an authentication is done for Aadhaar number “123412341234” and using demographic attributes “name”, “gender”, “date of birth”, “phone”, along with biometric FMR and OTP;

<Pid ts=”public” ver=”1.0”><Demo><Pi ms=”E” name=”Anand John” gender=”M” dob=”19690126” phone=”9999912345”/></Demo><Bios> <Bio type=”FMR”> YjRmYmJkMTZkZGQ4OGQxYTY5YjI0M2ZiYjU4YTFlNmQwMmQ1YTgyYjNmODU4YT MzYzQyZmNhOWUxN2QwNGVhNGMyMzExZjUyYmY4NjA5ZDVkZDY4YWU2NWE4OTNjNTMwNTJi M2U1YzQ5YTZkMGM2NzkyYTJlOGNhMTMxNDg0YWQ2MWM1ZGYzZGU0MTAzNExZWVlN2E0MjU 4ZjQ3ODg3NTU3ZWNmYzcwY2NkM2QwZmIzZjg5OTg3NjEzNzA3ZDliZjkyMWU3NTc3OGU2NGJk MmM3MDhiNGQ4NDgyZGJmMGM3YjY3ZGZkZGZkNjIyNgwMTllNjhhMmI4MjQxZWY0MA==

</Bio></Bios><Pv otp=”111111”/></Pid>

then the value of the “info” attribute may be:

“0166c782e8f95ba958f28adaae576c42a263c2449af416fb844499bef7fd41b2d00212be474bf2 a6bfd4f361389ae66809babc144829129ae2315d6bab02045aa1B8002200000”

where:

“01” – is the version of info structure

“66c782e8f95ba958f28adaae576c42a263c2449af416fb844499bef7fd41b2d0” – is the SHA-256 hash of Aadhaar Number

“0212be474bf2a6bfd4f361389ae66809babc144829129ae2315d6bab020455aa” – is the SHA-256 hash of “Demo” element (as a String)

“1B8002200000” (binary bits “000110111000000000000010001000000000000000000000”) – is the encoded usage data representing usage of name, gender, date of birth, phone, FMR, and OTP portions within authentication request.

Annex 4

I. Detailed Description of Technical Components of EISDP

Public Portal Features

1. **Public Information and Mobile Services.** The Electronic Identity Service Delivery Platform (EISDP) could provide the common public portal for sharing all public information related to Electronic Identity (eID) services accessible over the Internet. The portal could support Internet browser on laptops, desktops and mobile devices. The portal could have information that is publically available to all users, and some content could require registration and authentication. The public portal could provide registration capabilities for accessing the protected content on the portal. The portal could also provide information related to the registration process for eIdentity Service Provider Agencies (ISPAs) and eIdentity Service Consumer Agencies (ISCAs).

2. **Developer Information and Services.** The portal could also provide the content for software developers to help them develop their EISDP eID services-enabled software applications. The developers' content could include technical user guides, sample codes, blogs, discussion groups and a test environment for applications.

3. The portal could be hosted on the load-balanced web farm on virtualized web servers at the centralized Electronic Identity Authority of Vietnam (EIDAV) data center. The portal software could have content and user management capabilities and support multi-lingual capabilities.

4. The development environment could include the installation of the eID services such as authentication, electronic Know-Your-Customer (eKYC) and mobile ID services as stateless web services. The data could be hosted on active-active cluster-based database servers with Storage Area Network (SAN).

5. The public portal and development environment could have failover support from a disaster recovery system that is in a geographic location different from that of the data center. The system could failover to the disaster recovery site in case of failures. The data from the public portal and development environment database could be replicated in an asynchronous mode to the backup site.

IT Infrastructure (Hardware & Software)

The EISDP could be the common IT infrastructure and shared services for delivering Electronic Identity Service Delivery Framework (EISDF) eID services. It may be hosted in the two tier 3 EIDAV data centers in active-active mode. The detailed deployment architecture is described below.

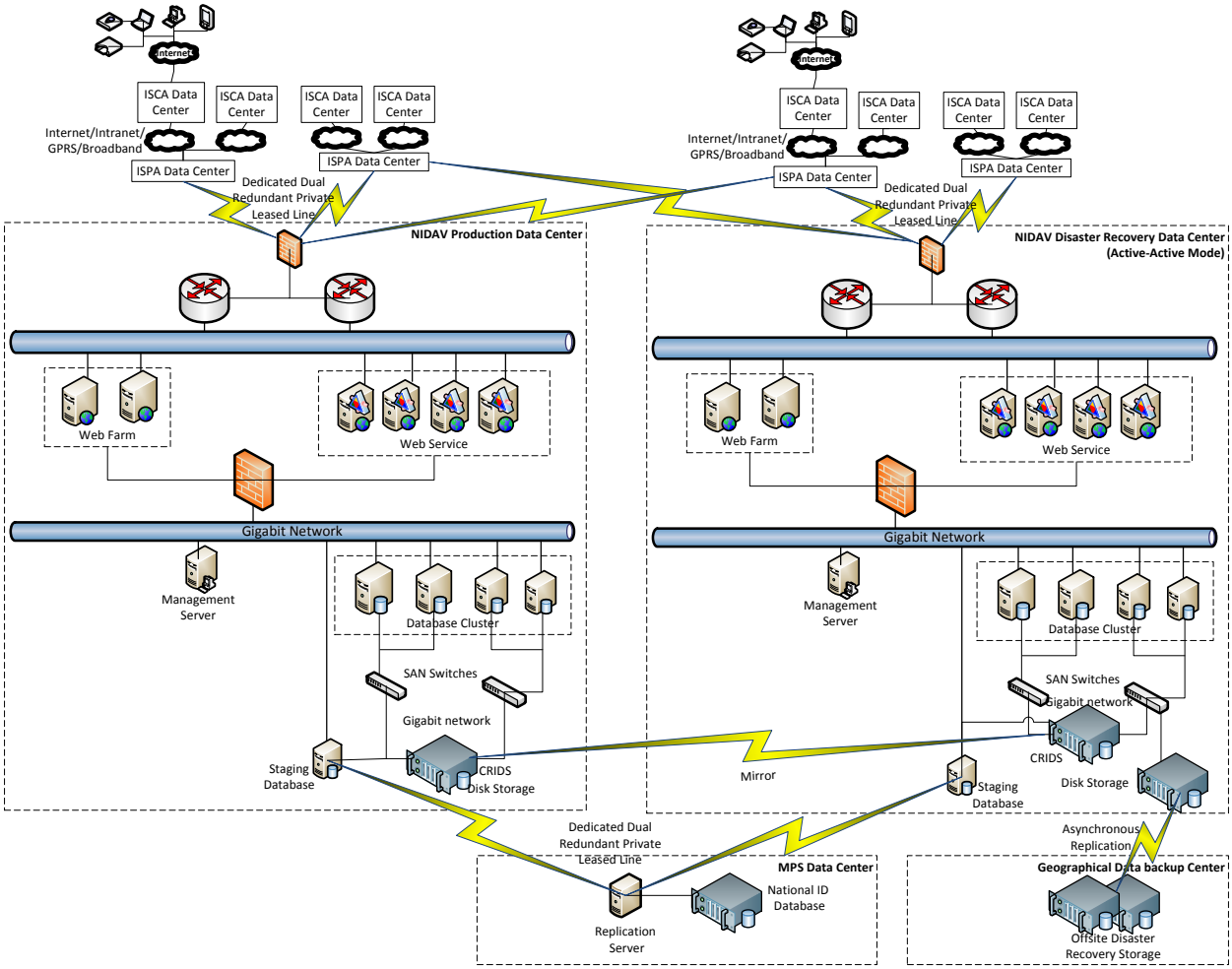


Figure 8.1: EISDP Deployment Architecture

1. The EIDAV data centers – namely, production and disaster recovery – could be hosted in the active-active mode with failover support for each other.

2. The data centers could be connected to each other using the fiber optic cable-based dual redundant private leased line connectivity. The data centers do not have direct access to the public network. It may only be accessed by the registered ISPA using the dual redundant private leased line connectivity between ISPA and the two EIDAV data centers.

3. The bandwidth requirements could be computed based on the expected volume of transactions from ISCAs.
    a. Approximately 5K average bandwidth is required for each Application Programming Interface (API) call.
    b. Handling about one million transactions per hour requires about 280 transactions per second (tps) on average. Considering a 30-40 percent spike, bandwidth for about 400 tps needs to be planned for. This turns out to be around 16 Mbps (400*5K*8 bits/sec)
    c. The ISPA may start with an 8 Mbps link and expand as the volume increases.

4. The eID services could generally be exposed as stateless web services. It could be hosted on the virtualized web farm with clustered virtual web servers. It could run the hypervisor with virtual machine manager software on a separate server. It could help to manage the provisioning and de-provisioning of virtual machines on the servers. The server hypervisor and virtual machine management software suite may be installed to manage the overall physical and virtual IT infrastructure for the two data centers. It may also implement the failover support using the migration of the virtual machines across the physical servers and across the data centers.

5. The eID services business applications such as ISPA and ISCA registrations, management and monitoring applications, reporting and Management Information System (MIS) applications, analytics applications, intranet portal, and mailing solution could be hosted on another virtualized web farm with clustered virtual web servers.

6. Both web farms could be hosted in a secure zone of the network infrastructure protected by firewall, and the separate isolated network with the redundant switches to prevent any malicious access outside of the private network.

7. The data could be stored on the servers and storage devices in the data zone that may be separated from the secure zone using the firewall. The data storage system may include the cluster-based database server with SAN storage connected to the database servers in the active-active mode. The SAN storage may be connected to the database server using the redundant storage switches over the one gigabit fiber optic cable. The storage capacity of the SAN storage media may be based on the expected volume of transactions from ISCAs.

a. Approximately about 5KB of data is used for storage of one transaction.
b. For 10 million transactions per day, the SAN storage may require 50 GB of storage size.
c. If online data storage of one month of is required, then 1.5 TB of online storage is required on the SAN storage beyond which it could be moved to tape.
d. Approximately, the size of national ID data for one resident is 5 MB. This includes the demographic and biometric data. The biometric data may include 10 fingerprints, photograph, and 2 iris scans. The total size needed to store data of 91 million residents of Vietnam growing at a rate of 10 percent could approximately be 500 TB (100 million x 5 MB) by 2015.
e. The total SAN storage capacity for the ID data of all Vietnam residents and one month of transaction data could be approximately 500 TB.
f. The total cost of the 15K RPM SAS disk could be USD 800,000 – based on the cost of USD 1,600 per one TB.

8. The SAN traffic could use one Gigabit Ethernet (GbE) in the data zone for data transfers between the web servers in the secure zone and database clusters within the data zone. It could also be used for SAN traffic between the storage media and the database cluster servers. The network architecture may include cabling, network cards, aggregation layer switch, and Top-of-Rack (ToR) switches. The capital cost may include core networking switches, cabling, network adapter card, aggregation layer switches and ToR switch costs. The operational cost could include power usage and cooling, electronics and underlying infrastructure updates, projected growth, management and risk factors costs.

9. The disaster recovery center could have the same configuration and capabilities as that of the production data center and could operate in the active-active mode.

10. The EISDF could also provide a public portal that could be accessible over the Internet. The public portal, apart from providing information-related Identity services to the individual residents and organizations, could also provide information targeted at the software developers who may want to design their own eID-based applications. The public portal could also expose the development environment for testing applications. The technical deployment architecture for the public portal and the development environment is described below.

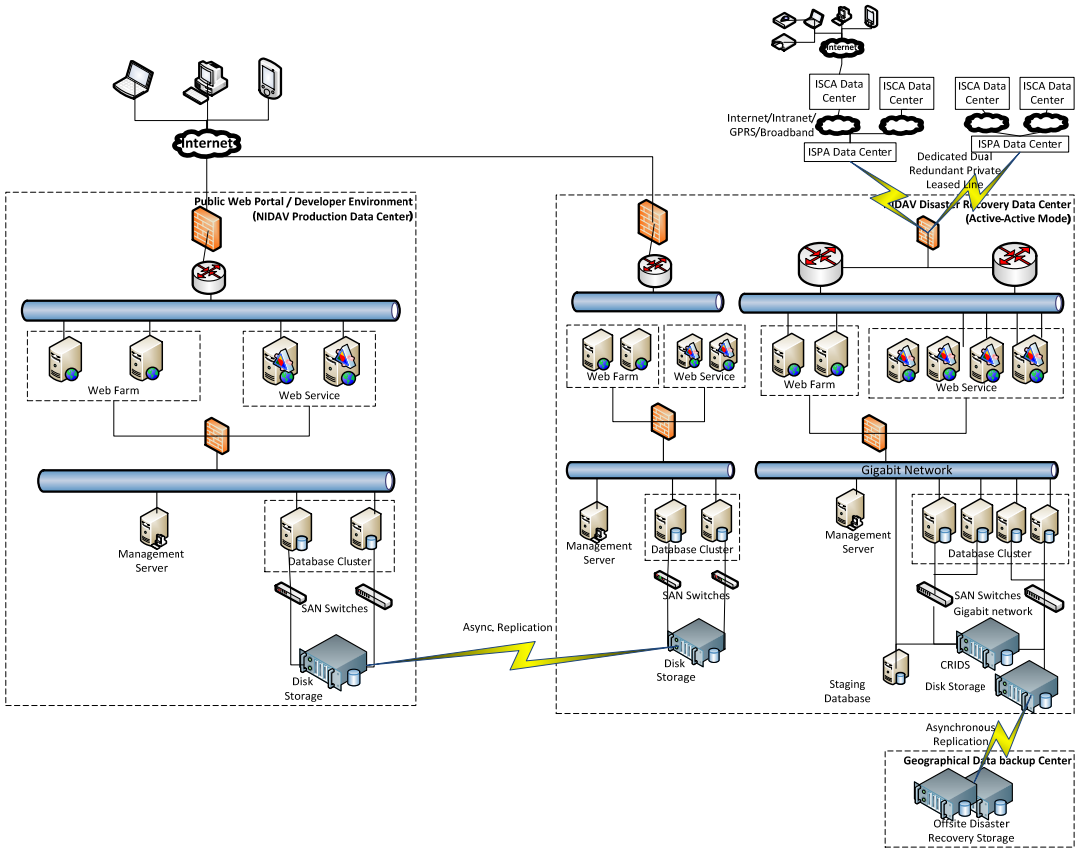


Figure 8.2: Technical Deployment Architecture for the Development Environment and the Public Portal

11. The public portal and the development environment could be hosted in EIDAV production data center with failover support from the EIDAV disaster recovery center. They could have a fault tolerance and load-balanced solution across both centers.

12. The public portal and development environment servers could be accessible over the Internet and could be completely isolated from the servers and the network of the secure and data zones in the De-Militarized Zone (DMZ). Their servers could be hosted on a different segment of the network completely separated from the servers in the secure and the data zones.

13. The public portal could be hosted on the virtualized web farm on virtual machines hosted on two clustered physical web servers.

14. The development environment could expose the identity functions as stateless web services on the virtualized web farm on virtual machines hosted for clustered physical web servers.

15. The management server could run the virtual machine manager software. It could help to manage the provisioning and de-provisioning of the hypervisor and virtual machines on the servers. The server hypervisor and virtual machine management software suite could be installed to manage the overall physical and virtual IT infrastructure for the two data centers. It could also implement the failover support using the migration of the virtual machines across the physical servers and across the data centers.

16. Both web farms could be hosted in the DMZ and could be made accessible over the Internet.

17. The development environment database and the documents in the content management server may be hosted in the secure data zone separated from the DMZ by firewall.

18. The sample identity database for the development environment could be hosted on the clustered server connected to the SAN using the latter's dual switches over the fiber cable-based Ethernet network.

19. The storage capacity of the SAN could be approximately 15 TB.

Physical Infrastructure

The EISDF could include the implementation of the physical infrastructure such as the data centers at various locations based on the topology and implementation requirements for the EISDF. The figure below describes the topology of the physical infrastructure to be established for the implementation of the EISDF.

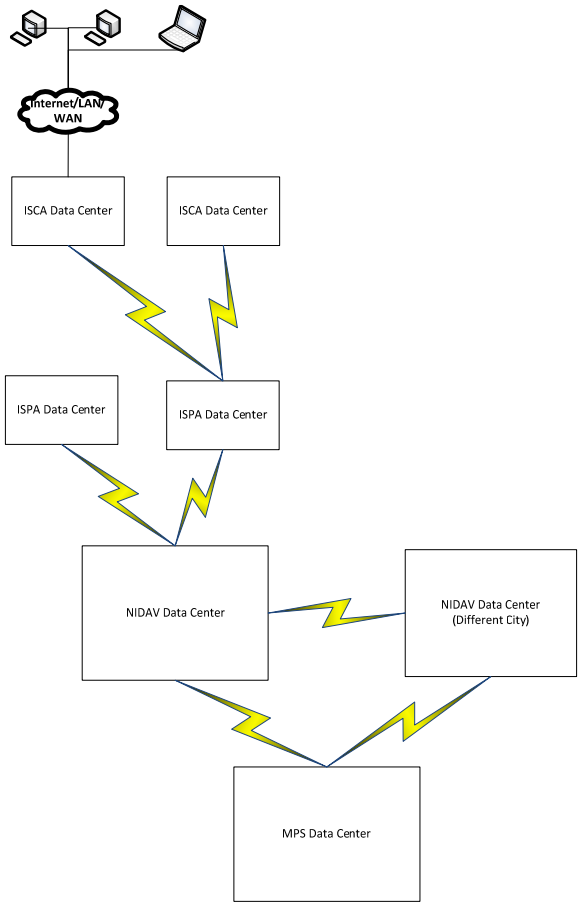


Figure 8.3: EISDF Physical Infrastructure Topology

EIDAV Data Center Features

1. The EISDP could be hosted at the EIDAV data center. All EISDF identity functions could be hosted at this data center and the services could be used by the mission-critical applications of government and private sector organizations; therefore, this data center could be designated critical infrastructure.

2. The data center could be designed as a tier 3 data center with 99.982 percent up time. The design could include building architecture, facility topology, engineering infrastructure and technology infrastructure. The facility topology could include space planning. The engineering infrastructure could address mechanical systems involved in the maintenance of the interior environment of a data center such as Heating, Ventilation, and Air Conditioning (HVAC). It could also include electrical infrastructure such as utility service, distribution, switching, and bypass from power sources, Uninterrupted Power

Sources (UPS), etc. The electrical system design could adhere to the Power Usage Effectiveness (PUE) requirements and energy standards.

3. The data center building could be constructed in an area of 1,000 square meters. The building could have server room, central control room, network management center, UPS distribution room, power distribution and management room, fire control room, conference and display room, etc.

EIDAV Disaster Recovery Center Features

1. The disaster recovery center could be built in a different geographical location such as a different city in a different seismic zone from the EIDAV data center. It could provide the failover support for the identity services, applications and the IT infrastructure of the EIDAV data center. It could work in the active-active mode and could host the identity services and applications to provide load balancing and fault tolerance solution to the EIDAV data center in case of failures.

2. The building size may be the same as the EIDAV data center's 1,000 square meters. The building specifications could also be the same with respect to mechanical, electrical and telecommunication infrastructure designs.

3. The network between the two data centers could be the dual redundant private leased line connectivity.

NID System Data Center Features

1. Thedata center could be the same as that which hosts the national identity database.

2. The National Identity Data (NID) could be used to populate the EIDAV database. The data could be transferred using a highly secure database replication mechanism.

3. There could be a dual redundant dedicated private leased line setup between the NID system's data center and the two EIDAV data centers.

Safety and Security System

The EISDP could provide the common security services that could be used by the services hosted on the platform. They are discussed below.

1. The end-to-end network security could be implemented using the standard network practices such as usage of encrypted channel, usage of digital certificates, IP filtering, authentication of systems and devices, network protection through firewalls and Network-based Intrusion Prevention System (NIPS), auditing, etc.

2. Multiple levels of network security through the creation of DMZ, application and data zones, and protecting all these zones using multiple firewalls, NIPS, and strong access control and audit schemes.

3. The servers hosting the services could be exposed only to authorized service providers through secure private connections using leased line to ensure multiple end-points exist to provide service in an always-available mode.

4. The physical security infrastructure could have multiple levels of security system for authorized personnel entry such as biometric-based access, among others.

Electronic Identity Authentication Service

The eID authentication may be done using demographic data and/or biometric data and/or One-Time Password (OTP)/digital certificate. There could be several ways for residents to be authenticated and they are discussed below.

1. The eID authentication functions may be exposed as stateless web service over Hyper-text Transfer Protocol Secure (HTTPS). The use of open data format in Extensible Markup Language (XML) and widely used protocol such as Hyper-text Transfer Protocol (HTTP) may enable easy adoption and deployment of eID authentication. The eID authentication may be exposed as formatted Uniform Resource Locator (URL) with input data sent to this URL as an XML document using content-type application/XML or text/XML. The corresponding response from the service may also be in XML format.

2. The eID authentication functions could be exposed in the form of APIs that could be used by the service providers to incorporate the eID authentication service types and features in their service delivery application.

