Government Publications Registration Number
11-1051000-001424-01

Knowledge Sharing Program

Consultation for the Improvement of National Certificate Authentication in the Lao PDR

Lao PDR

2023/24 KSP POLICY BRIEF

Presented by the MOEF, Republic of Korea

Ministry of Economy and Finance
KDI Korea Development Institute
IGB & COMPANY
KICA Korea Information Certificate Authority Inc.

Presented by the MOEF, Republic of Korea

2023/24 KSP POLICY BRIEF

Consultation for the Improvement of National Certificate Authentication in the Lao PDR

Lao PDR

Ministry of Economy and Finance

KDI Korea Development Institute

IGB & COMPANY

KICA Korea Information Certificate Authority Inc.

Project Title: Consultation for the Improvement of National Certificate Authentication in the Lao PDR

Prepared for
The Government of the Lao People's Democratic Republic

In Cooperation with
Ministry of Technology and Communications (MTC), Lao People's Democratic Republic

Supported by
Ministry of Economy and Finance (MOEF), Republic of Korea
Korea Development Institute (KDI)

Prepared by
IGB & Company Co., Ltd. (IGB)
Korea Information Certificate Authority Inc. (KICA)

Project Director
Jungwook Kim, Executive Director, Center for International Development (CID), KDI

Project Manager
Taihee Lee, Specialist, CID, KDI

Project Officers
Yeongjin Jeon, Senior Research Associate, CID, KDI
Seunga Cho, Consultant, IGB

Senior Advisor
Soohyun Choi, Former Governor of Financial Supervisory Service, Republic of Korea

Principal Investigator
Seung Yong Lee, Chief Consultant, IGB

Authors
Seung Yong Lee, Chief Consultant, IGB
Jae Jung Kim, CISO & Managing Director, KICA
Chang Hyun Yi, Director, IGB
Young Joo Ko, Leader of the Information Security Team, KICA
Ksenia Bakhtiarova, Senior Consultant, IGB
Anoloth Phanvongsa, CEO, S-Tech Development Co., Ltd.
Nilapheth Khammoungkhoune, Director of the NRCA Division, LANIC
Somchai Moua, Deputy Director of the NRCA Division, LANIC

English Editor
Editage

Government Publications Registration Number 11-1051000-001424-01
ISBN 979-11-5932-895-4 94320
979-11-5932-904-3 (set)

2023/24 KSP POLICY BRIEF

Consultation for the Improvement of National Certificate Authentication in the Lao PDR

Lao PDR

Preface

As the only country in the world to have transformed from being an ODA recipient to an ODA donor, South Korea stands an exceptional example of how knowledge and dedicated effort can fuel unprecedented progress. This remarkable transformation was made possible through the transfer of technology from abroad and significant investments in education, enriching the country's domestic knowledge resources and paving the way for its remarkable development journey. Along this path, the Korean government gleaned invaluable practical insights not typically found in conventional textbooks, further contributing to its growth and success.

The Ministry of Economy and Finance (MOEF) of Korea introduced the Knowledge Sharing Program (KSP) in 2004 to share Korea's development experience with the international community through joint research, policy consultations, and capacity-building activities. Since its inception, the program has played a vital role in supporting the socio-economic development of partner countries worldwide.

IGB & Company has actively participated in the KSP since 2019, collaborating with countries like Costa Rica, Uzbekistan, Hungary, and Honduras. Committed to its mission of "Making the World a Better Place," IGB & Company has conducted ODA projects since 2008 and continues to stand strong by this guiding motto. To date, the company has successfully completed over 40 projects in more than 20 countries. This year, we are delighted to welcome Lao PDR as another valued project partner with whom we look forward to further collaboration.

On behalf of IGB & Company, I would like to express my deepest appreciation to the Government of Lao PDR, the Ministry of Technologies and Communications, and the Lao National Internet Center (LANIC) for their invaluable collaboration in the project. I extend my profound gratitude to H.E. Boviengkham Vongdara (Minister) and H.E. Keovisouk Solaphom (Vice Minister) for their unwavering support. The successful completion of this project would not have been possible without their dedicated commitment. I also wish to thank the KSP consultation team—Mr. Soohyun Choi (Senior Advisor), Mr. Jaejung Kim (Lead Researcher for Task 2), Mr. Changhyun Yi (Lead Researcher for Task 3), Mr. Youngjoo Ko (Researcher for Task 2), Ms. Ksenia Bakhtiarova (Researcher for Task 1 and 3), and Ms. Seunga Cho (Project Officer)—for their contributions to this report.