3. The EISDP could maintain an updated version of the residents' eID information, i.e., the National Identity Number (NIN) + demographic and biometric data, in the Centralized

Resident Identity Data Store (CRIDS). The eID authentication services could be hosted on the eID authentication server; and the CRIDS, on a separate database server. The two servers could be hosted in the highly secure EIDAV data center.

4. In order to ensure a highly scalable and fault-tolerant solution that meets the response time Service-level Agreements (SLAs), the eID authentication services and the CRIDS could be hosted on load-balanced and cluster-based set of servers. The eID authentication services, along with the CRIDS, could be hosted on a secure zone and exposed only to authorized service providers through private connections using leased line to ensure multiple end-points exist to provide service in an always-available mode.

5. To support a strong end-to-end security and avoid request tampering and man-in-the-middle attacks, it is essential that data encryption take place at the time of data capture from the device. For security reasons resident data collected for eID authentication may not be stored in the devices or log files. It is also essential for ISCAs and ISPAs to maintain audit records for all the authentication request metadata along with the response.

6. The eID database in the CRIDS may be populated and updated on a regular basis using a centralized national-level identity creation process. Instead of recreating this process, the EISDP could reuse the resident data collected by the GoV in issuing the National Identity Data (NID) card and the NIN.

7. Given that the NID card and NIN is now being piloted by the MPS at the national level, there could be a single process for identity creation and verification. Hence the problem with multiple identities for the same resident could be solved. The NID card could be used as the centrally issued national identity token to identify the resident uniquely, while the NIN could be used as the unique identifier for the eID of the resident in the envisioned EISDF.

8. The eID authentication function could take the NIN along with the eID-holder's Personal Identity Data (PID) as the input which in turn submits the data to the CRIDS for matching, following which the CRIDS verifies the correctness of the data provided on the basis of the match with the eID-holder's identity information available with it. The service may respond with a "yes/no" response to either confirm the proof of identity or verify the information provided by the resident.

9. In all forms of eID authentication, the NIN could be submitted along with the single/multiple authentication factors so that the result is reduced to a 1:1 match.

10. The authentication function could search and select the residents' information record in the CRIDS using the NIN; thereafter the demographic/biometric inputs are matched against the stored data that was provided by the resident during the enrollment/update process.

11. The implementation of demographic authentication type may include the matching of the following basic demographic attributes:
    - Name in English and Vietnamese
    - Address
    - Gender
    - Date of birth (full date or just the year)
    - Age (verifying if a resident is above/below a given age)
    - Phone (verified mobile number of the resident)
    - Email (verified email address of the resident)

12. The demographic data matching features could be implemented based on the following design.
    - **Name Matching.** This may allow verification of the residents' name against their record stored in the CRIDS. The name-matching feature may implement various strategies that could be an exact match or a partial match with configurable match tolerance levels so that based on the application needs (i.e., having a strict match against a slightly loose flexible match), different strategies can be used. For example, while a bank application may choose a partial matching strategy, a passport/visa application may choose an exact matching one since it requires a resident's actual full name (as found in the CRIDS). Another example: a resident with NIN 123443211234 and whose name in the CRIDS is "Kim Pham Nguyen" wants to open a bank account. The banking application does a demographic authentication using the eKYC process where the application may choose not to require an exact full name matching, but instead allows a partial name matching. If the application uses partial matching strategy and prescribes a match value (or threshold) of 50 – meaning 50 percent or more of full words match those in the CRIDS – and the latter is obtained, then the customer account may be created. The rules for name matching are described in detail in Annex 2.

- **Date of Birth Matching.** This may allow complete date of birth or just the year.
- **Age Matching.** Some citizen benefits offered by the government may have age requirements. This feature may compare the age of the individual stored in CRIDS with the age provided at the time of service delivery.
- **Mobile and Email Matching.** This feature may compare the mobile number and email address stored in the CRIDS with those provided by the individual at the time of the service delivery.
- **Address Matching.** Some services such as banking, communication, and government welfare in Vietnam depend on address verification to complete the initial transaction and initiate the KYC process. Currently, verifications are done through paper-based documents that are also the basis of transaction trail preservation in the fulfillment of regulatory requirements. Address matching may be done online by verifying the address against the CRIDS data. The common address structure defined by EIDAV with the help of relevant ministries, departments, and other agencies may be used for storing and matching urban and rural addresses in electronic format. Address matching at this level may support the following.
    i. **Structured address matching** allows fields such as village/city, commune, district, province, zip code, etc., to be matched individually or in combination. This feature could enable address verification by the service provider applications and could give the option to validate the address using the eID standard address structure in full or in part. The proposed standard address structure is defined in Annex 3. For example, while issuing a SIM, the telecom operator application may capture the address and simply verify the province and district or zip code to ensure that the resident belongs to a particular telecom circle. To enter data in the application faster, the NID card could contain a 2-D barcode or Quick Response Code (QR code) written in XML format that can be read with a standard web/mobile camera. Service provider applications are encouraged to scan the 2-D barcode on the NID card so that the address field is populated in a structured fashion. If an application does not scan barcodes, but needs to have the address data manually entered from the NID card as a single string, then the unstructured address-matching scheme may be used. The detailed matching strategy for unstructured address is defined in Annex 2. The structured address may contain the following fields that can be verified individually or in combination:

- Fields that are free flow (as provided by the resident)
  - ✓ Care of person name
  - ✓ House identifier (single string containing house, apartment, or building number, name, etc.)
  - ✓ Street Identifier (single string containing street number, name)
  - ✓ Landmark details
  - ✓ Locality name and details
- Fields that are based on codified master data
  - ✓ Village/town/city name
  - ✓ Region name
  - ✓ Province name
  - ✓ District name
  - ✓ Commune name
  - ✓ Zip code
  - ✓ Post office name

ii. **Unstructured address matching** is used when the service provider application captures the address manually from the NID card or from the information provided by the resident. This allows an address to be captured as a single string and be matched against the address in the CRIDS. Although this option is easy for verifying existing or manually entered data, it requires matching without strict order and without all parts of the full address being there. For this reason, eID authentication may allow partial matching strategy during address matching and applications may be allowed to choose the match tolerance level based on their needs. In general, while structured matching provides greater accuracy, the unstructured kind allows flexibility.

13. Biometric authentication could allow service provider applications to verify if the resident is "who he/she claims to be". Several applications require physical, in-person verification. Biometric authentication could have the following features:
    - o **Fingerprint matching.** This may allow one of multiple fingers to be used for matching depending on the needs of the application. Use of multiple fingers allows better fusion strategy on the authentication server for greater accuracy. Authentication using fingerprints could either be Fingerprint Minutiae Recognition

(FMR) or Fingerprint Image Recognition (FIR). While applications for FMR could operate on low bandwidth network, those for FIR could require higher bandwidth.

- **Iris matching.** In general, iris matching is more accurate than fingerprint matching. Iris matching relies on Iris Image Recognition (IIR).

14. The biometric data captured as input data may comply with open standards. FMR could comply with ISO 19794-2 finger minutiae format with no proprietary extensions allowed. FIR could comply with ISO 19794-4 image format that could contain a compressed or uncompressed image, of type PNG, WSQ, or jpeg2000. IIR could comply with ISO 19794-6 image format that could be of type png, or jpeg2000.

15. In order to improve accuracy and reduce the number of matches, the authentication request could contain the biometric "position hint" for each biometric template. Position hint is used on the server to optimize the match. The valid position hint values are LEFT_IRIS, RIGHT_IRIS, LEFT_INDEX, LEFT_LITTLE, LEFT_MIDDLE, LEFT_RING, LEFT_THUMB, RIGHT_INDEX, RIGHT_LITTLE, RIGHT_MIDDLE, RIGHT_RING, and RIGHT_THUMB.

ISPA Data Center Features

1. The Identity Service Provider Agency (ISPA) may be a government or private sector entity. The ISPAs offer their network connectivity to Identity Service Consumer Agencies (ISCAs) and transmit latter's identity service requests to the EISDP. Only agencies contracted with the EISDF as ISPAs may send identity service requests to the EIDAV data center. The ISPA registration process, as well as the detailed technical guidelines for setting up and operating an ISPA date center, could be published on the EISDF public portal.

2. The ISPAs could setup dual redundant and dedicated private leased line connectivity between its data center and the EIDAV data center. An ISPA data center could be a critical infrastructure in the delivery of the identity services; hence, its design could include a disaster recovery solution with a remote data backup support. The ISPAs could setup their data center with the capability to extend assistance to the ISCAs. The technical deployment architecture for that data center is described in Figure 8.4.

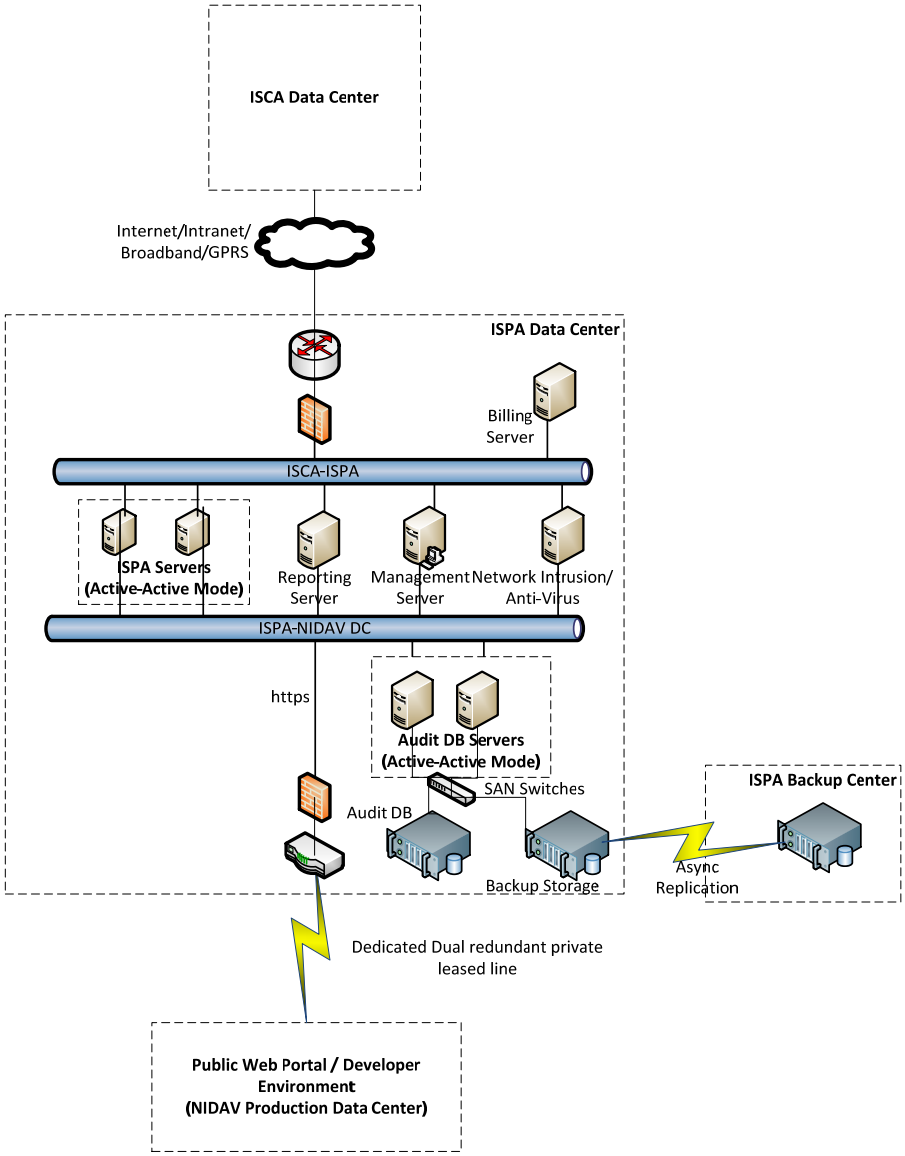


Figure 8.4: Technical Deployment Architecture for ISPA Data Center

3. The bandwidth requirements for the ISPA data center may be computed based on the expected volume of transactions from ISCAs. Approximately 5K bandwidth is required for each API call. Further, handling about one million transactions per hour could require 280 Transactions Per Second (TPS) on average. Considering a 30-40 percent spike, the bandwidth for about 400 TPS could have to be planned for. This turns out to be around 16 Mbps (400x5Kx8 bits/sec). Based on the above estimates, the ISPA could start with an eight Mbps link and expand as volume increases.

4. An ISPA could provide a pair of routers to the EIDAV data center for terminating leased line. Network devices such as routers and switches may be installed to enable connectivity

between the ISCA and ISPA data centers. An ISPA could deploy at least two servers in the active-active mode for hosting in its data center. The servers may be clustered and virtualized with dual quad-core blade/rack servers with 64 GigaByte (GB) Random Access Memory (RAM).

5. A firewall server could be deployed for securing the network between ISCA and ISPA, and between ISPA and EIDAV. In addition to the firewall, an ISPA could deploy network intrusion detection and prevention systems as well as anti-virus and anti-malware systems to ensure protection against attacks.

6. To prevent single-point failure of the audit database, two database servers in high availability active-active clustered mode could be deployed. The SAN storage may be connected to the database servers using switches and a fiber optic-based network.

7. Six months of audit data could be maintained by the ISPA. Considering an audit data size of 5K per transaction, ten million transactions per day could require the ISPA to have 50 GB a day, or 1.5 TB a month. Beyond one month, data could be moved to a backup storage. In order to ensure high availability of the data, the audit transaction data could also be backed up at a remote site using asynchronous replication.

8. The ISPA may setup separate servers: one for MIS reporting and billing, and another for management and monitoring of the virtualization, network, servers, database, backup, replication and applications. The server class operating system and the hypervisor could be deployed on all physical servers in the data center.

9. The host Virtual Machine (VM) and guest VM could be set up using the VM Manager deployment on the management server. The ISPA server software may be deployed on the VMs. The database software could be installed on the database servers, while any Enterprise Monitoring Software (EMS) could be deployed to effectively oversee the production system.

ISCA Data Center Features

1. The Identity Service Consumer Agency may be a government or private sector entity that registers with the EISDF to avail of services in the identification and authentication of its clients. The ISCA identity service requests could be coursed through an ISPA, sole direct channel to EIDAV.

2. The ISCA registration process, as well as the detailed technical guidelines for setting up and operating an ISCA data center, could be published on the EISDF public portal. The ISCA could provide itself a disaster recovery solution with remote data back up support as prescribed by the EISDF guidelines for ISCA data center.

3. The ISCA could set up network connectivity to be able to send request to and receive response from its designated ISPA. It could be recommended that the ISCA have a private leased line; however, it could be allowed to use existing broadband or GPRS Internet connectivity.

4. The ISCA could develop its own service delivery application that could integrate the identity service API calls. The technical guidelines provided by EISDF could be followed to establish a secure and fail-proof delivery of services.

5. The ISCA could host its own web-based service delivery applications in their data center and its client-based application on the PoS terminal that is integrated into the EISDF. Requests could be sent from the PoS terminal to the ISCA data center that could then forward them to the ISPA via a secure network.

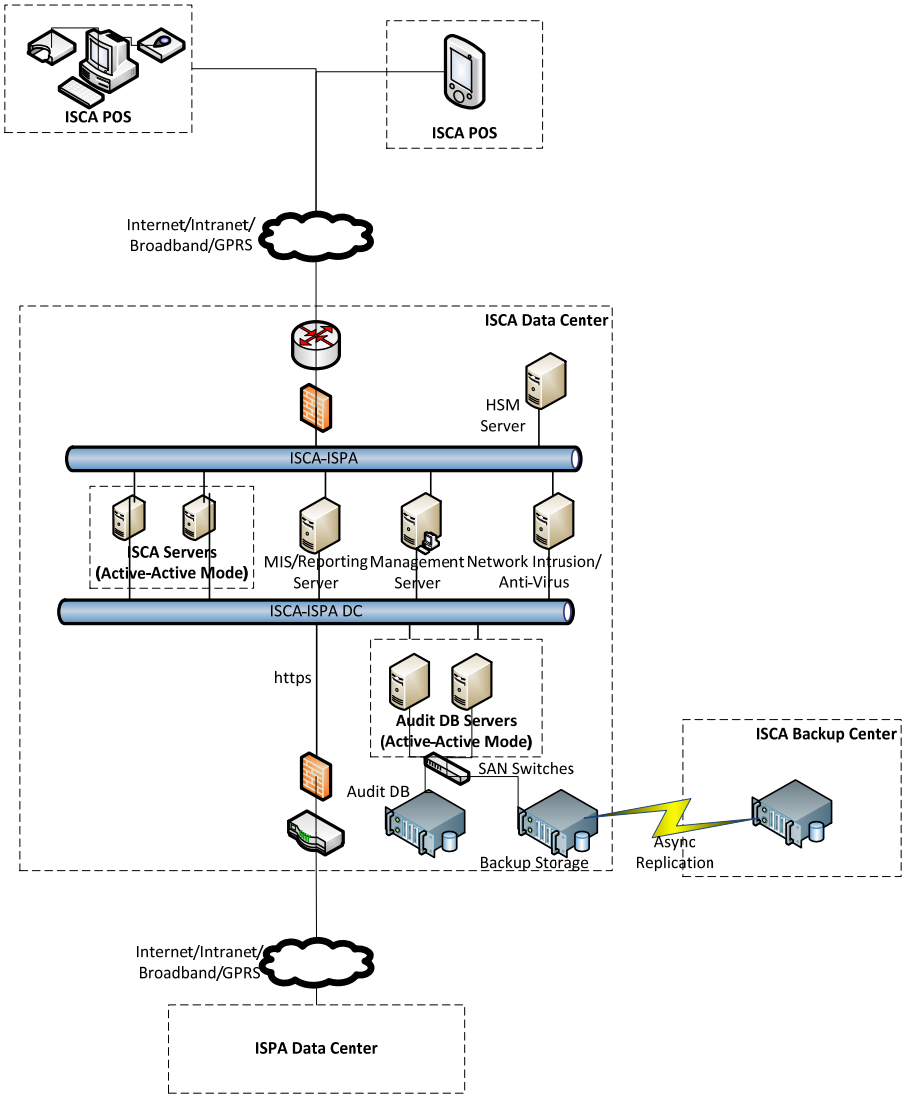


Figure 8.5: Technical Deployment Architecture for ISCA Data Center and PoS

6. Depending on business requirements, different identity services such eKYC, mobile ID, etc., may be employed. The business establishment could use demographic, biometric, or a combination of the two types of authentication.

7. The PoS software may be a centralized web-based or rich client-based application. The PoS terminal could be equipped with EIDAV-compliant biometric devices for fingerprinting, iris scanning, and facial photography. The data captured could then conform to data standards as defined by EIDAV.

8. The PoS application could package the demographic and biometric data following EIDAV's technical guidelines for eID authentication. The package could include data encryption using symmetric key and, in addition, the private key of the ISCA as assigned by EIDAV. The data packaged may be transmitted over the network between the PoS terminal and the ISCA data center.

9. The ISCA data center could secure the incoming traffic from PoS terminals using firewall, intrusion detection, anti-virus, and anti-malware systems. It may be hosted on a separate server. It may also host the hardware security module for private key management.

10. The ISCA server application receives the incoming encrypted data, processes it and forwards the validated data packages to the ISPA. The ISCA server application could be hosted on the ISCA servers that are two virtualized and clustered servers in active-active mode. The process of virtualization could be handled by the management server that is hosted separately.

11. The MIS capabilities could be hosted in the ISCA data center for internal and external reporting and data analysis.

12. Two database servers in high availability active-active clustered mode could be deployed for the audit database to prevent single point of failure.

13. The SAN storage could be connected to the database servers using SAN switches and fiber optic-based network. Six months' worth of audit data could be maintained by the ISCA. Considering 5K audit size per transaction and one million transactions per day, the ISPA could require five GB of storage size daily. For one month, 150 GB of storage could be needed; beyond one month, data could be moved to the backup storage.

14. The SAN storage data could be backed up in-site and off-site using asynchronous replication.

15. Monitoring software to effectively oversee production system could be deployed. Any EMS may be used.

16. The ISCAs could be assigned a unique alphanumeric code by EIDAV at the time of the registration to uniquely identify the ISCA. The ISCA could send its unique ISCA code as part of service request input parameters to identify itself to EIDAV as the registered user of the eID authentication service.

17. The ISCAs could automatically validate the Secure Sockets Layer (SSL) certificate and ensure it is validated against the revocation list online.

18. The ISPA may host a server in its data center that could send the service request from the ISCAs to the authentication server in EIDAV data center. The ISPA server could add one of its valid license keys to the service request package from the ISCAs. The authentication server may accept the request only from valid ISPAs and only from their registered static IP addresses coming through a secure private network.

19. EIDAV could define a standard XML data format for inputting authentication service requests. The format may enable the storing of both the demographic and biometric data. The demographic data in the data fields could comply with the Know Your Residence (KYR) specifications and could support data capture in both English and Vietnamese. The format could support the provision for defining the language for the demographic data for the service request.

20. The audit trail could be stored and maintained by ISCAs, ISPAs and EIDAV on their servers; each service request and response in XML documents could be kept for a defined period of time to allow for issue resolution, audits and business intelligence.

21. Since the technical architecture is based on stateless protocol, there could be a unique Transaction Identifier (Transaction ID) attached to every service request and response in order to track the proceedings in the full round trip across the various systems. It is highly recommended that ISCAs use this attribute for correlating requests with responses for auditing and verification.

22. **License Key.** Each ISCA could be assigned a valid license key by EIDAV that could be used in the authentication process. The license key could be a unique alphanumeric string of length up to 64 characters, and could have expiry built into it. The administration portal

of EIDAV could provide a self-service mechanism for the ISCA administrator to generate a new license key and renew before expiry.

23. **Session Key.** The session key is single-use symmetric key that may be employed for encrypting all request and response messages in one communication session. The session key, possibly a 256-bit Advanced Encryption Standard (AES), could be generated by the ISCA using encryption facilitated by the public key of EIDAV digital certificate or biometrics. It is further encoded using the base-64 encoding to enable transmission over the HTTPS. The encoded and encrypted session key may be added to the XML document sent as the input data in the service request. The encryption of the key could ensure that it is known only to the ISCA involved and EIDAV – and is not captured by the man-in-the-middle attacks on the wire.

24. The PID captured on a device is encrypted on the capture device itself for security reasons. The PID, which may include both binary biometric and demographic textual data, could be further encoded to stream over the HTTPS protocol that is designed to deal with the textual data. The authentication services may provide both options of encoding the binary and textual data into either the base-64 encoding[11] to transfer the binary data over media that is designed to deal with textual data, or in binary format based on Protocol Buffers standard[12]. The base-64 encoding of the PID and further packaging of the input data with enveloping XML may be done on the device or the ISCA server depending on ISCA needs. Device capability, protocol between devices and the ISCA server, and data format used between devices and the ISCA server, etc., could be taken into consideration when making the choice.

25. The authentication service design may be extensible and support different tokens such as mobile phone, Near Field Communication (NFC) token, smart card, etc., today and in the future. This may be useful in adding second factor authentication ("what resident has") for a self-service transaction by the resident. EIDAV could support the new national ID card, mobile ID, registered mobile phone, and resident email ID as token types.

---

[11] Base-64 encoding - https://en.wikipedia.org/wiki/Base64

[12] Protocol Buffers standard - http://code.google.com/p/protobuf/

26. The ISCA could work with the Telco operator to obtain the mobile number of the mobile device from which a service request is being made in order to ensure that the request is originating from the registered mobile number of the resident.

27. Each authentication request may capture the token type and value of the token used for initiating the service request.

28. **Tampering of Personal Identity Data.** In ensure that the PID is not tampered with during transport from device to authentication server, the former may compute the SHA-256 hash of the PID XML string before sending. The hash value computed could be added to the XML document that is sent as the input data to the service request. Also, when the authentication server receives the request XML document, it may re-compute the hash of the PID and compare it with the hash value received in the service request. If the values do not match, it rejects the authentication request with an error code stating the PID has been tampered with.

29. **Ensure message integrity and prevent non-repudiation.** ESignature could be used to ensure integrity of the message during transmission and prevent non-repudiation of the source of the service request. The service request XML document may be digitally signed using the XML eSignature of the ISCA or ISPA, depending on which agency creates the final request XML document. By signing the XML document, it is certified that the message security and integrity between servers are intact and that the request was indeed sent by the signer.

30. The eSignature could be procured by the ISCA and the ISPA from the valid certification authority as per the ESignature Act[13]. The eSignature may be a class II or class III certificate. The digital certificate may include two parts: X.509 certificate representing the public key, and the private key that is used for digital signing. The private key could be stored securely and the certificate owner could have the responsibility of ensuring that it is not compromised. The EIDAV authentication server could check to ensure that the certificate belongs to the ISCA or the ISPA and that it had been issued by the valid certification authority. Hence, it is mandatory that "O" attribute of "Subject" in the X.509 certificate does match the name of the agency.

---

[13] ESignature Act - http://www.moj.gov.vn/vbpq/en/Lists/Vn%20bn%20php%20lut/View_Detail.aspx?ItemID=4172

31. There could be a capability to timestamp the capture of authentication input on a device. The format of the timestamp could be "YYYY-MM-DDThh:mm:ss" and may be derived from the ISO 8601. Time zone may not be specified and is automatically defaulted to ICT (UTC +7.00). The timestamp plays a critical role; hence, it is recommended that devices are time-synchronized with a time server.

32. The ISCA and ISPA servers could support buffering of authentication requests and could send requests to the authentication server to support occasional lack of network connectivity on the field. The maximum time that requests may be buffered (queued) could be defined by the National IT Security and the National Identity Service Delivery Framework (NISDF) IT Operation policy. All requests with timestamp value older than the prescribed limit could be rejected.

33. As per EIDAV's security policy, if the number of failed attempts crosses the upper limit, the resident record in the CRIDS may be put on hold. The upper limit may be dynamically computed based on various heuristics and it may not be a static number.

34. The response from authentication service is an XML document. For privacy reasons, it does not return any personal data of the resident and responds only with "yes/no".

35. The authentication service could provide a mechanism to validate the authenticity of the response for non-repudiation purposes. In order to enable verification and audit, the authentication response could be digitally signed by EIDAV and the signature could be part of the response. The signature could be verified using the EIDAV public key and the signature could comply with the W3C XML signature standard[14]. The ISCAs could preserve the authentication response for each request that originates from their server for non-repudiation purposes.

36. The authentication response could provide a mechanism to co-relate the response with the request by passing the same transaction identifier that came with the request back in the response. It could also include the timestamp when the response is generated.

---

[14] W3C XML Signature standard - http://www.w3.org/TR/xmldsig-core/

37. In order to enable a mechanism wherein the authentication response could be used as the digital Proof of Identity (PoI) and Proof of Address (PoA) at a later time, the response could add the meta information to the PID details included in authentication request. This could include the SHA-256 hash value of the NIN, the SHA-256 hash value of the demographic part of the PID block and the encoded usage data in HEX format of the various demographic attributes usage of this authentication request. The design of the encoded usage data for India Aadhaar system is described in Annex 5.

38. The eID authentication service may be originated from either a "registered" or a "public" terminal device. The public devices are those without a secure container to store the keys. The connectivity between the public devices and the authenticator could use a secure protocol such as HTTPS.

39. For public devices, data could be encrypted with a dynamic session key using AES-256 symmetric algorithm (AES/ECB/PKCS7Padding). The session key, in turn, could be encrypted with 2048-bit EIDAV public key using asymmetric algorithm (RSA/ECB/PKCS1Padding). The session key may not be stored anywhere, except in memory, and it may not be reused across transactions. When using public devices, it is highly recommended that an OTP be used.

40. The steps for packaging and encrypting the service request on the "public" device are:
    a. The NIN, demographic and biometric details — as required by the application — are entered into the device along with other factors such as OTP, if it is used. If OTP is used, the request for it is sent to the eID authentication server along with the NIN. The eID authentication server sends the OTP back to the resident's registered mobile phone as a Short Message Service (SMS) and to the registered email address.
    b. The ISCA/Sub-ISCA application generates a one-time session key.
    c. The authentication "data" XML block could be encrypted using the one-time session key and then encoded (base 64).
    d. The session key could then be encrypted with the EIDAV public key.
    e. The ISCA application on the device could send the encrypted block along with Hash-based Message Authentication Code (HMAC) data to the ISCA server.
    f. The ISCA server could form the final authentication XML input for service request, including license key and transaction reference (txn attribute), and send the data to the eID authentication server through an ISPA network.

g. The eID authentication server decrypts the session key with the EIDAV private key. The data block is then decrypted using the session key.
h. The resident's decrypted biometric and demographic information – and optional OTP – are taken into account during the matching process based on the input.
i. The eID authentication server responds with "yes/no" in the digitally signed XML.

41. **Authentication Audits.** The eID authentication could record all the authentication requests and their responses for audit purposes. By providing the NIN and the authentication response code, the ISCA could request EIDAV to confirm the result of an authentication, along with the authentication factors that were presented in that request. National IT Security and EISDF IT Operation policy could determine how long these audits could be maintained.

42. All authentication responses could be digitally signed by EIDAV and the ISCAs could be advised to validate the response integrity and may keep track of these for audit purposes. In addition, attributes such as timestamp and demographic usage data within the authentication response may be used to verify if the request was indeed for a particular NIN, if the request indeed had a biometric factor, or when the authentication was done, etc. Such self-verifiability of the authentication response may allow third party applications to trust and electronically verify the digitally signed response quite similar to that of an offline trust establishment honoring a notarized document.

43. In order to ensure that the solution is widely adopted and is interoperable with the existing systems, it is recommended that technologies that comply with open standards be used. Some of the open standards that may be look into are:
    a. **Demographic data standards.** There could be a standard for capturing necessary demographic data of the resident so that this identity information works across various systems and ensures interoperability across various government and private agencies that use the EISDF. It is important that the capture and verification of basic demographic data for each resident is standardized across all partners of the EISDF. For instance, the Unique Identification Authority of India (UIDAI) set up the Demographic Data Standards and Verification Procedure (DDSVP) committee[15] for this purpose.

[15] Demographic Data Standards and Verification procedure (DDSVP) committee – http://uidai.gov.in/UID_PDF/Committees/UID_DDSVP_Committee_Report_v1.0.pdf

b. **Biometric standards.** EIDAV could set up a committee for defining the biometric standards based on the national and international standards; it could also define best practices, expected accuracy, interoperability, conformity, and performance in biometric standards. For instance, the UIDAI set up a committee for biometric standards[16].
c. eID Biometric APIs[17]
d. Data Encryption Algorithm – ANXI X3.92
e. Banking—Retail Financial Services Symmetric Key Management – ANSI X9.24
f. Public Key Cryptography for the Financial Service Industry: Agreement of Symmetric Keys Using Discrete Cryptography – ANSI X9.42
g. Triple Data Encryption Algorithm: Modes of Operation – ANSI X9.52
h. Security Requirements for Cryptographic Modules – FIPS PUB 140-2
i. Personal Identification Number (PIN) Management and Security – ISO 9564
j. Information Technology – Security Techniques – Hash Functions – ISO 10118
k. Information Technology – Security Techniques – Key Management – ISO 11770
l. Information Technology – Security Techniques – Encryption Algorithms – ISO 18033
m. Biometric Standards – ISO 19794-4, ISO 19794-6
n. Date and Time Format Standard – ISO 8601
o. XML Signature – http://www.w3.org/TR/xmldsig-core/
p. Metadata and Data Standards for Person and Land Region Codification – e.g., eGovernance standards[18] defined by the Government of India.
q. Protocol Buffers – http://code.google.com/p/protobuf/
r. Geolocation Standard – ISO 6709

Mobile ID Service Features

1. Assuming the use of a physical card for the SIM, the card to be used for mobile ID service should be produced in a secure environment and could comply with the protection profile defined by the European Committee for Standardization Workshop Agreement (CWA)

---

[16] Biometric standards – http://uidai.gov.in/UID_PDF/Committees/Biometrics_Standards_Committee_report.pdf

[17] eID Biometric APIs – http://uidai.gov.in/UID_PDF/Working_Papers/Aadhaar_ABIS_API.pdf

[18] Metadata and data standards – http://egovstandards.gov.in/standardsandFramework/metadata-and-data-standards/MDDS_Standard_release_version_1.0__Dec_24_2k9.pdf

14169 with Evaluation Assurance Level 4+ (EAL4+) according to Common Criteria (CC) security standard (ISO/IEC15048). The SIM vendor should provide the certificate upon request from the Certification Authority (CA) for a particular SIM product.

2. The SIM could have the Secure-Signature-Creation Device (SSCD) module with two key pairs: one for authentication, the other for signing/non-repudiation purposes. The signing key may be protected by a PIN.

3. The application that may be stored on the SIM is the Over-The-Air (OTA) SMS interface for authentication transaction, eSignature transaction, changing of PINs, unblocking private keys with PIN Unlock Key (PUK) code, decryption of encrypted data, and decryption and display of text message.

4. The mobile phone could support at least Phase 2+ SIM Toolkit.

5. The estimated cost of the production of SIM with Wireless Public Key Infrastructure (wPKI) capabilities may be USD 1-2 with digital certificates or biometrics, and application loaded on the SSCD area.

6. EIDAV may have to provide the standard technical specifications for the wPKI-enabled SIM for mobile ID services and supported mobile phones.

7. SIM Provisioning Design

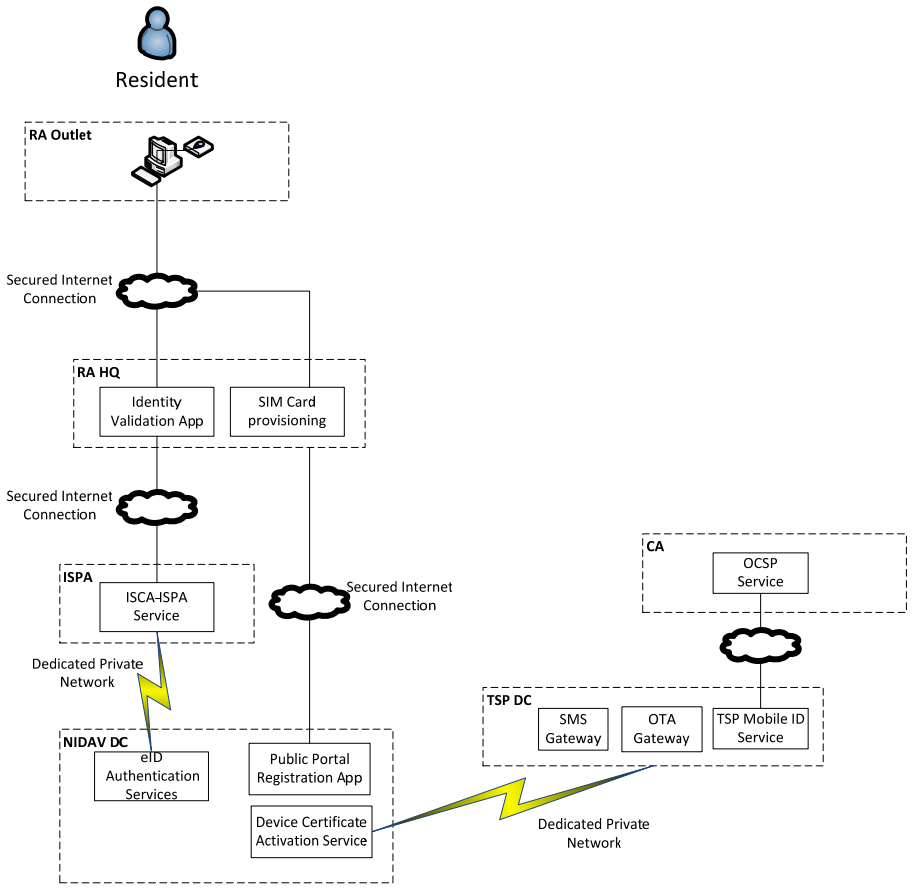


Figure 8.6: SIM Provisioning Technical Architecture

a. The EIDAV portal could provide the registration applications for entities that could be involved in mobile ID services as Registration Authority (RA), Trusted Service Provider (TSP), ISCA, ISPA and CA.
b. The RA could set up outlets for SIM provisioning, user registration and certificate activation.
c. The RA could host the application for resident identity validation on the servers in its data center and provide access to the Internet at the outlets for performing identity validation of the resident at the time of SIM provisioning. The identity validation application may have the same technical architecture as the ISCA application that could call the identity authentication service provided by EISDF for biometric authentication. The outlets could install biometric readers with the application for identity verification of the resident.
d. The RA may also host the web application for activating the device certificate of a SIM and circulating it to TSPs. EIDAV may host a web service in its production data

center for the purpose of disseminating device certification activation details to TSPs. The RA outlets could call this application over the Internet.

8. User Registration/Certificate Activation Design

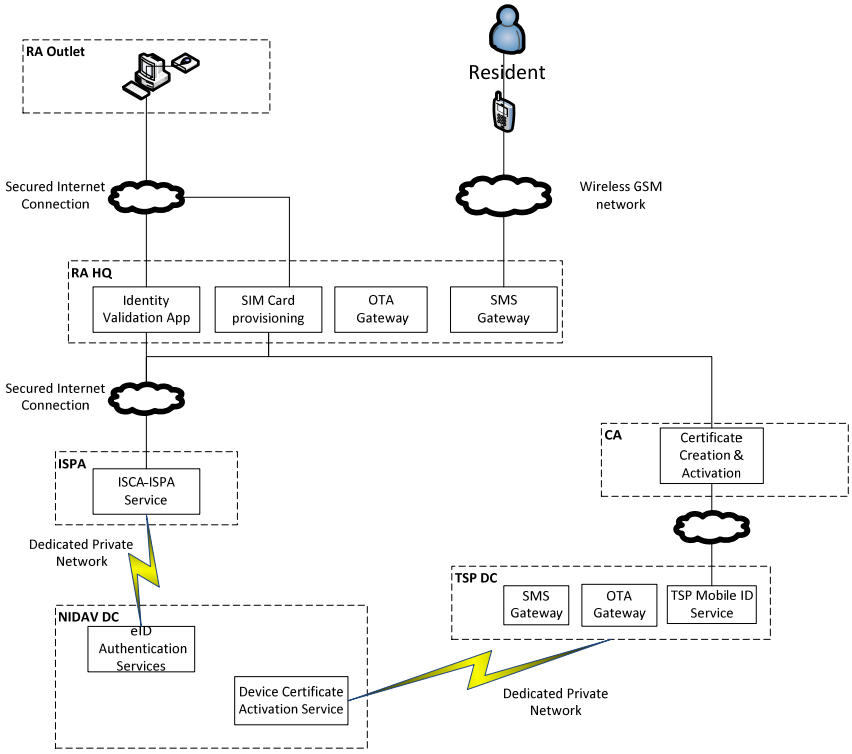


Figure 8.7: User Registration/Certificate Activation Technical Architecture

a. The user initiates the SIM activation application on the mobile phone. The application sends the activation request over the wireless Global System for Mobile communication (GSM) network to the Short Message Service Center (SMSC)/SMS gateway hosted in the RA data center. The SMSC forwards the request to the SIM activation application hosted in the back-end servers in the data center.
b. In response, the application sends the request for signature on the personal identity data via the OTA and the SMS gateways. The resident verifies the data and signs it by inputting the device certificate activation code.
c. The RA receives the signed personal data and includes other information such as the device certificate; it then forwards the request for certificate activation to the designated CA over a secure Internet connection. The RA also sends the service request to EIDAV via a registered ISPA to update the resident's identity record with the mobile number.

d. The CA creates and activates a qualified certificate and publishes it to inform TSPs and EIDAV.

9. Usage Design

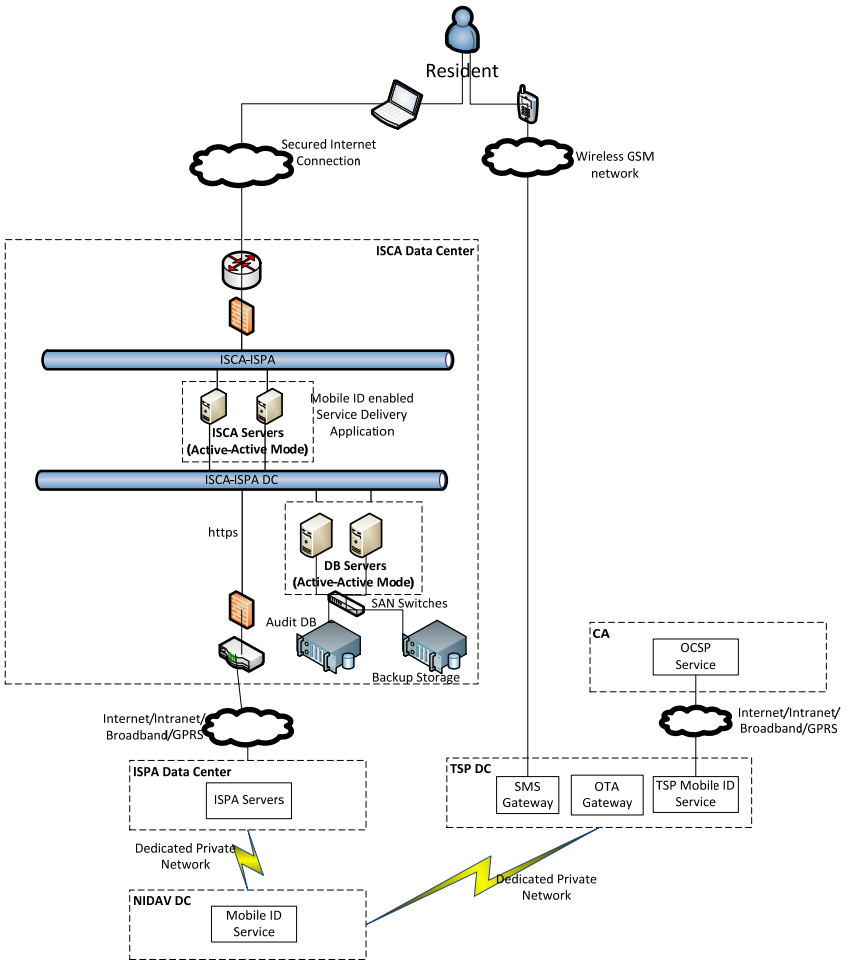


Figure 8.8: Mobile ID Usage Technical Architecture

a. The service provider integrates the service delivery application into the mobile ID service and hosts it on the ISCA data center. The service delivery application has the option to click the “Log in with mobile ID”.
b. The ISCA system calls the EISDF mobile ID web service hosted on the EIDAV data center with the NIN, mobile number and PIN of the resident via the ISPA.
c. The EIDAV mobile ID web service validates the mobile number provided using the stored mobile number for the given NIN in the CRIDS.

d. After successful validation, it calls the TSP web service hosted in the TSP data center over the secure Internet connection with the mobile number, verification code and the PIN.
e. In response, the TSP service generates the verification code and sends it to the ISCA website. It also generates the signature request with the verification code, mobile number and PIN; then it sends it to the resident's mobile phone using the OTA and SMS gateways of the TSP over the wireless network in SMS format.
f. The specialized OTA SMS activates the identity verification application on the SIM card. It displays the verification code that is the same as that displayed on the computer of the resident. The resident validates the verification code displayed on the mobile device with the one displayed on the computer and signs the request by entering the PIN.
g. The TSP receives the signature data and calls the Online Certificate Status Protocol (OCSP) service of the CA to validate the signature data and the certificate.
h. The TSP forwards the response received from the CA to the ISCA via EIDAV and the ISPA.
i. On successful authentication, the resident logs into the secure website.

10. Termination Procedure
    a. In cases of certificate revocation, the RA informs the CA of certificate revocation and the CA immediately revokes the certificate and publishes the updated Certificate Revocation List (CRL) for the benefit of the TSPs. It also alerts EIDAV via the ISPA to update the identity record in the CRIDS and deactivate the mobile ID service for the resident along with the reason.
    b. In cases of SIM blocking due to loss or SIM damage, the device certificate is taken out of the list of valid SSCDs available to TSPs. EIDAV is alerted via the ISPA to update the identity record in the CRIDS and deactivate the mobile ID service for the resident along with the reason.

Electronic Identity Seeding Service

Seeding Utility could be a desktop program available for download from EIDAV's public portal after successful registration.

1. The ISCA downloads the utility from the portal and installs it on its server as the executable.

2. The utility provides the capability for data extraction, consolidation, normalization and matching. The utility connects to different data sources to pull the relevant PID from reference databases. It also pulls the data from the relevant data tables in the service delivery database of the service provider.

3. The utility provides the capability in which one or more PID equivalent fields (name, fate of birth, age, gender) from resident records in the service delivery database may be matched with equivalent fields in PID records from the reference database. The mapping thus created may be exported to Excel for further review and approval by a competent authority appointed by the service provider. The utility's match-and-seed functionality is limited only to the creation of the mapping and its export. Based on mapped data, the service provider may create custom Structured Query Language (SQL) scripts to update the service delivery database.

4. The utility also enables the validation of the seeding by performing demographic/biometric authentication using the eID authentication service. The ISCA registers with EIDAV to call eID authentication service.

Prerequisites to eID Seeding

The eID seeding process is necessarily preceded by data digitization and centralization.

Data digitization essentially means collation of service delivery data in an electronic format (database/Excel or similar) from where data can be retrieved using standard SQL queries from a Relational Database Management System (RDBMS) – the latter may be MySQL, SQL Server, Oracle, Sybase, DB2 or similar. It is also important that the personal identity data slowly become consistent across multiple systems. The EISDF is also an initiative to standardize personal identity information, and the eID data may be used to clean the existing data.

Data centralization primarily manages availability and accessibility of distributed service delivery data. The objective here is to allow the seeding utility to access the service delivery data and all related information in at least the read-only mode. For example, in Vietnam pensioners' data may be made available in data silos across districts. A consolidated view of the entire data may allow the Vietnam Social Security (VSS) to improve its service delivery while at the same time eliminate the problem of having one person avail of the same benefit from two different districts.

eID Seeding Strategies

The EISDF may support two ways of seeding the service delivery database with the eID/NIN: the top-down method and the organic method.

Top-Down method may use as input the resident PID captured at the time of enrollment for generating the NID and NID card, and the national population database available with GoV. In this method, the PID fields in the reference database created using the NID database are compared with the equivalent fields in the service delivery database in order to find a suitable match. Upon finding a match, the NIN from the reference database is seeded into the service delivery database of the service provider. Depending on the resident PID fields captured at the time of the enrollment in the NID system, the EISDF may support two possible scenarios for unique matching of resident record. Consider the example where the health insurance card number was captured in the resident data fields at the time of the enrolment in the NID system. The field health insurance card number, along with the resident's name, may then be used to find a matching unique record in the health insurance database maintained by the VSS.

Service Delivery Database

Health Insurance Card Number	NIN	Name	DoB	Province Code	Applicant No	Bank Code	Bank Name
1234523		Viet Huong Thảo	16-Aug-78	234	...	...	...
4453898		Hau Hung Vuong	12-Sep-76	234			
2545322		Trang Nguyen	2-Jan-65	234	...	...	...
4352893		Nam Luong	4-Feb-68	234	...	...	...
5423492		Hieu Duong	23-Apr-75	234			...
7354858		Hoang Trần	13-May-56	234	...	...	..

NIN	Name	Age	DoB	Address	Health Insurance Card Number
345674565234	Viet Huong Thảo	22	16-Aug-78	63 Ly Thai To, Hanoi, Vietnam	1234523
345676565678	Hau Hung Vuong	24	12-Sep-76	63 Ly Thai To, Hanoi, Vietnam	4453898
245678565123	Trang Nguyen	45	2-Jan-65	63 Ly Thai To, Hanoi, Vietnam	2545322
123674565234	Nam Luong	35	4-Feb-68	63 Ly Thai To, Hanoi, Vietnam	4352893
439667365834	Hieu Duong	38	23-Apr-75	63 Ly Thai To, Hanoi, Vietnam	5423492
534457456503	Hoang Trần	32	13-May-56	63 Ly Thai To, Hanoi, Vietnam	7354858

NID Card Enrollment Database

Another scenario could be a case where there are no extra fields captured during the enrollment for the NID card. In such a case, one or more PID fields may be used for matching. Consider the example of the service delivery database of the telecom provider with customer ID.

Service Delivery Database

NIN	Name	Age	DoB	Address	Mobile No
345674565234	Viet Huong Thảo	22	16-Aug-78	63 Ly Thai To, Hanoi, Vietnam	84-4 39346600
345676565678	Hau Hung Vuong	24	12-Sep-76	63 Ly Thai To, Hanoi, Vietnam	84-4 39346719
245678565123	Trang Nguyen	45	2-Jan-65	63 Ly Thai To, Hanoi, Vietnam	84-4 39312330
123674565234	Nam Luong	35	4-Feb-68	63 Ly Thai To, Hanoi, Vietnam	84-3 23446600
439667365834	Hieu Duong	38	23-Apr-75	63 Ly Thai To, Hanoi, Vietnam	84-4 39344321
534457456503	Hoang Trần	32	13-May-56	63 Ly Thai To, Hanoi, Vietnam	84-4 39231344

Customer No	NIN	Name	DoB	Address	Mobile No	Email	Plan Name
12434		Viet Huong Thảo	16-Aug-78	63 Ly Thai To, Hanoi, Vietnam	84-4 39346600	...	...
12342		Hau Hung Vuong	12-Sep-76	63 Ly Thai To, Hanoi, Vietnam	84-4 39346719	...	...
23453		Trang Nguyen	2-Jan-65	63 Ly Thai To, Hanoi, Vietnam	84-4 39312330	tra...	XYZ
22342		Nam Luong	4-Feb-68	63 Ly Thai To, Hanoi, Vietnam	84-3 23446600	....	...
34567		Hieu Duong	23-Apr-75	63 Ly Thai To, Hanoi, Vietnam	84-4 39344321	...	...
23123		Hoang Trần	13-May-56	63 Ly Thai To, Hanoi, Vietnam	84-4 39231344	...	...

Customer Table of Telecom Company's Database

As shown above, the PID fields (name, date of birth, address) from the NID enrollment database are matched with the PID equivalent field in the service delivery table and – based on match percentage of individual fields – an overall match score is calculated. It may be ideal to have a 100 percent match for seeding to take place, but that may happen rarely; therefore, it may be assumed that if the match score exceeds a predefined threshold (possibly 80 percent) then a match may take place.

The capture of additional information during NID enrollment could make seeding simple; it could be used for matching records between the PID and the service delivery tables whose unique identifier has been captured previously. The presence of a health insurance card number, an employment card number, or any other unique identifiers could prove beneficial to finding a match.

Organic method may require the service provider to contact the resident, or vice-versa, to update the NIN/eID in the service delivery database. It may involve creation of touchpoints where the resident voluntarily, or in response to service providers' call, initiates inclusion of his/her NIN/eID in the service delivery databases. This approach can be implemented in interactive or batch modes.

In the interactive mode, the resident may approach the service provider for the following reasons:

1. To avail of department-specific benefits scheme and/or services. The touchpoints could be in the field or in the service provider offices.

2. In response to a campaign by the service provider for NIN/eID registration to serve specific benefits and services.
3. The resident voluntarily approaches the service provider to register the NIN/eID for a specific service.

In the batch mode, the service provider gives the list of data pair (eID/NIN, KYR+) to be processed. The service provider could launch a new scheme where offline data entry is done with an application form submitted by the resident; it could also use the existing scheme for new enrollees.

The departments may leverage one or more channels of communication with the residents in order to capture their NIN/eID. Some of the channels that may be used are:

1. **Document Collection at Touchpoints.** Residents may hand over copies of their NID card and registration form with the service provider (e.g., for health insurance card). The service provider later updates the service delivery database based on the information supplied.

2. **SMS.** The service provider enables an SMS-based application. Residents are expected to send an SMS containing the NIN and a registration number to the service provider. For example: UPD <NIN> <Health Insurance Card Number> is sent to a number 59999 (illustrative only). The application at the back-end seeds the NIN into the database by using the health insurance card number as key. For the verification of information supplied, the service provider needs to conduct a demographic authentication after seeding.

3. **Operator-assisted Update at Touchpoints.** The service provider enables direct seeding of the NIN/eID at resident touchpoints where residents are expected to come along with supporting documents such as the NID card and a service registration document. A resident is authenticated both demographically and biometrically before the NIN is seeded in the service delivery database.

4. **Email.** Similar to the SMS-based approach, an email is sent in a pre-defined format along with scanned copies of supporting documents as attachments. Upon receiving the email, the back-end application extracts the required information from the email and seeds the database appropriately. In case of failure, the resident is informed by a reply email.

5. **Post/Courier.** This is similar to the previously mentioned document collection approach; however, in this case document collection takes place through the post/courier.

6. **Interactive Voice Response.** A telephone-based Interactive Voice Response (IVR) application captures the NIN and registration number in an interactive manner. Upon capturing the required information, the back-end application seeds service delivery database appropriately. Demographic authentication may be conducted after seeding for verification.

7. **Self-service Web Portal.** The service provider may open up a web portal for residents to update their beneficiary identifier number or account number, along with the NIN. Service providers may do a demographic authentication at the back-end before updating their database with the NIN/eID.

Common Seeding Challenges and Solutions

The eID Seeding services may be designed to address some of the common challenges during seeding. Below are some of the common challenges for which necessary processes or workarounds may be designed to overcome them.

1. **Complete data is not captured in service delivery databases.** Data are often entered manually by semi-skilled operators resulting in incomplete and incorrect entries in the service delivery database. Lack of an adequate Quality Assurance (QA) process by service providers also contributes to the problem. A data digitization strategy may address this potential issue.

2. **Similar information across different data sources do not have exact match between them.** It has been observed the same data across different tables are not entered similarly. Take the case of names “Hau Hung Vuong” and “H H Vuong” which refer to same person. Seeding may support exact/partial match of various data fields; therefore, such issues may be handled during data cleansing and normalization.

3. **Data in service delivery database is in Vietnamese.** Matching of data in the same language can be done with standard comparison algorithms, but if the information in the database is in different languages (e.g., English and Vietnamese) there is no way a match can be made. If a match could made, then the algorithms need to be made extremely intelligent and complex unless data level changes are made in the database.

4. **All the required data is not available.** Careful planning and coordination with support groups need to be done. As an example, codec information for encoding and decoding may be made available in cases where only codes are stored (often in the gender field, male is stored as 1 while female is 2).

5. **Normally available tools become incapable to handle high volume of data.** Normally people prefer using Microsoft Excel for data handling. However, it has been observed that after a few thousand records are entered into an Excel sheet, the response time of the tool deteriorates significantly. In such cases, alternative database tools may be considered; e.g., import data into a database (MySQL, MS SQL Server, Oracle, etc.).

6. **Mobilization of residents.** In the case of organic seeding, the mobilization of residents is required in order to complete seeding. A multi-channel organic seeding approach needs to be employed for effective mobilization.

II. Organizational Structure: Roles and Responsibilities

Electronic Identity Authentication Service

Responsibilities of the Electronic ID Authority of Vietnam

1. EIDAV could implement a mechanism to get the latest update on the PID of residents from the NID system of the NID system on a regular basis.

2. EIDAV could provide EISDF identity services such as authentication to ISCAs that wish to use them for establishing the identity of eID-/NID-holders before conducting business with the latter.

3. EIDAV could determine the operating and engagement model for EISDF identity services.

4. EIDAV could determine the rules regarding the use of eID, NIN and EISDF identity services.

5. EIDAV could determine the eligibility criteria for Managed Identification Service Providers (MISPs), facilitate the application and registration process and enter into contract with them.

6. EIDAV could determine the eligibility criteria for ISPAs, facilitate the application and registration process and enter into contract with them.

7. EIDAV could determine the eligibility criteria for ISCAs, facilitate the application and registration process and enter into contract with them.

8. EIDAV could determine standards and specifications that could be adhered to by all those participating in the EISDF identity services ecosystem – including ISPAs, ISCAs and sub-ISCAs. The standards and specifications could include systems and processes, and specifications pertaining to API, infrastructure (including devices), process, technology, certification (if applicable), audit, security and SLAs (if applicable). In summary, EIDAV could determine minimum standards and specifications for EISDF identity services, while ecosystem partners could extend and add more specifications and standards to meet their domain and application needs.

9. EIDAV could publish documents on its website giving the standards and specifications it prescribes. EIDAV could choose to certify all applications that could be used by ISCAs (and sub-ISCAs) to enable their eID authentication operations. This could include:
    a. Certification (by itself or through approved independent agencies) of applications (such as those driving the authentication process in the ISCA systems) that may be used by ISCAs and other participants in eID authentication.
    b. Certification of fingerprint and iris sensors, and extractor pairs that could be incorporated in authentication devices. It is the responsibility of vendors of relevant equipment to get their products certified by the Standardization Testing and Quality Certification (STQC) department of the Ministry of Information Technology (MIT).

10. EIDAV could reserve the right to conduct audits of all key players in the EISDF identity services ecosystem including ISPAs and ISCAs – either by itself or through EIDAV-appointed/approved independent audit agencies – to examine compliance with prescribed standards and specifications. As part of these audits, EIDAV/audit agency could inspect the premises, operations and systems, infrastructure, security, etc., of the entity being audited.

11. EIDAV could retain the right to take appropriate action against parties not complying with its specifications, including disqualifying them from using EISDF identity services system

or terminating their contract after an appropriate grace period for remedial action as specified in the respective contracts.

12. EIDAV could provide a framework for the dispute resolution mechanism of the EISDF identity services ecosystem.

13. In the future, if any charges are associated with EISDF identity services, EIDAV could decide on the charges or establish the framework for determining charges.

14. EIDAV could play any role, when necessary, to ensure that the system continues to offer uninterrupted services and run successfully.

Responsibilities of a Managed Identification Service Provider

The MISP's main area of responsibility includes EISDF Identity transaction operations (i.e., receive authentication requests, execute a match of PID received with the identity information on the CRIDS, and transmit the result) involving networks, data centers, availability of identity service, SLAs with ISCAs (if any) and monitoring of operations and performance metrics.

Responsibilities of an Identity Service Provide Agency

1. The ISPA adheres to its contract with EIDAV by complying with EIDAV standards and specifications, including the SLA if relevant.

2. The ISPA ensures that all its infrastructure and operations – including systems, processes, IT and biometric infrastructure, security, etc. – are compliant with EIDAV standards and specifications.

3. When the ISPA receives a service request such as authentication from an ISCA, it is recommended that the ISPA perform basic checks on the service request input before forwarding it to the EISDP server. The request is forwarded to the authentication server only if it is compliant and complete. Otherwise, it is returned to the ISCA with appropriate error message (which then forwards it to the authentication device with necessary instructions).

4. On receiving the response from the authentication server, the ISPA transmits the result of the transaction to the ISCA that placed the request.

5. It is highly recommended that the ISPA maintain a log of all identity transactions it processes. The log could be retained for a specified duration determined by EIDAV and may be shared with other entities, but only on a need-basis. The log may capture transaction details such as NIN, requesting ISCA, timestamp, etc., but not PID associated with an authentication transaction. The storage of the transaction log could comply with the applicable laws of the country.

6. In conducting its operations, the ISPA complies with all applicable laws and regulations in the country in the area of data security and management.

7. The ISPA ensures that its identity service systems are audited by an information systems auditor certified by a recognized body before commencing of its operations. The ISPA may provide a certified audit report to EIDAV from time to time confirming its compliance with prescribed standards, directions, specifications, etc.

8. The ISPA ensures that its operations and systems related to identity services are audited by an information systems auditor certified by a recognized body on an annual basis. The ISPA may provide a certified audit report to EIDAV from time to time confirming its compliance with prescribed standards, directions, specifications, etc. In addition, EIDAV may reserve the right to audit the ISPA (by itself or through EIDAV-appointed/approved agencies). During such audits, the ISPA cooperates fully with EIDAV/audit agency and provides access to its premises, procedures, records, systems, personnel and any other relevant part of its authentication operations. In case of non-compliance, EIDAV may take appropriate action such as termination of contract after an appropriate grace period for remedial action. The cost of the audits may be borne by the ISPA.

9. The ISPA keeps EIDAV informed of the list of ISCAs it serves. On entering into contract with a new ISCA, the ISPA informs EIDAV (along with details sought by EIDAV) before commencing service to the ISCA. Similarly, when an ISPA disengages with an ISCA, the ISPA informs EIDAV within seven days of the disengagement.

10. The ISPA may have a contract with the ISCA to provide any value-added services to the latter. However, such value-added services do not form part of identity services.

11. The ISPA is responsible to EIDAV for all its authentication related operations as covered in the contract between EIDAV and the ISPA. Even if the ISPA outsources part of its operations

to other entities, the responsibility for the operations and authentication results lies with the ISPA.

12. In case of investigation of an authentication-related fraud or dispute, the ISPA extends full cooperation to EIDAV (or its agency) and/or any other authorized investigation agency. This includes providing access to its premises, records, systems, personnel, infrastructure, any other relevant resource/information and any other relevant aspect of its authentication operations.

Eligibility Criteria

The eligibility criteria of an ISPA are enumerated below.

1. The agency may be:
    a. A central/provincial government ministry/department or its Public Service Undertaking (PSU) owned and manage by the central/provincial government; or an authority constituted under a central/provincial act; or a not-for-profit company/special purpose organization of national importance; or a company registered in Vietnam meeting the following requirements.
        i. Financial capabilities. An annual turnover of at least VND 100 million in the last three financial years.
        ii. Technical capabilities.
        iii. A Telecom Service Provider (TSP) operating pan-Vietnam fiber optics network and having a minimum of 100 MPLS Points of Presence (PoP) across all provinces; or a Network Service Provider (NSP) capable of providing network connectivity for data, voice transmission and having an agreement with a TSP that has 100 MPLS PoPs; or a System Integrator (SI) having the necessary arrangement with a TSP/NSP as described above.
    b. The agency has not been blacklisted by the central/provincial government, or any of its PSU, in the last five years.

2. The agency demonstrates its capability to undertake the design, configuration, implementation and maintenance of the infrastructure and systems required of an ISPA following EIDAV specifications; it certifies that the necessary human resources with the requisite skills are in place to perform its intended functions. The decision of EIDAV with regard to entering into contract – or not – with a potential ISPA could be final.

3. The ISPA may enter EISDF identity services ecosystem through the appointment process determined and conducted by EIDAV. Entities wishing to become an ISPA may apply with EIDAV by providing the necessary information along with supporting documents where relevant. EIDAV examines the application and approves qualifying applicants as ISPA. Approved ISPAs enter into contract with EIDAV and are permitted to build secure leased line connections to EIDAV authentication server; the connections comply with EIDAV standards and specifications.

4. Each ISPA contract may be for a specified duration, at the end of which an ISPA may be free to apply for a renewal. EIDAV evaluates the renewal application and approves the renewal of qualifying applications.

Responsibilities of an Identity Service Consumer Agency

1. The ISCA informs EIDAV of each transaction it wishes to have an authentication service performed on and the appropriate authentication type it wishes to avail of. The choice of authentication type indicates the specific identity information to be sought from the eID-/NID-holder to enable that service. The choice of authentication type is a decision of the ISCA alone; none of the other entities, including EIDAV and its ISPA, are responsible for this decision. It is possible for an ISCA to change the authentication type of any service if it so desires, and makes it known to EIDAV.

2. The ISCA adheres to the processes and the ISCA onboarding checklist provided by EIDAV for getting started with EISDF identity services. As and when there are any changes in the parameters, the ISCA keeps EIDAV informed of the list of its services that are enabled by authentication. This process may be done in a self-service mode, such as an online update through EIDAV portal.

3. The ISCA establishes its identity services-related operations (including systems, processes, technology, infrastructure, security, etc.) in compliance with EIDAV standards and specifications.

4. The ISCA is responsible for the provisioning of network from authentication devices to the ISCA server and between the ISCA and ISPA servers; it ensures compliance with EIDAV security specifications. In addition, it is responsible for procuring and deploying any hardware/software/certificate/etc. that are compliant with eID authentication standards.

5. The ISCA ensures that devices used for eID authentication are procured, deployed, and managed by them or their agent(s) in compliance with EIDAV specifications and standards published by EIDAV from time to time.

6. The ISCA logs all its identity service transactions and maintains them for a specified period of time. The log may capture details of an authentication transaction, but not the corresponding PID. The storage of transaction logs could comply with applicable laws and regulations of the country. The details of logs stored, the duration of storage and any other aspect of data storage could be determined by EIDAV specifications, regulations applicable to the ISCA service and industry, the ISCA's own requirements and other applicable laws and regulations.

7. It is highly recommended that the ISCA deploy a Fraud Analytics module that is capable of analyzing identity services-related transactions to identify fraud cases and patterns. If the ISCA is a victim of a fraud, or identifies a fraud pattern through its Fraud Analytics system, it shares all necessary information with EIDAV.

8. The encrypted PID block may not be stored, unless it is for buffered authentication for only a short period of time; and after transmission, it is deleted. Biometric and OTP data captured for the purposes of eID authentication may not be stored on any permanent storage or database. The ISCA ensures that all relevant laws and regulations are adhered to in relation to data storage and data protection in their systems; it also ensures that their agents (if applicable) and authentication devices are in compliance.

9. In cases where the authentication devices are operated by ISCA personnel (or that of its agent), it is the ISCA's responsibility to ensure that adequate training on the operation is given to its service representatives.

10. The ISCA ensures that its eID authentication systems are audited by an information systems auditor certified by a recognized body before commencing its operations; the ISCA provides a certified audit report to EIDAV confirming from time to time its compliance with prescribed standards, directions, specifications, etc.

11. The ISCA ensures that its eID authentication operations and systems are audited by an information systems auditor certified by a recognized body on an annual basis to confirm compliance with EIDAV standards and specifications; the audit report is shared with EIDAV

upon request. It is the ISCA's responsibility to ensure that its sub-ISCAs and agents are also audited regularly. In addition, EIDAV may reserve the right to audit the ISCA's operations and systems (and their agents, if applicable) by itself or through its appointed auditor. During these audits, the ISCA cooperates fully with the audit agency and provides them necessary access to its premises, procedures, records, systems, personnel and any other relevant aspect of authentication operations. In case of non-compliance, EIDAV may take appropriate action (such as termination of a contract after a suitable grace period for remedial action). The cost of these audits may be borne by the ISCA.

12. The ISCA is responsible for identifying exception-handling mechanisms and back-up identity authentication mechanisms when the eID-based federated authentication fails. Authentication failures may occur in the process, infrastructure (including power, IT, devices, network connectivity), or biometric reading (where the eID-holder's biometric data cannot be acquired or used for some reason).

13. When an ISCA partners with a sub-ISCA, the ISCA informs EIDAV of the partnership before starting to serve the new sub-ISCA. Similarly, when a sub-ISCA disengages with the ISCA, the ISCA informs EIDAV within seven days (or a period specified by EIDAV) of disengagement. The process of such updates is envisaged to be in a self-service mode (such as an online update through EIDAV portal). When an ISCA engages with a sub-ISCA, it generates a sub-ISCA code to identify the specific sub-ISCA. When informing EIDAV of its engagement with the sub-ISCA, the ISCA also informs EIDAV of the new sub-ISCA code. When transmitting identity service requests from a sub-ISCA, the ISCA always includes the sub-ISCA code so that the eID authentication transaction log can track the origin of all authentication requests. It is necessary that for each sub-ISCA, a separate license key is used so that the engagement and disengagement of sub-ISCAs can be easily accomplished by creating and revoking their respective license keys.

14. It is the ISCA's responsibility to ensure that all sub-ISCAs under it are regularly audited for compliance with EIDAV specifications. In case of non-compliance or default, the ISCA may report it to EIDAV and take correction action according to EIDAV guidelines.

15. When an ISCA engages a sub-ISCA, from EIDAV perspective, the ISCA is responsible for the connectivity between the sub-ISCA's authentication devices and the ISCA systems.

16. Even if the ISCA outsources part of its operations to third party, the responsibility for the identity services operations and results lies with the ISCA. The ISCA is also responsible for ensuring that the identity service operations of the third party comply with EIDAV standards and specifications, and that they are regularly audited by approved independent audit agencies.

17. In case of investigation of an authentication-related fraud or dispute, the ISCA extends full cooperation to EIDAV (or its agency) and/or any other authorized investigation agency. This includes providing access to its (and, if applicable, their agents') premises, records, personnel, systems, relevant resource/information and any other relevant aspect of authentication operations.

18. An ISCA proactively informs EIDAV of any misuse of eID data, authentication services, or any compromise of eID-related data or systems within its network.

Eligibility Criteria

The eligibility criteria of an ISCA are enumerated below.

1. The agency may be:
    a. A central/provincial government ministry/department or a PSU owned and managed by the central/provincial government; or an authority constituted under a central/province act; or a not-for-profit company/special purpose organization of national importance; or a bank/financial institution/telecom company.
    b. A legal entity registered in Vietnam that seeks to use eID authentication to enable its services. Applications from such agencies may be considered and approved by the ISCA approval board to be constituted by EIDAV.

2. The agency demonstrates the capability to undertake the implementation and maintenance of the infrastructure and systems required to become an ISCA. The decision of EIDAV regarding engagement of an ISCA could be final.

3. Agencies seeking to use eID authentication to enable their services may apply with EIDAV by providing the necessary information along with the required supporting documentation, as well as the information on the ISPA through which the ISCA could connect to the authentication server.

4. On receipt of the necessary information (and documentation, if relevant), EIDAV approves an ISCA. On approval, the ISCA and EIDAV enter into contract.

Responsibilities of a Sub-ISCA

The responsibilities of a sub-ISCA could be similar to that of an ISCA. The responsibilities of an ISCA covered above could be applicable to the sub-ISCA as well.

Eligibility Criteria

1. An entity desiring to become a sub-ISCA identifies the ISCA it wishes to engage with and applies with that ISCA by providing the necessary information and supporting documentation, if necessary.

2. The sub-ISCA commits to comply with EIDAV standards and specifications in their eID authentication operations.

3. The ISCA informs EIDAV of the engagement with the sub-ISCA and commences its services to the latter.

Authentication Devices

Deployment Criteria

1. Authentication devices may be deployed in the eID authentication ecosystem by the ISCA, sub-ISCA or the agents of ISCA/sub-ISCA or the eID-holder.

2. The ISCA/sub-ISCA is responsible for the provision of network from devices to the sub-ISCA/ISCA server and on to the ISCA/ISPA server; it is also responsible for ensuring network security. In addition, they may be responsible for procuring and deploying any hardware/software/certificate/etc. that comply with eID authentication standards.

3. The ISCA/sub-ISCA is responsible for the installation of eID authentication standards-compliant hardware/software/certificate/etc. on the Internet-connected device of their customers/beneficiaries/subscribers (CBS).

Features of Authentication Devices

1. They are compliant with EIDAV standards and specifications.

2. Biometric authentication devices are compliant with EIDAV biometric data standards and are certified to be so by the designated department in the government.

3. Biometric authentication devices employ “best finger” detection exposed by the EISDP.

4. Biometric authentication device vendors equip their product using Software Development Kit (SDK) Application Programming Interface (API) specification published by EIDAV to ensure interoperability.

5. Authentication devices may be operator-assisted or self-operated.

6. They are capable of collecting relevant information from NID-/eID-holders, preparing authentication data packets (PID block), performing structural validation of data, transmitting data packets and receiving authentication results along with instructions on next steps, if any. Collection of eID information by the authentication devices is carried out in compliance with EIDAV specifications.

7. Authentication devices are deployed such that they cannot retain eID-holders’ biometric and OTP data captured for the purposes of eID authentication during a transaction, except in case of buffered authentication described below, in which case they may be able to store encrypted data for a certain period of time.

8. In terms of data storage, authentication devices comply with all applicable laws and regulations of the country.

Responsibilities of the eID-/National ID-holder

1. eID-/NID-holders consent to be authenticated with their eID-based PID and present it voluntarily to access the ISCA/sub-ISCA services.
2. It is the eID-/NID-holders’ responsibility to keep their PID in the CRIDS valid and current. They do so on a periodic basis or on a need-basis, as the case may be. Some instances where an update may be necessary:
    a. To inform releavant GoV agencies of a change in address
    b. To update the collection of fingerprints on a periodic basis
    c. To correction any errors

3. eID-/NID-holders may approach EIDAV in case they have reason to believe that their eID PID has been compromised by any of the agents in the authentication ecosystem.
4. eID-/NID-holders proactively inform EIDAV of any misuse of eID data or authentication services.

The rights, responsibilities and obligations of eID-/NID-holders are covered in detail in the eID-/NID-holder's Charter.

Eligibility Criteria

Eligible individuals seeking eID identity enter the eID authentication ecosystem when they enroll with the NID system by providing their demographic and biometric identity information. On successful completion of the enrollment process, each eligible individual obtains his/her unique NIN. This identity information is stored against the corresponding NIN in the CRIDS.

eID Seeding Service

The operating model for eID seeding service could be managed and operated by the following EISDF organizational structure entities that could have well-defined roles and responsibilities. The key roles and responsibilities are described below:

1. The **National Identification Authority of Vietnam** could provide the necessary tools, expertise, best practices, and consulting advisory on request to the service providers for implementing the eID seeding, such as:
    a. Seeding utility and the National Electronic Seeding Platform (NESP) for use by the service providers.
    b. Necessary documentation on its public portal.
    c. Online registration on its public portal for ISCAs to access relevant tools.

2. The **Identity Service Consumer Agency** could be a service provider interested in availing of identity verification functions for use in its service delivery process; it could be responsible for the seeding of the NIN/eID in its service enablement database. Among its responsibilities are:
    a. Preparing its service enablement database by performing data digitization and centralization.
    b. Choosing its seeding strategy: top-down or organic method.
    c. Registering with EIDAV for using the offline utility and NESP.

d. Performing the demographic and biometric authentication using eID authentication.
e. Setting up the required communication channels with the CBS, if using organic seeding.

eKYC Service

The operating model for the eKYC process may be managed and operated by the same organizational structure entities involved in the eID authentication service. The key roles and responsibilities from the eKYC perspective are described below.

1. **National Identification Authority of Vietnam.** As in eID authentication, the NIDAV could be the overall regulator and overseer of the eKYC process and supporting ecosystem. Its functions:
    a. To provide eKYC access to ISCAs wishing to use it in business operations as a prerequisite extending their service to eID-/NID-holders.
    b. To determine the operating and engagement model for the eKYC.
    c. To determine the rules regarding the usage of eKYC.
    d. To ensure that the eligibility criteria for the MISP include the design and implementation of the eKYC as part of the responsibilities.
    e. To determine the eligibility criteria and entry process for ISCAs to access the eKYC service, facilitate the application and registration for its use, then enter into contract with them.
    f. To determine the standards and specifications that could be adhered to by all (including ISPAs, ISCAs and sub-ISCAs) that participate in the eKYC ecosystem. The standards and specifications include systems and processes; it also includes specifications for API, infrastructure, devices, processes, technology, certification (if any), audit, security, and SLAs (where applicable). In summary, the NIDAV could determine the minimum standards and specifications for eKYC, while ecosystem partners may extend and add other specifications and standards to meet their domain and application needs.
    g. To publish documents on its website on eKYC-related standards and specifications it prescribes. The NIDAV could choose to certify all applications that could be used by ISCAs (and sub-ISCAs) in enabling their eKYC operations – by itself or through approved independent certification agencies.

2. **Managed Identification Service Provider.** The MISP could offer eKYC service on behalf of the NIDAV. Its main area of responsibility could include eKYC transaction operations (i.e., receive authentication request, execute a match of PID received by calling eID authentication service and transmit the result), network and data center operations, availability of eKYC service, SLAs with ISCA (if any) and monitoring operations and performance metrics.

3. **Identity Service Provider Agency.** The sole channel to the eKYC process could be through the secure leased line network of an ISPA.

4. **Identity Service Consumer Agency.** The ISCA could be any agency that seeks to use the eKYC service to enable its service delivery. Each ISCA may use the eKYC process to enable one or more of its services. An ISCA enters into a formal contract with the NIDAV in order to access it. The ISCA ensures that the eKYC request originating from its device is compliant with the standards and specifications prescribed by NIDAV and duly completed before transmission to its ISPA.
    a. The eKYC service delivery workflow requires a call to the authentication service for getting the consent of the resident. Hence the ISCA, in addition to its eKYC service responsibilities, could also have all the responsibilities involved in the delivery of authentication service.
    b. The ISCA adheres to the processes and the ISCA onboarding checklist provided by NIDAV for getting started with the eKYC service. As and when there are any changes in the parameters, the ISCA keeps the NIDAV informed of the list of its services that are enabled by eKYC. This exercise may be done in self-service mode, such as an online update on the NIDAV portal.
    c. The ISCA may up its eKYC-related operations (including systems, processes, technology, infrastructure, security, etc.) in compliance with NIDAV standards and specifications.
    d. The ISCA may use the network provided by the ISPA between Identity service devices, and ISCA and ISPA servers, for authentication service. In addition, it could be responsible for procuring and deploying any hardware, software, certificate, etc., in compliance with eKYC standards.
    e. The ISCA logs all its eKYC transactions and maintains them for a specified period of time. The log captures details of an eKYC transaction, but not the corresponding PID. The storage of transaction log complies with applicable laws and regulations of the country. Details of the log stored, the duration of storage and any other

aspect of data storage could follow NIDAV specifications, regulations applicable to the ISCA service and industry, the ISCA's own requirements and other applicable laws and regulations.

f. The Fraud Analytics module deployed by the ISCA could be capable of analyzing eKYC-related transactions to identify fraud cases and patterns.
g. In cases where the Identity service devices are operated by ISCA personnel (or their agents'), the ISCA could be responsible for ensuring that it gets adequate training for performing eKYC-related tasks.
h. The ISCA ensures that its eKYC-related systems are audited by an information systems auditor certified by a recognized body before commencing operations; the ISCA provides a certified audit report to the NIDAV from time to time confirming its compliance with prescribed standards, directions, specifications, etc.
i. The ISCA is responsible for identifying exception-handling and back-up mechanisms when the eKYC function fails. Failures may occur in the process, infrastructure (including power, IT, devices, network connectivity) or biometric reading (where eID-holder's biometric data cannot be acquired or used for some reason).
j. When transmitting eKYC requests from a sub-ISCA, the ISCA always includes the sub-ISCA code so that the log can track the origin of all transactions.
k. Could the ISCA outsource part of its operations to third party entities, the responsibility for the eKYC operations and results could still lie with the ISCA. The ISCA could also be responsible for ensuring that the eKYC-related operations such as those performed by third party entities comply with NIDAV standards and specifications. The ISCA could likewise ensure that the third party entities are regularly audited by approved independent audit agencies.
l. In case of investigation of an eKYC-related fraud or dispute, the ISCA extends full cooperation to the NIDAV (or its agency) and/or any other authorized investigation agency. This includes providing access to its premises, records, personnel, systems, relevant resource/information and any other relevant aspect of authentication operations – as well as those of its agents.

5. **Sub-ISCA.** Any legal entity registered in Vietnam wishing to use eKYC service to enable its services could become an ISCA or it could access it through an existing one. In the latter case, it becomes a sub-ISCA of the ISCA it engages with.

6. **Identity Service Device.** It may be the same device as that used for eID authentication and it could have the capability to capture the inputs required by eKYC service. It could be operator-assisted or self-operated. The device may be a desktop, laptop, kiosk, handheld mobile, etc., that are – if required – integrated with or connected to biometric tools for capturing fingerprints and/or iris images. It could be operated by the ISCA or a sub-ISCA, or agents of the ISCA/sub-ISCA.

7. **eID-/NID-holders.** In the context of eKYC service, they are usually associated with ISCAs or sub-ISCAs as customers, employees or associates; as such, they seek access to ISCA/sub-ISCA services. For them to gain access, they need to provide their KYC data for registration in the eKYC service. The eID-/NID-holders are responsible for providing consent to the eKYC process.

Mobile ID Service

Mobile Phone with Specialized SIM

A mobile phone with specialized SIM has SSCD capability, activated digital certificate or biometrics, and a private key. It is issued by the RA and hosts the mobile service request application and the private keys stored on the SIM.

Responsibilities of a Registration Authority

The RA could typically be a nationalized mobile operator such as Vittel, Mobiphone, Vinaphone, etc., responsible for the provisioning of specialized SIMs with SSCD functionality to residents at its service outlets across the country. For a mobile operator to become an RA, it could have to register with EIDAV.

The RA could be responsible for user registration and certificate activation of mobile ID service provided to residents. It could also be responsible for termination of service due to such reasons as resident's request, lost/compromised SSCD, certificate expiry, or violation of the user-CA agreement.

Responsibilities of a Trusted Service Provider

The Trusted Service Providers (TSPs) could be the mobile operator responsible for forwarding the mobile ID service request from EIDAV to the mobile phone of the resident over the mobile network. It could also be responsible for sending the signed data from the mobile phone to the CA, and getting back to EIDAV with the authentication response.

Mobile operators may have to register with EIDAV to become an authorized TSP. The TSP provides the wPKI service to EIDAV and the ISCAs and it could be responsible for monitoring PKI-related problems and providing support for their resolution.

Responsibility of a Certification Authority

The CA could be responsible for issuing and validating the certificate; it could also validate the signed data in response to the TSP request.

Responsibility of the Electronic Identification Authority of Vietnam

EIDAV could host the mobile ID service in its data center, and register and hire all the ecosystem entities that could play roles in this scalable delivery of services.

Responsibility of an Identity Service Consumer Agency

The ISCA could be any agency seeking to use mobile ID functions to enable its services. Each ISCA may use mobile ID to enable one or more of its services. The ISCA could be responsible for integrating its service delivery application (websites) to the mobile ID service provided by EIDAV.

Responsibilities of an Identity Service Provider Agency

The ISPA may be an agency that establishes secure leased line connectivity with the mobile ID service hosted on the mobile ID servers in EIDAV data center. It transmits authentication requests on behalf of an ISCA and receives the response back from the mobile ID server.

Responsibilities of a Resident User

The resident may obtain the specialized SIM from the RA service outlet. To acquire one, the resident could have to provide his/her NIN and demographic data to allow verification of identity through authentication at the RA service outlet. The resident could validate his/her identity-related data on the mobile phone during the registration process after which, the resident acquires the PIN and activation code. Henceforth, the resident could be responsible for the card.

Annex 5: International Experiences

Many countries have launched the national Electronic Identity (eID) system and are at various stages of deployment and usage. Since many nations have only recently begun their rollouts, adoption levels are expanding daily as more citizens receive their eID and government agencies and businesses launch new services that make use of this platform. While no country has achieved universal adoption and use, some countries have made more progress than others. This section identifies the various eID services implemented by three countries, notably India, Estonia and Belgium; and how the eID has improved the quality of citizen/customer service delivery. It also looks at the experiences of these countries and highlights the key factors that have impacted the successful implementation and increased usage of the eID system.

I. India

1. In India, an inability to prove identity was one of the biggest barriers preventing the poor from accessing benefits and subsidies. The Government of India did not provide a national identification document with a unique number to the residents. In the absence of resident identity creation at the national level, service agencies typically followed their own process for identity creation and entitlement identification for their customers/beneficiaries/subscribers (CBS). The tokens provided by service agencies to individuals were used for both identity authentication and entitlement verification. As part of the identity creation process, most of the service agencies required the individuals to furnish physical identity documents or service utilization bills provided by other service agencies like Permanent Account Number (PAN) card, passport, driver's license, telephone bill, etc. Only 50 million Indians had a passport, close to 100 million had a PAN card, and approximately 200 million had a drivers' license, but there was a vast section of the population who did not have any identity proof. This approach resulted in a situation where a part of the population had multiple identity tokens, while a significant portion did not have any at all as they did not avail any of those services. Also, only certain identity tokens were accepted as identity proof at the national level, e.g., PAN card, passport, and ration card. In order to achieve the goal of financial inclusion and reduce the poverty within the country, it was felt there needed to be an identification system to cover those who did not possess any proof of identity so that they could participate in the social programs and avail of benefits they were entitled to.

2. The move to have an identity creation system resulted in the following challenges:
   a. Multiple identities for the same person due to the lack of a national mechanism to uniquely identify an individual.

b. Limited or no interoperability as most of the identity tokens were accepted for a specific purpose and at a specific location only.
c. Leakages of welfare benefits owing to the creation of numerous duplicates and fake identities within the same benefit program as it was impossible to uniquely identify the individuals.
d. High risk of resident identity theft and misuse of photocopied identity documents submitted as proofs, it being easy to forge paper-based documents.
e. Duplication of effort in identity creation in silos by each service agency increased overall cost of identification, and caused extreme inconvenience to the individuals.
f. Creation of separate identity for each program for the same individual results in service agencies unable to correlate different benefits given to an individual through various programs resulting in the inability to verify correct entitlements and a potentially lower impact from welfare programs.

3. Most of the service agencies issued physical identity tokens of the "what the user has" type like cards for PAN, ration, pension, National Rural Employment Guarantee Scheme (NREGS), etc., which can only be authenticated manually. This identity authentication mechanism presented the following challenges:

a. Higher setup cost with limited scalability. It works only in the assisted mode.
b. Difficulty in identifying fake documents and copies.
c. Inability to verify that the person carrying the token is the rightful owner unless it carries the person's photo.
d. Difficulty in recognizing misuse – there is no authentic audit trail mechanism; instead it requires exhaustive manual checking.

4. Given this context, the Government of India embarked on the **Unique Identification** (UID) project in January 2009 with the mission to issue a unique identification number that became known as **Aadhaar**. The Aadhaar may be verified and authenticated in an online cost-effective manner that is robust enough to eliminate duplicate and fake identities.

5. The Aadhaar identifies a resident and provides the resident the means to clearly establish his/her identity to public and private agencies across the country. The three key characteristics of Aadhaar are: (a) permanency (it remains the same throughout an individual's lifetime); (b) uniqueness (one resident has one ID; no two residents have same); and (c) globalness (the same identifier can be used across applications and domains).

6. The Aadhaar is provided during the enrollment process when a resident's demographic and biometric information are collected and the uniqueness of the data is established through a process called deduplication. Post deduplication, an Aadhaar number is issued and a letter is sent to resident informing of the details.

7. The **Unique Identification Authority of India** (UIDAI) has adopted the use of biometrics technology as part of its core strategy in meeting its goal of preventing issuance of duplicate identity number to a resident. The biometrics used are fingerprint and iris scans. The deduplication process involves matching the biometric data of the resident against those of every resident in the database to ensure uniqueness. Only after this process is a 12-digit Aadhaar number issued.

8. For any service agency, establishing both identity and service entitlement of the beneficiary is necessary. Though individual identity may be unique and independent of services desired, entitlement is very specific to the service being availed of and it has to be established by each service agency separately. Hence, instead of assigning the role and responsibilities of the authentication service to an existing ministry, the UIDAI was created as the overall regulator and overseer of the Aadhaar authentication system.

9. The UIDAI was established under the Planning Commission. It was created by an executive order under the aegis of the Planning Commission to ensure a pan-departmental and neutral identity for the authority and, at the same time, enable a focused approach to attaining the goals set for the Eleventh Five-Year Plan that covered 2007-2012. Its role was to develop and implement the necessary institutional, technical and legal infrastructure to issue unique identity numbers to Indian residents. The UIDAI was created as a statutory body under a separate legislation to fulfill its objectives. The law also stipulates rules, regulations, processes and protocols to be followed by the different agencies partnering with the UIDAI in issuing and verifying unique identity numbers.

10. The UID only provides identity[19]. The UIDAI purview is limited to the issuance of a unique identification number linked to a person's demographic and biometric information. It is not responsible for issuing the card. The UID may only guarantee identity, not rights, benefits or entitlements.

---

[19] http://uidai.gov.in/UID_PDF/Front_Page_Articles/Documents/Strategy_Overveiw-001.pdf

11. The UID number does not contain intelligence. Loading intelligence into identity numbers makes them susceptible to fraud and theft. The UID is a random number.

12. A steering cabinet committee headed by the Prime Minister and a group of ministers from key ministries such as Finance, Agriculture, External Affairs, Law and Justice, Communication and Information and Technology, and Labor and Employment among others, was constituted with the function of managing all issues related to the UIDAI, including its organization, plans, policies, programs, schemes, funding and methodology to be adopted for achieving the objectives of that authority.

13. The project included the establishment of the national identity infrastructure for the creation and usage of the national unique identity that is digital and verifiable online. It addressed the existing challenges faced by service agencies in identity establishment. Following are its key benefits.

a. Since it works anywhere in India, it is portable identity that is verifiable online.
b. It does away with duplicate and fake identities thereby plugging leakages of welfare benefits.
c. It authenticates the individual every time as that same and unique person anywhere and anytime; therefore, it ensures that the rightful claimant gets the service or benefit.
d. It has higher scalability of services with online authentication, allowing the service agencies to use multiple channels for service delivery.
e. It reduces beneficiary harassment and rent seeking due to lower dependency on manual processes.
f. It is a more efficient service delivery process and reduces the cost of identity establishment.
g. It eliminates the need to submit physical copies of identity documents and reduces the risk of identity theft associated with physical documents usage.
h. It has a built-in electronic audit trail allowing service agencies to track their service delivery process more effectively.

14. The UID proves identity, not citizenship. The UID is proof of identity and does not confer citizenship.

15. The previous identity databases in India were fraught with problems of fraud and duplicate or ghost beneficiaries. To prevent this from seeping into the new database, the UIDAI decided not to use the data that existed previously. Instead, it undertook a new enrollment process for

the proper collection and verification of residents' demographic and biometric information. This ensured that the data collected is clean from the start of the program.

16. The UIDAI introduced the "introducer system" for residents who do not have any form of identification and where the UID could be the first form of identification they have access to. This was to enable financial inclusion so that much of the poor and underserved population could get a UID. The introducer could be a person who stands as the guarantor of a resident's personal demographic data in the UID system.

17. The main service offered to the residents and service providers in both public and private organizations is Aadhaar authentication. The purpose of authentication is to enable Aadhaar-holders to prove their identity digitally and online, and for service providers to confirm the residents' identity claim before supplying services or giving access to benefits.

18. Typically, an individual identity is defined in terms of demographic attributes, i.e., name, gender, age and address. But demographic data alone cannot guarantee uniqueness. Uniqueness of identity, however, is possible by linking demographic attributes with biometric attributes like fingerprint and iris patterns of the individual. Aadhaar is a unique 12-digit randomly generated identity number assigned to the resident. It is linked to the resident's unique personal demographic and biometric data stored in the centralized database, the **Central Identities Data Repositoty** (CIDR). For the sake of uniqueness, there is one identity number to one person, and one person has one unique identity number. To achieve this, the resident profile is run through a rigorous demographic and biometric deduplication process with 99.99% accuracy before assigning the unique identity number to the resident profile.

19. The incentives in the UID system are aligned towards a self-cleaning mechanism. The past patchwork of multiple databases in India gave individuals the incentive to provide different personal information to different agencies. Since deduplication in the UID system ensures that residents have only one chance to be in the database, individuals are encouraged to provide accurate data. This incentive may become especially powerful as benefits and entitlements are linked to the UID.

20. **Aadhaar authentication**[20] is the process in which the unique identification number, along with the holder's Personal Identity Data (PID), is submitted to the CIDR at UIDAI for matching,

[20] Aadhaar Operating Model - http://www.uidai.gov.in/images/authDoc/d3_1_operating_model_v1.pdf

following which the CIDR verifies the correctness on the basis of the match with the Aadhaar holder's identity information available with it. The UIDAI either confirms proof of identity or verifies the information provided by the resident. To protect resident privacy, the Aadhaar authentication service responds only with "yes/no"; none of the PID is mentioned in the response.

21. The authentication services are available to the resident to prove his/her identity anywhere, anytime and in multiple modes. A service provider can choose either single-factor or multi-factor authentication. The Aadhaar, by itself, is not a factor for authentication. The Aadhaar, along with demographic attributes (name, address, etc.) or One-Time-Password (OTP) or single/multiple biometric attributes (fingerprint, iris, etc.), may be used to provide single-factor authentication. Alternatively, the three attributes may be used in combination for a multi-factor authentication process.

22. Authentication services are of different types[21] depending on the authentication attributes used.

a. **Type 1: Demographic.** This uses demographic attributes (name, address, date of birth/age, gender, mobile, email) singly or in combination. It can be used periodically to check validity of the credential,s or for cleaning up the service provider database by removing duplicates.
b. **Type 2: OTP.** This uses a one-time password that is delivered to a mobile number or email address on request initiated by a resident or an application. It may be used for authenticating residents for Internet and mobile transactions, as well as in cases where deployment of biometric technology is difficult or not practical.
c. **Type 3: Biometric.** This uses fingerprint and/or iris scans. It requires residents to be present to allow fingerprint and iris capture on a device. It is used when biometric authentication is considered essential as in Know-Your-Customer (KYC) process, financial transactions, attendance tracking, etc.
d. **Type 4: Multi-factor.** This uses biometric scans and OTP/mobile. As it is a multi-factor authentication, therefore, it provides greater assurance.

[21] Aadhaar Authentication Framework - http://www.uidai.gov.in/images/authDoc/d2_authentication_framework_v1.pdf

23. The features[22] in the Aadhaar authentication service include demographic and biometric data matching. It also offers OTP usage, "yes/no" response, digitally signed request/response, response code, response timestamp, self-verifiability of response, encryption and tamper-proofing.

24. **Federated Mode of Aadhaar Authentication.** Most current authentication systems could be described as "local" (i.e., pertaining to and/or valid for a few services, situations or entities) and "revocable" (in which an existing identity factor could be revoked and reissued as a result of expiry, compromise or other valid reasons). Such revocable, local authentication systems come with a set of strengths and limitations. The Aadhaar authentication system, on the other hand, could be described as "global" due of its applicability across situations, service providers and services. It is also "non-revocable" since Aadhaar identity factors, such as fingerprints and iris scans, cannot generally be revoked or replaced. Global, non-revocable/permanent authentication systems come with their own set of strengths and limitations. In the federated authentication model, the global-irrevocable Aadhaar authentication co-exists with and strengthens the local-revocable kind done by authentification user agencies. It is expected that such a federated approach may result in authentication systems that are stronger and more reliable than those that are based solely on either the global-irrevocable model or the local-revocable model. Aadhaar authentication has been designed with the view to strengthening the service providers' existing authentication systems, rather than as a replacement. While the federated model does not mandate the existence or use of a service provider's own authentication (if a service provider so wishes, it could use only Aadhaar authentication by itself), service providers are encouraged to use Aadhaar authentication in conjunction with their own local authentication to render the overall authentication system stronger and more reliable. This is called the federated mode of Aadhaar authentication.

25. Aadhaar and identity authentication are used by the service delivery provider mainly for establishing presence and proof of delivery, KYC credentials, and as a unifier for resident-centric information.

26. In the case of establishing presence and proof of delivery, confirming beneficiaries is a common usage of the authentication services that ensures that the services are delivered to the right individuals. It supports attendance tracking in the cases where wages/outlays are linked to

---

[22] Aadhaar Enabled Service Delivery
http://uidai.gov.in/images/authDoc/whitepaper_aadhaarenabledservice_delivery.pdf

the actual number of days a beneficiary reports for the program. It also facilitates financial transactions as when a bank authenticates a customer using Aadhaar as well as bank-related identity information (account number/user ID along with OTP, etc.) before enabling fund transfers or withdrawals.

27. In the case of establishing KYC credentials, Identity and address verification is a key requirement for enrolling a new customer or opening a new account for an individual. The service provider in all such cases can verify applicant identity and address using Aadhaar authentication. This is expected to substantially reduce the cost of KYC in providing these services. It can also be used as a general Proof of Identity (PoI) for standard security-related requirements such as entry to areas like airports; and in various examinations (medical or scholastic) where a large number of impersonations are reported every year. The application of authentication in demographic data and address verification in service delivery databases may help in their cleansing and management.

28. The Aadhaar is a common identifier to link related databases. It enables the State view of residents across schemes, e.g., the number of schemes accessed by a resident. It provides a potential linkage of Janani Suraksha Yojana (JSY), a government scheme to decrease neo-natal and maternal death; Integrated Child Development Services (ICDS); and Sarva Shiksha Abhiyan (SSA), an education program. A linking of services could facilitate the tracking of health and education for every child, healthcare and patient records database (local, regional and national levels); credit bureaus could be able to avail of customer rating information; there could be a national skills registry and tracking of individuals through the lifecycle; and large institutions could have a single customer view across services provided by banks, insurance companies, etc.

29. The UIDAI has defined a scalable operating model with key players, their roles, responsibilities and obligations in the Aadhaar authentication model[23]. Any agency that could like to utilize Aadhaar authentication to enable its services may sign up as an **Authentication User Agency** (AUA) and enter into an agreement with the UIDAI. The AUA in turn may need to engage with an **Authentication Service Agency** (ASA). An ASA is an agency that has established secure leased line connectivity to the CIDR at the UIDAI to transmit authentication request on behalf of AUAs and receive response back from the CIDR. The ASAs build and maintain their secure connectivity to the CIDR in compliance with the standards and specifications set by the UIDAI. An AUA has the option of connecting to the CIDR by itself or through an existing ASA. Further, an

[23] Aadhaar Authentication Operating model - http://www.uidai.gov.in/images/authDoc/d3_1_operating_model_v1.pdf

agency desiring to use Aadhaar authentication could choose to become an AUA or it could choose to access the authentication services through an existing AUA. In the latter case, it becomes a sub-AUA of the AUA it engages with.

30. Terminal devices are devices employed by AUAs (both government and non-government) to provide services to the residents. Examples include micro-ATM devices, Point of Sales (PoS) devices, Position Detection System (PDS) terminals, and MGNREGA (a program which guarantees the right to work), terminals and Access Security devices. These devices may host the applications of the AUA and support biometric capture mechanism to collect biometrics of residents for authentication purposes. Any additional features of these terminal devices may depend on the specific needs of services offered by AUAs. These devices could comply with specifications issues by the UIDAI to protect all the biometric and demographic information provided by the residents. Terminal devices are registered with the Aadhaar system for encryption key management and are referred to as registered terminal devices. Public terminal devices are not registered.

31. **Biometric Device Specifications.** The terminal device used in Aadhaar biometric-based authentication has the capability to capture fingerprints and iris images of the resident at the time of the service delivery. The UIDAI has defined its specifications[24] based on open standards so data captured using the device could ensure high data quality and result in greater accuracy.

32. The fingerprint-based biometric system is at the core of the UIDAI deduplication and unique identification of the resident. Fingerprinting, the oldest biometric technology, has the largest market share of all biometrics modalities globally. The fingerprint industry also has a variety of suppliers and a base of experienced professionals necessary to implement the unique identity management solution at the scale that India required. Face is the most commonly captured biometric, and frequently used in manual checking. However, stand-alone, automatic face recognition does not provide a high level of accuracy, and can only be used to supplement a primary biometric modality.

33. **Biometric Device Certification for UID Application.** The UIDAI has adopted a certification process for biometric devices to ensure the latter's compliance to UIDAI specifications. The UIDAI has delegated the responsibility of implementing the certification process to the Standardization

---

[24] Biometric Devices Specifications for Aadhaar Authentication - http://stqc.gov.in/sites/upload_files/stqc/files/New%20Revision%20_May_%201%20STQC%20UIDAI%20BDCS-03-08%20UIDAI%20Biometric%20Device%20Specifications%20_Authentication_.pdf

Testing and Quality Certification (STQC) directorate under the Department of Information Technology (DIT). The directorate provides quality assurance services in the area of electronics and IT through countrywide network of laboratories and centers. It maintains a list of certified vendors' biometric devices that may be used by service providers for biometric authentication. Vendors who could like to get their biometric device certified have to follow the certification process defined by the STQC that is published on the UIDAI portal[25].

34. **Best Finger Detection Service.** Based on the results of a series of Proof of Concept (PoC) studies on Aadhaar biometric authentication, it was learned that a resident being fingerprinted for authentication may give prints of varying quality across all the fingers. Therefore, the accuracy or the chances of being matched may vary due to these differences. This variation may also be present due to the manner in which the resident normally interacts with a typical fingerprint scanner, and the various fingers may inherently have different amount of identifying information depending on the size of the finger and the commonness of the pattern it carries. Hence, the UIDAI provides the Best Finger Detection (BFD)[26] as stateless web service that can be called by the service providers' service delivery application to detect a resident's finger that has the greatest accuracy and yields successful matching results. The resident may then use the best finger to ensure a high success rate in biometric authentication.

35. **Biometric Software and Programming Specifications.** The UIDAI has published on its public portal the Aadhaar biometric Software Development Kit (SDK) and Application Programming Interface (API) specifications[27] that provide a single unified interface across multiple modalities (face, fingerprint, and iris) for SDK developers from biometric device vendors to expose their functionality to various modules of the Aadhaar system. This promotes vendor neutrality as the use of standard APIs and open standards could eliminate proprietary and vendor-specific features. It also promotes interoperability by using standard interfaces, common data format definitions, and protocols across the components that expose similar functionality. The open API allows the best of the breed algorithms to be used for special purposes. The API exposes quality check, segmentation, sequencing, extraction and matching functionalities.

---

[25] Biometric Device Certification Process - http://uidai.gov.in/biometric-devices/180.html

[26] Aadhaar Best Finger Detection API Specifications - http://uidai.gov.in/images/FrontPageUpdates/aadhaar_bfd_api_1_6.pdf

[27] Aadhaar Biometric SDK API Specification version 2 - http://uidai.gov.in/images/aadhaar_biometric_sdk_api_2_0.pdf

36. The Aadhaar authentication supports the use of multiple factors. These factors include demographic data, biometric data, PIN, OTP, possession of mobile, or combination thereof. Adding multiple factors increases the strength of authentication depending on the factors. Applications using Aadhaar authentication need to choose appropriate factors based on their needs. However, not all factors are implemented at this time.

37. The UIDAI has published on its public portal the Aadhaar authentication API specifications[28] that are used by the AUAs and ASAs to integrate the authentication service call into their service delivery application. They include API data format, protocol, and security specifications.

38. The Aadhaar authentication services are exposed as stateless service over Hyper-text Transfer Protocol Secure (HTTPS). The usage of open data format in Extensible Markup Language (XML) and widely used protocol such as HTTP allows easy adoption and deployment of Aadhaar authentication.

39. In order for service provider agencies to leverage the Aadhaar authentication service in delivering their services, they capture and store the 12-digit Aadhaar number (UID) with the unique identifier (customer or beneficiary ID, etc.) in the service delivery databases. The process by which the UID of residents are included in the service delivery database of service providers for enabling Aadhaar-based authentication during service delivery is referred to as Aadhaar seeding[29].

40. Going forward, the Aadhaar may form the basic, universal identity infrastructure with which registrars, government and other service providers across the country may be able to build their identity-based applications. These features, in turn, are expected to serve multiple transformational benefits in development and equitable growth through proper identification. Eventually, they will lead to better targeting by development schemes of the government and the private sector, ensuring that all fake, duplicate and ghost records are weeded out from databases so that leakages resulting from such records are avoided. In the same vein, they will increase the reach and efficiency of delivering many goods and services like PDS, banking and finance,

---

[28] Aadhaar Authentication API Specifications - http://uidai.gov.in/images/FrontPageUpdates/aadhaar_authentication_api_1_6.pdf

[29] Aadhaar seeding - http://uidai.gov.in/images/aadhaar_seeding_v_10_280312.pdf

telecom, health, insurance, education, etc. and could no longer need repeated KYC checks on residents. The seeding process, however, has to necessarily be preceded by data digitization and centralization.

41. Data digitization essentially means collation of service delivery data in an electronic format (database/Excel or similar) from where data can be retrieved using standard Structured Query Language (SQL) queries. It is also important that personal identity data slowly becomes consistent across multiple systems. The Aadhaar is also an initiative to standardize personal identity information, and Aadhaar data may be used to clean the existing data.

42. Data centralization primarily manages availability and accessibility of distributed service delivery data. The objective here is for the seeding process/utility to be able to access the service delivery data and all related information in at least the read-only mode. For instance, in one state pensioners' data may be available in data silos across districts. A consolidated view of the entire data may facilitate the social welfare department of the state to improve the service delivery in its programs, while also being able to ensure that the same person is not availing double benefits from two different districts. In case service delivery data is already digitized and centralized, then no action is required from the seeding perspective.

43. There are two ways of seeding the service delivery database with the Aadhaar number: top-down method and organic method. The former uses enrollment information available in the Know-Your-Residence + (KYR+) and the Electronic Identity (eID)/UID files as input, while the latter requires a service provider to contact the resident, or vice-versa, for the purpose of updating the individual's personal information through a process decided by the service provider**Error! Bookmark not defined.**. The completion of the seeding process may be followed by the demographic/biometric authentication, especially where no direct update of the service delivery database is enabled.

44. There are some common challenges**Error! Bookmark not defined.** faced during the seeding process and an understanding of these challenges has resulted in necessary precautions taken early during the planning process. Some of the common challenges faced are: the complete data were not captured in the service delivery databases; similar information across different data sources do not have an exact match among them; the data in the service delivery database is in a local language; all the required data are not available; and the regular tools cannot handle high volume of data.

45. The seeding process typically involves data extraction, consolidation, normalization and matching. For performing these activities, the UIDAI developed **GingerError! Bookmark not defined.**, an in-house tool which may be used by service providers after signing a contract agreeing that the tool is not to be used for purposes other than what it was intended for.

46. **Remote Aadhaar Seeding Framework.** The UIDAI designed and implemented the centralized platform hosted by UIDAI, namely the Remote Aadhaar Seeding Framework[30] (RASF) with the objective of enabling the states to expedite their seeding efforts for a faster adoption of Aadhaar-enabled service delivery. The service provider may use the centralized platform to seed its service delivery database in a seamless manner by inserting the seeding request and validating the data; this operation is performed by authorized users from the service providers.

47. Government and private sector service providers such as those in banking[31], insurance[32], capital markets[33], telecom[34], LPG[35], and railways[36] have updated their KYC norms to include Aadhaar as the valid KYC credential.

48. For stakeholders wishing to leverage the Aadhaar Identity solution in their service delivery applications, the UIDAI has created a support group and a set of artifacts. The support structure includes an applications group at the UIDAI, and empanelled consultants and software vendors to help service providers build necessary processes and applications. Further, there are detailed support documents for guidance on leveraging and integrating the Aadhaar solution such as:

a. Applications Onboarding and Readiness for service delivery providers.
b. Authentication Framework, Operating Model and Guidelines.
c. Criteria, checklists and activity templates for becoming an AUA or an ASA.
d. Aadhaar seeding solutions for service delivery databases to embed Aadhaar number.

49. The UIDAI has defined the registration process for the selection of key players (ASA, AUA, sub-AUA, etc.) in the delivery of authentication services to the government and private organizations. The process is simple enough for aspiring agencies to adopt but, at the same time,

---

[30] Remote Aadhaar Seeding Framework - http://uidai.gov.in/images/uidai_rasf_v06_27022013.pdf

[31] http://www.rbi.org.in/scripts/BS_ViewMasCirculardetails.aspx?id=7367

[32] http://www.irda.gov.in/ADMINCMS/cms/whatsNew_Layout.aspx?page=PageNo1322&flag=1

[33] http://www.sebi.gov.in/cms/sebi_data/attachdocs/1344851126270.pdf

[34] http://www.dot.gov.in/as/2011/as_14.01.2011.pdf

[35] http://uidai.gov.in/images/FrontPageUpdates/aadhaar_news_release_28_june.pdf

[36] http://www.indianrail.gov.in/id_proof.doc

it includes the necessary checks and balances to ensure that the agencies selected for the role are capable of delivering the services. The UIDAI clearly defines the step-by-step process in applying for the position and provides the supporting documents applicable to each player.

50. **Technical Awareness and Adoption.** The UIDAI has setup a public portal[37] for building technical awareness and providing technical support to the user agencies in both public and private sector. It publishes technical documentations on the portal on a regular basis targeted at software professionals working in the technology domain and interested in incorporating Aadhaar authentication into their applications.

51. **eKYC Service.** The UIDAI has implemented eKYC service[38] through which the service providers can perform the KYC process electronically with explicit authorization by the resident. In the eKYC process, the residents authorize the UIDAI through Aadhaar authentication using either biometric data or OTP to provide their demographic data, along with their photograph digitally signed and encrypted, to service providers. This helps the service providers perform a paperless KYC on the residents in real time as part of their service delivery process using the eKYC function. This could enable service providers to make instant service delivery to residents, which otherwise could take a few days for activation pending verification of KYC documents, digitization, etc. Also eliminated are the cost of repeated KYC, paper handling and storage, and the risk of forged Proof of Identity (PoI) and Proof of Address (PoA) documents.

52. **Aadhaar Payment Bridge (Aadhaar as a Payment Address).** The UIDAI implemented the Aadhaar Payment Bridge (APB) using Aadhaar-enabled payments Infrastructure: a system that routes money to any resident on the basis of the Aadhaar number. This system facilitates seamless transfers of all welfare scheme payments to beneficiary residents' Aadhaar-Enabled Bank Account (AEBA). At the time of Aashaar enrollment, residents provide their existing bank account details or request for the opening of a new account that may be attached to their Aadhaar number for all welfare scheme payments. The APB maintains a repository of residents' Aadhaar number with the corresponding primary bank account number used for receiving social security and entitlement payments from various government agencies. The APB uses the compulsory Aadhaar number as the primary key for all entitlement payments. This may weed out fake and ghost identities from the system and ensure that the benefits reach the intended beneficiaries.

---

[37] UIDAI public facing portal - http://uidai.gov.in/

[38] e-KYC service - http://uidai.gov.in/images/e_kyc_policy_note_final.pdf

53. The UIDAI solution to financial inclusion makes use of the combination of Aadhaar as a payment address and the eKYC for instant account creation with the Aadhaar-enabled payment infrastructure. The funds are able to reach residents with an Aadhaar number, irrespective of whether they have a bank account or not. If they have an AEBA, the money can be transferred into it. If they do not have one, an instant account may be created on the basis of the Aadhaar number with a debit freeze. The money that is transferred is credited into the instant account which is activated during the first withdrawal on the basis of the eKYC function.

II. Estonia

1. Estonia has one of the most advanced eSocieties in the world. An incredible success story that grew out of the partnership between a forward-thinking government, a pro-active ICT sector, and a switched-on, tech-savvy population. Seventy-eight percent of the population aged 16-74 years uses the Internet[39] (Statistics Estonia). Seventy-one percent of households have Internet capabilities (Statistics Estonia, 2011) and all the Estonian Schools are connected to the Internet.

2. Estonia did not have any national personal identification document – neither physically nor electronically. Hence, Estonia implemented the eID system to identify its citizens and alien residents within the country using the ID card as the primary identification document.

3. The ID card provides two main functions. The first is as a physical form of identity – used as a regular ID in conventional real-world situations, anywhere one may typically need to prove identity, age and so on. The second function is for electronic identification – it enables citizens to use the same card to electronically authenticate to websites and networks, and/or to digitally sign communications and transactions, as required.

4. The first electronic ID card was issued in 2002; it was issued to 130,000 residents that first year[40]. As of January 2012, more than 1.1 million people in Estonia (almost 90 percent of inhabitants) had ID cards[41]. The **Estonian ID card** is used for delivering auxiliary identity services and it is the mandatory document for personal identification of residents from the age of 15. It can be used for signing documents electronically, for personal identification, and for data

---

[39] Who, where and why uses the Internet - http://www.stat.ee/dokumendid/68627

[40] eID in action: Estonia - http://ec.europa.eu/idabc/en/document/4487/5584.html

[41] e-Estonia - http://estonia.eu/about-estonia/economy-a-it/e-estonia.html

encryption functions. The card has two certificates in X.509 v3 format and two associated private keys protected by a PIN saved on the ID card: (a) a certificate for digital personal identification, data signing and encryption; and (b) a certificate for digital signing, enabling the cardholder to issue a eSignature. On ID cards issued after January 1, 2007, the certificates are valid for as long as the card itself, i.e., five years; and there is no need to renew the certificates.[42] The card bears the personal digital file containing the residents' personal profile[43]. The card is a smart card and complies with ISO/IEC 7816 standard. The ID card was created to function both as a physical ID and an electronic ID and may be valid for up to ten years. In emergency cases (e.g., loss of the card), the certificates can be suspended, if required – disabling the ability to use the card for electronic authentication and transactions.

5. The digital certificates issued in association with the ID card scheme are qualified certificates as per the European Digital Signature e directive 1999/93/EC[44].

6. Apart from physical identification for service delivery, the key eID services delivered are eSignature (digitally sign eDocuments), authentication (electronic authentication of the resident), and document encryption. They are used by service providers in the government and the private sector as the common auxiliary services enabling service delivery.

7. The **digital personal authentication** service authenticates the resident electronically at the time of the eService delivery using the personal identification certificate on the eID document. The personal identification certificate contains the information about the resident and the resident can prove that it is him/her by entering the PIN. Desktop and web applications use this information to identify the users at the time of service delivery.

8. The **eSignature** enables residents to sign eDocuments digitally using the signing certificate and a pair of keys on their eID document (ID card or mobile phone) apart from the identification certificate. The Estonia ESignature Act (ESA)[45] passed in 2000 ensures that the eSignature of the resident given with the signing key pair on the e-ID token that have the validity

---

[42] http://www.id.ee/index.php?id=31015

[43] Personal Data File on the card – https://eid.eesti.ee/index.php/General_information_for_developers#Using_the_personal_data_file

[44] European ESignature Directives 1999/93/EC – http://www.columbia.edu/~mr2651/ecommerce3/2nd/statutes/ElectronicSignaturesDirective.pdf

[45] Estonia ESignatures Act (DSA – 2000) – http://www.legaltext.ee/text/en/X30081K4.htm

certificate has legal binding and is equal to a traditional signature. Estonia is one of the few European countries where the electronic signature functionality is not optional.

9. The certificates contain the cardholder's name and personal ID number, and the authentication certificate also contains an official email address unique to each cardholder. Estonia provides an official email address to each citizen. The email address is used for official government communications, but it can also be used for private communications. A citizen's email address is in the format "firstname.lastname_NNNN@eesti.ee" where NNNN represents four random digits. Every cardholder can also receive email at the address "ID_CODE@eesti.ee" where ID_CODE represents the personal ID number of the citizen. Estonia does not provide an email service to its citizens; instead, the email address acts as a relay, and citizens specify an email account where the messages are delivered. All email addresses are publicly listed on Estonia's National Registry of Certification Service Providers' certificate directory.

10. The government implemented reliable and trustworthy identification infrastructure in Estonia, receiving high acceptance by citizens and businesses and hence becoming a success in terms of effectiveness and efficiency of its use in everyday life.

11. Given that the eID infrastructure is a very sensitive area in the public administration of Estonia, it has been designed to be highly reliable and provides fulltime technical support. The technical solution is based on the already proven technology that is provided by inner country software and vendors. The solution is scalable, flexible, and standards-based for expansion to other services as well as forward-looking to also enable cross-border use.

12. The **digital stamp** is a service that allows legal entities (e.g., companies) to sign documents digitally. It is an equivalent of the ID card for companies. This confirms that the document comes from the company that has signed it and that the document has not been changed in the interim. Signatures (also in large quantities) can be attached to invoices, payment orders, confirmations, certificates, bank statements (e.g., SEB bank offers an automatically digi-stamped bank statement), etc. The company is issued a USB crypto-stick that has an X.509 certificate and, similar to the eSignature, when the stamp is used, a container in DigiDOC format may be created that contains the signed data.

13. The eID documents offer the functionality to encrypt and decrypt eDocuments using the authentication certificate. This function is primarily meant for the safe transport of files in an unsafe environment (e.g., the Internet) as opposed to the long-term storage of data.

14. In Estonia, the usage of eID is regulated by the ESA[Error! Bookmark not defined.] and the Identity ocuments Act[46], on the basis of which the Estonian ID card is issued. Estonia launched its electronic ID card program in February 1999 when the Estonian Parliament passed the Identity Documents Act. The Act became effective January 1, 2000, and established national guidelines for the creation of a mandatory national identity card for the citizens of Estonia and permanent resident aliens of the age of 15 years and above. Before this, Estonia did not have a national personal identification document.

15. The Identity Documents Act also states that the deduplicated and processed residents demographic and biometric data used for the personalization of the identity card is also entered into the National Population Register pursuant to the Population Register Act[47].

16. The specific legislation associated with eSignatures, the ESA, was passed separately by the Estonian Parliament (Riigikogu) on March 8, 2000, and came into force on December 15, 2000. This law regulates the framework and rules required to effectively govern a national Public Key Infrastructure (PKI) and eSignature infrastructure. The primary aim of the ESA was to give electronic signatures the same level of trust and assurance as handwritten signatures. As a rule the handwritten and eSignatures may be equivalent in both the public and private sector. The ESA also states that public service departments could accept digitally signed documents. The ESA requires that each eSignature may uniquely identify the signatory, bind the individual to the signed data, and ensure that the signed data cannot be tampered with retrospectively without invalidating the signature itself.

17. **Rules and Regulations for Certificate Service Providers.** One of the core components of the ESA was the establishment of rules and regulations with regard to Certificate Service Providers (CSPs) that issue digital certificates to users and manage related security services. The ESA mandates a number of stringent financial and procedural requirements to ensure that CSPs are set up and managed properly to perform their function to the highest possible standard.

18. **Rules and Regulations for Timestamp Service Providers.** The ESA also regulates time stamping services that are provided by the Timestamp Service Providers (TSPs). The TSPs have to adhere to similar laws and regulations as CSPs. The timestamp is simply a piece of information

---

[46] Estonia Identity Documents Act (1999) – http://www.legislationline.org/documents/id/5718

[47] Estonia Population Register Act (2000) – http://www.legaltext.ee/text/en/X40051K5.htm

that attests to the occurrence of an event at a specific time. The ESA does not define timestamps in great detail, but it ensures that timestamped data cannot be tampered with or amended without invalidating the timestamp itself.

19. **Personal Data Protection Act.** Personal Data Protection Act regulates the use of personal data and databases containing personal data by public authorities and private entities. Data Protection Inspection is the government body overseeing that the requirements of the act are met and enforcing compliance, if necessary. The strategy for data protection and ID card in Estonia is that the card may contain as little private data as possible. Instead, the data may be kept in databases at relevant authorities, and a person can use the card as the key (authorization method) to access his/her data in the database. Requests by third parties (e.g., representatives of authorities) for private data are logged and logs are available online for the individual on request (via the citizen's portal).

20. **Digital Certificate of Identity.** More commonly referred to as Digi-ID, this is a state digital document for personal identification in an electronic environment and for issuing a eSignature. Unlike the ID card, Digi-ID is not designed for visual personal identification; therefore, it does not carry a photo - just the name, personal identification number and validity end-date. Also, the personal data file is empty on a Digi-ID card, except for the document number field. Cryptographically, it is a smart card similar to the ID card. While the issuance of an ID card can take up to a month, Digi-ID cards are issued within minutes from the service points of the Police and Border Guard Board.

21. **Electronic Residence Card.** Issued to foreigners residing in Estonia who are not citizens of the European Union, the electronic residence card carries the data of the residence permit. In terms of available electronic services, the functionalities of the residence card and the ID card are the same. The main difference is that the ID card issued to citizens of Estonia and the EU can be used as a travel document within the EU, while the residence card cannot be used for travelling outside of Estonia. Another difference is that the residence card also carries a contactless chip with the user's fingerprints and face image.

22. **Mobile ID.** Given that the penetration of mobile phones in Estonia is more than 100 percent, the government introduced the concept of mobile ID for electronic personal identification and digital signing to accelerate the adoption of the eID for accessing its eServices. Mobile ID is an electronic document of personal identification that can be used for electronic personal identification and digital signing with a mobile telephone, where the mobile phone with

its SIM functions simultaneously as the ID card and the card reader. For using a mobile ID, a specialized SIM is required to enable the service. It may be obtained by signing a service contract with a mobile operator. The mobile ID may become usable after it has been activated in the electronic application environment of the Police and Border Guard Board, where the necessary certificates are requested. Unlike other documents, certificates of a mobile ID are not saved on the SIM. Unlike the ID card, a mobile ID cannot be used for document encryption – otherwise, both DigiDocService and the mobile phone operator may see the decrypted data.

23. The mobile ID is issued by the national mobile operators in Estonia such as Elisa, EMT[48], at Tele2 at their local stores. Residents approach their mobile operator for the issuance of the mobile ID at the nearest local store. Residents present their ID card with valid certificates for getting the mobile ID. A resident has to sign a contract (mobile ID subscription agreement[49]) with the mobile operator to get the mobile ID. The government has delegated the responsibility of issuing mobile ID to the national mobile operators.

24. **Mobile ID Certificate Activation.** Residents have to activate the service on their handset with the specialized SIM. To activate mobile ID service or to apply for certificates, the resident has to go to the website of the Police and the Border Guard Board[50] and submit an application for the issue of new certificates. To get the certificate for mobile ID, the resident has to fill an online application form on the police website and enter the ID card into the card reader and follow the instructions.

25. The mobile operator charges the resident for the mobile ID service. The charges include a one-time subscription fee and monthly fees. If the mobile ID is used outside of Estonia, each mobile ID transaction is charged at the cost of sending one text message as per the package's price list.

26. The government implemented four main operating procedures for implementing the mobile ID in Estonia. They are:

a. **SIM Provision.** The resident may go to any of the service providers offering mobile ID service for registering the new mobile ID SIM. The service provider forwards the

---

[48] EMT website – https://www.emt.ee/en/mugavusteenused/mobiil-ID#open-4077133-tab-5

[49] Mobile ID Subscription agreement – https://www.emt.ee/en/era-arve

[50] Police Web Site for activation of the Mobile ID – http://www.politsei.ee

application to the Mobile Network Operator (MNO) and informs the resident of the location from where to pick up the SIM. The MNO identifies the user using the ID card and, on successful authentication, hands over a new SIM card to the resident or installs the software into the resident's SIM as needed. As part of the provisioning process, the SIM is attached to a unique secure signature creation device (SSCD) for the unique resident; the SSCD may be later used for issuing a qualified certificate. The SSCD certificate is declared active for a particular SIM and is made available to all the TSPs. The MNO provides a unique code to the resident for activation of the qualified certificate.

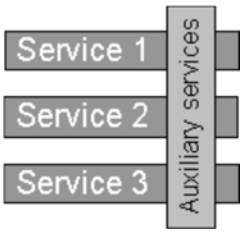
b. **User Registration/Certificate Activation.** The purpose of the certificate activation process is to create and activate a qualified certificate. Residents issue a request to activate their qualified certificate using their mobile phone with the new SIM. The Registration Authority (RA) initiates the signing request to a resident's mobile device to sign the personal data. The resident verifies the data and signs it by inputting his/her device certificate activation code. The RA receives the personal data signed. The RA enters additional data including the device certificate and forwards the request for certification activation to a Certification Authority (CA). The CA creates and activates a qualified certificate and publishes it.

c. **Usage.** The service provider requests identity service from a TSP and uses a Global System for Mobile Communication (GSM) subscriber number and/or personal identification code to identify the resident. The TSP generates the signature request and sends it to the resident's mobile phone. The resident signs the request by entering his/her PIN. The TSP receives the signature data and checks its validity and that of the certificate. The service provider receives the identity-related services from the TSP.

d. **Termination.** It is possible for the resident to stop using the mobile ID for several reasons: e.g., the resident may not be using the service, a lost/compromised SSCD, the qualified certificate expired, or the resident has violated the user-CA agreement. In case of certificate revocation, the RA informs the CA of certification revocation, the CA immediately revokes the certificate, and the certificate revocation list (CRL) is updated. In case of SIM blocking due to loss or SIM damage, the device certificate is taken out of the list of valid SSCDs available to all TSPs.

27. **Interoperability.** These auxiliary services have been designed to ensure that they can be integrated with the existing and planned primary service delivery systems of service providers in Estonia to enable functionalities such as eSignature, electronic authentication and document encryption. The interoperability requirements were met by:

a. **Employment of standardized workflows**. A standardized workflow was made possible by adopting a common document format applicable to each service independent of its provider (DigiDoc) and a central common public, service-rendering resource that connected national databases.



b. **Centrally provided unique identification number for each Estonian resident.** A central database of unique identification numbers allocated to each Estonian resident was established providing authentication of the cardholder (i.e., the applicant or signatory). A centralized infrastructure of a national, unique identification number for each Estonian resident was employed to serve their authentication in electronic processes.
c. **Common public, service-rendering resource to connect national databases.** To enable identification and authentication for the various services via a corporate infrastructure, a common public, service-rendering resource called X-Road was developed. Based on the Internet, X-Road connects public databases and information systems, tools centrally developed by the State (i.e., the State Portal Center) and the X-Road Center (management and control of the gateway) with the Certification Center for the eID cards.
d. **Central single point of access to public services (eCitizen portal)**. The eID card of citizens is just a secure token for various purposes to which access is provided by a single point of entry: the eCitizen portal.
e. **Standardized workflows using a uniform document format (DigiDoc).** To digitally sign documents, a communication model using standardized workflows in common document format called DigiDoc was employed. The DigiDoc format is based on the XML Advanced Electronic Signatures (XAdES) standard. The XAdES defines a format that structurally enables storage of signed data, signature and security attributes associated with eSignature; hence, it lends itself well to having a common understanding.

28. The key organizational roles required for the wPKI/mobile ID operation are:

a. **Mobile Network Operator.** The MNO provisions the new SIM to the resident when the latter applies for mobile ID. The SIM includes SSCD function as per Directive 1993/93 EC[51].
b. **Registration Authority.** The RA is responsible for the user registration and activation of the mobile ID.
c. **Certification Authority.** The CA manages activation, suspension, and revocation of certificates.
d. **Trusted Service Provider.** The TSP acts as the central interface in the wPKI infrastructure. The main tasks include accepting authentication and signing transactions from service providers, passing requests to mobile operators, and checking certificate and signature validity.
e. **Relying Party/Service Provider.** The SP is a third party that is interested in authentication and/or eSignature of the users.

29. The Estonian ID card scheme is the overall responsibility of the Estonian Governments' Citizen and Migration Board (CMB). It is responsible for the issuance of identity documents to citizens and alien residents as required by the governments' National Identity Act. The CMB is the institution that physically receives card application forms from residents.

30. **Public-Private-Partnership.** The process is managed through a tight public and private partnership with two key private organizations. AS Sertifitseerimiskeskus (SK), which is a joint venture formed in 2001 between two of Estonia's largest banks (Hansapank, Eesti Ühispank), and telecommunications organizations (Eesti Telefon and EMT) act as Certification Center. TRÜB Baltic AS, a subsidiary of the TRÜB financial services organization and headquartered in Switzerland, is the company that personalizes the card itself — physically and electronically. TRÜB receives the card application from CMB and manufactures the card, printing and engraving the personal data on the card, generating keys on the chip and embedding the certificates.

31. SK functions as the certification authority for the Estonian ID card project and manages a complete range of associated electronic services, including Lightweight Directory Access Protocol (LDAP) directory service, Online Certificate Status Protocol (OCSP) validation service, and other certificate-related services. SK manages the end-user distribution channel through its parent retail bank outlets. SK is responsible for the development and maintenance of the ID-software

[51] SSCD Specification – Directive 1993/93 EC – http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&numdoc=31999L0093&model=guichett

that is installed on the resident device for accessing eID services offered by the government. It is similarly responsible for ID-software installation packages, instructions and video instruction that is published on the government's public portal. SK runs the call center and provides email support services to the resident on behalf of the government.

32. For processing and controlling eSignatures, the following authorities and agencies are relevant:

a. **Certification Service Providers.** According to the Estonian ESA, the CSPs certify actual individuals identifiable by name and ID code. CSPs could be legal entities fulfilling specific legal requirements.

b. **Timestamping Service Providers.** The ESA also regulates the work of TSPs). The requirements for TSPs are generally the same as those for CSPs. According to the ESA, a timestamp is simply a data unit that proves that certain data existed at a certain moment.

33. The **Estonian Information System Authority**[52] known as RIA coordinates the development and administration of the State's information system; it organizes activities related to information security, and handles the security incidents that have occurred in Estonian computer networks. RIA advises the providers of public services on how to manage their information systems as per requirements, and monitors them. It is also responsible for providing technical support and national shared IT Infrastructure and services to the government agency responsible for delivering identity services.

34. **ID-software.** The government of Estonia provides the software that are to be installed on the residents' Internet-connected device (laptop, desktop, etc.). The software, collectively referred to as ID-software, allows the residents to use their ID card electronically to access private and government eServices, digitally sign documents, and encrypt documents for safe transfer. The government provides on its public website[53] the steps for installing the ID-software on the device. During ID-software installation, three programs are installed on the computer:

a. **ID-card Utility.** The utility is used by residents to check the functioning of their ID-card and the certificate validity, and to extend it when necessary, to change and unblock PIN and PIN Unlock Key (PUK) codes, and to configure the @eesti.ee email address.

---

[52] Estonian Information System's Authority – https://www.ria.ee/about-estonian-information-systems-authority/

[53] Estonia government Web Site for installing ID-software – https://installer.id.ee/?lang=eng

b. **DigiDoc3 Client.** This is used to sign digitally with the ID-card and mobile ID, to check the validity of eSignatures, and open and save documents inside the signature container. Digitally signed containers are files with .bdoc or .ddoc extensions.
c. **DigiDoc3 Crypto.** This enables residents to secure files for safe transfer using the ID-card and to view secure documents (decrypt). The files are encrypted using the ID-card's authentication certificate and added to the secure container file with the .cdoc extension.
d. **Browser Plug-in.** This is installed on the residents' device when accessing the portal for the first time. The plug-in requests for the residents' certificate and the corresponding PIN to authenticate their identity before allowing them access to the service provider.

35. **Web Portal.** The portal is located at http://digidoc.sk.ee; it is available to all cardholders free of charge. Its functions are similar to the client program — one may use it to generate and verify eSignatures. In addition, one may use it to have a document signed by a number of people. With a few clicks of the mouse, the user is able to designate the people whose signatures are needed on the document, and they can all sign it on the same portal. Every user has a directory of his/her documents that no one else sees; however, anyone can send documents for the user's signature.

36. SK, together with its partners, delivered the comprehensive eSignature architecture known as DigiDoc[54]. It is a universal system for giving, processing and verifying eSignatures. It can be connected to any new or existing piece of software. Its components are a stand-alone client program, a web portal and a web service based on Simple Object Access Protocol (SOAP)[55] enabling easy integration of the functionality of digital signing, signature verification, and authentication with other information systems. The service is usable in different development environments and platforms featuring SOAP 1.0 encoded support.

37. SK based the DigiDoc document format on the XML Signature (DSig) standard. In February 2002, the European Telecommunications Standards Institute (ETSI) published its extensions to XML-DSig as ETSI TS 101 903, also known as XAdES[56]. DigiDoc document format is a profile of

---

[54] DigiDoc Specification – http://www.sk.ee/upload/files/DigiDocService_spec_eng.pdf

[55] SOAP – Simple Object Access Portal – http://www.w3.org/TR/soap/

[56] XAdES – http://www.openxades.org

XAdES, containing a subset of its proposed extension. The XAdES profile of XAdES-X-L (i.e., extended long term) is used in the DigiDoc system but "timemarks" are used instead of "timestamps" and signing and certification validation time comes from the OCSP response. This profile provides the following information on the signed document:

a. Certificate used for signing
b. Signing time
c. Place of signature
d. Signer role and resolution
e. Incorporated full certificate validity information within the signature
f. OCSP response
g. OCSP responder certificate

38. Based on the document format, a library was developed in the C programming language that binds together the following:

a. DigiDoc document format
b. SK's OCSP validation service
c. Interfacing with the user's ID card using Windows' native CSP interface or cross platform PKCS#11.

39. **eCitizen Portal.** The eID card of the resident is a secure token for providing eID services on the single point of entry: the eCitizen portal. The eID card is used for identification purposes at the eCitizen portal. After identification, the validity of the citizen's certificates may be confirmed using OCSP service; a timestamp is given to the eService application. Using X-Roads, the Internet gateway, the application messages are securely exchanged.

40. In order to drive the adoption of eSignatures within the region, the availability of software and technology to the parties looking to incorporate compatible applications was critical. The government was not able to find a domestic generic application or implementation that could fulfill this requirement. Still, it made the decision to not rely on a foreign software or technology vendor to provide and guarantee support for a critical piece of national infrastructure. A reliance on foreign suppliers could have detrimental impact on the country's day-to-day functioning going forward. Because of these considerations, a bespoke software model was developed specifically to cater to Estonia and its eSignature constituents.

41. It is possible to verify signature validity without any additional external information; the verifier may trust the issuer of the signer's certificate and the OCSP responder certificate.

42. Original files along with signatures, validation confirmations and certificates are encapsulated within container with “SignedDoc” as the root element.

43. The DigiDoc system framework consists of base libraries, intermediate libraries, web service and end-user applications.

a. Software Library. The DigiDoc library is available to all developers as a program library in C programming language and as a Windows Component Object Model (COM). It can be connected to any existing or new software. For instance, one could add DigiDoc support to accounting software, document management system, web and intranet applications, and so on.
b. OCSP Server. On the server side, DigiDoc provides an RFC2560-compliant OCSP server, operating directly off the CA master certificate database and providing validity confirmations to certificates and signatures.
c. In order to ensure realtime validity of the certificate, certificate validity information may be obtained from a live database rather than from CRL and the time value in the OCSP response may be the actual one. To achieve long-term validity of eSignatures, a secure log system is employed within the model. All OCSP responses and changes in certificate validity are securely logged to preserve eSignature validity.

44. **DigiDoc Security Model.** One of the most challenging issues in eSignature systems is the question of validating a signature long after it was given. Often, the hassle of ensuring the validity of a signer’s certificate at the time of signing is left to the verifiers. In DigiDoc based on OpenXAdES, the proof of validity of the signer’s certificate is obtained at the time of signature creation. This proof may be obtained in the format of the OCSP response from the standard OCSP service and stored within the signed document.

45. DigiDoc service provides separate methods for mobile authentication and mobile signing, namely MobileAuthenticate, MobileSign and MobileCreateSignature. All three methods accept mobile ID users’ personal identification code and/or phone number as input parameter. Using just the phone number for user identification is not recommended as mobile numbers are public and may result into security issues. It is recommended that both phone number and personal identification code be used since the latter is not public information and may be a safer option.

46. Wireless Public Key Infrastructure[57]. Mobile ID is based on the wPKI specification that is the wireless implementation of the PKI. With wPKI, mobile phone operates as a smart card reader with display. The communication between the PC/service and the mobile phone goes through mobile signing/authentication service on the phone and mobile gateway of the GSM operator.

47. The mobile gateway uses the Over-The-Air (OTA) technology[58] to communicate and run the applications on the SIM of the mobile phone without being connected physically to the card. The DigiDoc service sends the authentication/signing request (wPKI Request[59]) to the back-end system of the network operator that, in turn, sends the request to the OTA gateway/server. The OTA gateway transforms the request into short messages and sends them onto a Short Message Service Center (SMSC) that transmits them to the residents' mobile phone. The OTA gateway gets the service request using the OTA gateway API. The OTA gateway maintains the database of cards issued and activated with details such as SIM vendor, the card's identification number, the International Mobile Subscriber Identity (IMSI) and Mobile Station International Subscriber Directory Number (MSISDN). The OTA gateway has a set of libraries that contains the formats to use for each type of SIM that it uses for formatting the service request into a message that can be understood by the residents' phone. The OTA gateway sends the message to the SMSC using the right parameters as described in GSM 03.48. The SMSC may send a message of a maximum length of 160 alphanumeric characters to and from the mobile phone. If the mobile phone power is off or has left the coverage area, the message is stored and offered back to the subscriber when the mobile phone is powered on or has entered back into the coverage area of the network. The communication between the SIM and the OTA gateway is done by SMS exchange using the SMS channel.

48. The mobile phone should be Phase 2+ in the GSM standard[60] and could have the SIM Application Toolkit (STK)[61] with the OTA services support compliant with the GSM standards[62].

---

[57] wPKI Specification – http://www.signature.lt/KK/wPKI-specification.pdf

[58] Over-The-Air Technology – http://www.gemalto.com/techno/ota/

[59] WPKI Mobile Transactions – http://wpki.eu/doku/lib/exe/fetch.php/wiki:baltic_wpki_standard_draft-0.3.pdf

[60] GSM 11.11 Digital Cellular Telecommunications system (Phase 2+); Specification of the Subscriber Identity Module – Mobile Equipment (SIM-ME) interface – http://www.etsi.org/deliver/etsi_gts/11/1111/05.03.00_60/gsmts_1111v050300p.pdf

[61] SIM Application Toolkit – http://www.gemalto.com/techno/stk/

[62] GSM 11.14 Digital Cellular Telecommunications system (Phase 2+); Specification of the SIM Application Toolkit for Subscriber Identity Module – Mobile Equipment (SIM-ME) interface – http://www.etsi.org/deliver/etsi_gts/11/1114/05.04.00_60/gsmts_1114v050400p.pdf

49. In Estonia today, usage of eID cards as a proof of identity is more common among professionals and enthusiasts. This is due mainly to the time needed for people to change their mindset, the lack of applications, initial technical glitches that discouraged some first-time users, and the relative higher cost of ID card readers. The ID card is widely used as a token for verification of valid eTickets in the public transport system and it are cheaper than paper ticket. The eID function of the bank card is more frequently used than the ID card. As the use of eID card is cost-effective to banks and assuring to citizens in terms of Internet security, economic common sense may support the shift from bank cards to eID cards for public service applications.

50. The government of Estonia has taken the following measures to improve the adoption of the eID by residents:

a. To encourage eID use among residents, the government has published on its public portal the steps necessary to installing its ID-software on residents' Internet-connected devices. The video instructions for software installation have also been uploaded to further guide residents.
b. The public portal also provides video instructions for digitally signing eDocuments using the ID-card or mobile-ID using DigiDoc service.
c. A test service installed by the government for use by residents to check the performance of their ID-Software and card reader, is working properly; it gives access to eID services.
d. The government has also set up a call center and email support for residents needing assistance with software installation and eID services.
e. The government provides the Digidoc[63] and other services specification documents that may be useful to service providers wishing to access the eSignature functionality in their delivery applications.

III. Belgium

Official Web Site: http://eid.belgium.be/en/

1. Belgium has three statutory electronic identity documents: the eID for citizens over the age of twelve, the kids-ID for children under twelve, and the foreigners' card for foreigners living in Belgium.

[63] DigiDoc Service Specifications - http://www.sk.ee/upload/files/DigiDocService_spec_eng.pdf

2. The identity card is the proof that the residents' personal information has been entered in the National Population Register in Belgium. The residents can use the ID card to prove their nationality and identity. All the citizens of Belgium automatically receive an electronic identity card at the age of twelve. They provided by the local registry office. The citizens above the age of 15 years are required to carry the identity card at all the times.

3. In Belgium, the eID has been implemented using the electronic identity card. The Belgium eID card is a smart card with a built-in chip. The chip contains authentication and signature certificates along with the PIN for each certificate.

4. The eID card is used to deliver electronic identification and authentication, and eSignature services. The authentication certificate is used to confirm the identity of residents at the time of logging on to a website with the residents' eID. The signature certificate enables the eSignature for the residents. Residents are eligible to use their eSignature from the age of 18 years. Residents go to local registry office to activate the signature certificate on the card.

5. The kids-ID using Hello Service[64] provides kids the extra protection in case of emergency. The service makes it possible to contact parents (or family, friends, neighbors, etc.) by phone if a child is in difficulty. Once the service is activated, people who find a missing child could have a number to call; the application automatically calls the number that has been specified. A user may specify up to seven numbers. If no one answers, the call is automatically transferred to the emergency number of Child Focus that is available 24 hours a day.

6. To use the eID with the government and private sector service providers, the resident requires a computer with supported operating system and a card reader attached to the computer.

7. The resident could have to install the eID software that enables the eID to be used on the computer. The software recognizes the card in the card reader as an electronic identity card and ensures that the data on the card's chip are read.

8. The Federal Public Service for Information and Communication Technology (Fedict) has developed simple software for supported operating system to install the eID software on the

---

[64] Hello Service - http://www.halloouders.be/

computer; it is called eID QuickInstall[65]. The software is available for download on the website of the government of Belgium's public portal for eID[66]. Residents may install the software by following onscreen instructions that show up by running the program. The software checks the configuration of the computer and installs drivers for the card reader and eID software. On successful installation the software, using the testing service[67] provided by Fedict, reads the data on the card to check if everything is working as designed. The software also provides the mechanism to install regular updates to the software.

9. The eID works with a PIN code and PIN Unlock Key (PUK) code. The PIN code is issued by the government and is found in the sealed letter from the local government when collecting the eID. The PIN code is a 12-digit number and can be updated by the resident. The letter also includes the PUK code. The resident is advised to visit the local registry office with the PIN and PUK codes that could then be used to activate the microchip on the eID card with assistance from staff. The PIN code is the personal code used by the resident each time an eID-based service delivery application is accessed; it could also be used for issuing eSignature. The PUK code is only for activating or unblocking the eID.

10. Fedict has set up its own online service desk to support residents in solving software installation and usage problems. The residents may fill a contact form[68] on the Fedict website to report problems.

11. Federal Public Service Home Affairs along with Federal Public Service Foreign Affairs, Foreign Trade and Development Cooperation and the Federal Police has set up free DOC STOP service[69] and the CheckDoc Service to protect the privacy of the data on the card and prevent identity fraud. DOC STOP helps to avoid risks of fraudulent use as well the unfavorable financial consequences. It enables residents to block the identity card immediately if it is lost or stolen. The resident could have to call a toll-free DOC STOP number to report the card lost or stolen and to have it blocked. The service is available 24 hours every day year-round.

---

[65] QuickInstall software - http://eid.belgium.be/en/using_your_eid/installing_the_eid_software/

[66] Belgium eID government public portal - http://eid.belgium.be/en/

[67] eID Installation Testing Service - http://www.test.eid.belgium.be/

[68] Fedict Service Desk Contact Form - http://eid.belgium.be/en/contact/contactform.jsp

[69] Doc Stop Service - https://www.docstop.be/DocStop/docstop_en.jsp

12. CheckDoc[70] enables verification in realtime of the validity of the Belgian identity documents; it also identifies stolen, lost, expired, invalid or never-used identity documents. To use the service, the resident or the user organization has to fill in a form and access the website with the user name and password provided on successful registration.

13. The government portal provides a list of eID-supported public and private sector applications[71].

14. Fedict has opted for Open-Source Software (OSS) and intensive collaboration with developers. The source code for the eID initiatives is, therefore, available to interested parties who may view the software and propose and/or make improvements. This cross-fertilization in which experts worldwide make modifications, improves the stability and quality of the source code. In line with this approach, Fedict has produced an eID Developers' Guides[72]. They contain guidelines for developing eID applications by means of examples.

15. Fedict is promoting the use of eID in both the public and private sector applications by providing developers with eID building blocks[73], the basic blocks of eID applications. It provides services to the government departments in the integration of the eID into their own applications. The services provided by Fedict are available on their public portal in the identification and security[74] section.

16. The eID building blocks includes:

a. **eID-Software and eID Applet**[75]. The eID software ensures the use of the eID on the resident's computer. The software provides the user interface and it recognizes the card in the card reader as an electronic identity card. The source code is available as an open source project[76] and Fedict maintains an online mailing list and discussions for developer support[77].

---

[70] Check Doc Service - https://www.checkdoc.be/CheckDoc/

[71] Available eID Applications - http://eid.belgium.be/en/available_eid_applications/

[72] Belgium eID Developers' Guides - http://eid.belgium.be/en/binaries/UPD_Developers_Guide_tcm406-112228.pdf

[73] Belgium eID Building Blocks - http://eid.belgium.be/en/developing_eid_applications/eid-bouwstenen/

[74] Identification & Security Section - http://www.fedict.belgium.be/en/identificatie_beveiliging/

[75] Belgium eID Software and applet - http://eid.belgium.be/en/developing_eid_applications/eid-bouwstenen/eID_software/

[76] Belgium eID Building Block Source Code - http://code.google.com/p/eid-mw/

[77] Belgium Developers Help and Support - http://groups.google.com/group/eid-mw

b. **ESignature Service**[78]. The ESS is a service that can be used by web applications to apply or check a eSignature against an eID. ESS supports various document formats and provides all the necessary interactions with the user. Signatures applied via the ESS comply with XAdES specifications and European Directives 2009/767/EC. The source code is available as an open source project[79].

c. **eID Identity Provider**[80]. The eID identity provider allows a web application to be made accessible using the eID. This building block contains all the functionalities needed to correctly authenticate the user of an application with an eID. The source code is available as an open-source project[81].

d. **Quick Key Toolset**[82]. The EZ Key or Quick Key Toolset means that a Java smartcard can behave like an eID. In this way, the EZ Key is opening the door to the future, when electronic identity may be less dependent on possible carriers. The source code is available as an open-source project[83].

17. Fedict also provides an eID Software Development Kit[84] to enable the developers to use the content of the eID card from the desktop application. The Software Development Kit (SDK) includes the eID Middleware[85] and is based on Public-Key Cryptography Standards (PKCS) #11.

18. Fedict[86] is responsible for developing the software for the eID card. It defines and implements the federal eGovernment strategy. It uses innovative information and communication technology to help the various federal public services to improve their service portfolios. To this end, Fedict tailors technology to meet the needs of the general public, business and civil servants.

---

[78] Belgium ESignature Service - http://eid.belgium.be/en/developing_eid_applications/eid-bouwstenen/digital_signature_service/

[79] Belgium DSS Source code - http://code.google.com/p/eid-dss

[80] Belgium eID Identity Provider - http://eid.belgium.be/en/developing_eid_applications/eid-bouwstenen/eID_identity_provider/

[81] Belgium eID Identity Provider Source Code - http://code.google.com/p/eid-idp

[82] Belgium Quick Key tool set - http://eid.belgium.be/en/developing_eid_applications/eid-bouwstenen/quick_key_tool_set/

[83] Belgium Quick Key tool set source code - http://code.google.com/p/eid-quick-key-toolset

[84] Belgium eID Software Development Kit (SDK) - http://eid.belgium.be/en/developing_eid_applications/eid_software_development_kit/

[85] Belgium eID Middleware SDK 4.0 - http://code.google.com/p/eid-mw/wiki/SDK40

[86] Fedict - http://www.fedict.belgium.be/en/over_fedict/

[i] ISO 27001 – http://www.27000.org/iso-27001.htm
[ii] ISO 27002 – http://www.27000.org/iso-27002.htm
[iii] ISO 27003 – http://www.27000.org/iso-27003.htm
[iv] ISO 27004 – http://www.27000.org/iso-27004.htm
[v] ISO 27005 – http://www.27000.org/iso-27005.htm