This project has greatly benefited from the support and assistance of many others, both inside and outside the Ministry of Technologies and Communications and the Lao National Internet Center of Lao PDR. I extend my deepest gratitude to Mr. Minaxay Philavong (Director General of LANIC), Mr. Phommathat Phoumanivong (Deputy Director General of LANIC), Mrs. Nilapheth Khammoungkhoune (Director of NRCA Division), Mr. Somchai Moua (Deputy Director of NRCA Division), Mr. Anoloth Phanvongsa (CEO of the S-Tech Development Co., Ltd) and all the other participants from Lao PDR.

My heartfelt thanks go out to all those who made valuable contributions to the successful completion of the project, particularly the Center for International Development of KDI. I would like to acknowledge the hard work and dedication of Dr. Jungwook Kim (Executive Director), Mr. Taihee Lee (Project Manager) and Mr. Yeongjin Jeon (Project Officer).

I strongly believe that the KSP projects will be pivotal in fostering and advancing mutual economic and knowledge cooperation between Lao PDR and Korea. Being a part of this project has been a great fortune for us, and it will undoubtedly serve as a catalyst in our shared journey of development and collaboration.

Seung Yong Lee
Chief Consultant
IGB & Company Co., Ltd.

Contents

Tables & Figures

Tables

Figures

Abbreviations

Abbreviation	Definition
ADI	Accountable Digital Identity
AATL	Adobe Approved Trust List
ASEAN	Association of Southeast Asian Nations
ASYCUDA	Automated System for Customs Data
BoL	Bank of the Lao PDR
BCEL	Banque Pour Le Commerce Exterieur Lao Public
CA	Certification Authority
CIO	Chief Information Officer
DB	Database
DID	Decentralized IDentity
DGC	Digital Government Center
DMA	Digital Maturity Assessment
DSS	Digital Signature Software
eIDAS	Electronic IDentification, Authentication, and Trust Services
EU	European Union
FIDO	Fast IDentity Online
GPKI	Government Public Key Infrastructure
HW	Hardware
HRD	Human Resource Development
OCR	ID card Authentication
ICT	Information & Communications Technology
IoT	Internet of Things
e-KYC	Know Your Customer
KSP	Knowledge Sharing Program
KFTC	Korea Financial Telecommunications & Clearings Institute
KICA	Korea Information Certificate Authority
KISA	Korea Internet & Security Agency
KONEPS	Korea ON-line E-Procurement System
KTNET	Korea Trade Network
LCA	Lao Certification Authority
LICA	Lao ICT Commerce Association

Abbreviation	Definition
LANIC	Lao National Internet Center
LSSO	Lao Social Security Organization
MoU	Memorandum of Understanding
MDAs	Ministries, Departments, and Agencies
MoF	Ministry of Finance
MOHA	Ministry of Home Affairs
MoIC	Ministry of Industry and Commerce
MOPS	Ministry of Public Security
MTC	Ministry of Technology and Communications
NPKI	National Public Key Infrastructure
NRCA	National Root Certificate Authority
NW	Network
NMS	Network Management Software
NGOs	Non-government Organization
ODA	Official Development Assistance
OTP	One Time Password
OCSP	Online Certificate Status Protocol
OCR	Optical Character Recognition
PC	Personal Computer
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RA	Registration Authorities
SSL	Secure Sockets Layer
SW	Software
SDK	Software Development Kit
SMS	System Management Software
TSA	Time Stamp Protocol
ToT	Training of Trainers
TLSO	Trusted List Scheme Operator
UPS	Uninterruptible Power Supply
UNDP	United Nations Development Programme

Summary

The Laotian government has established the transition to the digital economy as a national strategy and a plan for entering it, which requires improvements in digital certification and signatures.

To this end, this project seeks to diagnose the digital certificate adoption challenges in the Lao PDR and propose actionable support programs and policy tools to tackle those challenges. In this process, we share the Korean government's existing policies and success stories so that the Laotian government can more effectively achieve its goals.

Overall, based on the current issues in Laos and lessons learned from the best practices, **we propose the following measures to improve the Laotian digital certification:**

- **Supplement and strengthen legal and compliance frameworks to ensure trust:** Lao PDR established a fundamental legal framework for digital certificates with some crucial framework acts still under development. However, specific regulations are required, including ministry-level decrees, adoption guidelines, and monitoring/audit tools for digital certification.
- **Establish centralized and collaborative governance: There is a visible lack of collaboration among the agencies, and many organizations are excluded from the dialogue on digital certification; to promote cohesive digital transformation across ministries, centralized governance under the Digital Government Committee is needed.**
- **Adopt a data exchange framework and integrated ID:** Data sharing among government organizations in Laos is limited and mostly done manually. Moreover, there are no data standards regarding personal identification data, leading to issues with interoperability and authentication services.
- **Digitalize and promote pan-government systems:** Most of the government services in Lao PDR are not digitalized, which means that digital certificates have limited applicability. There are promising developments, as the MOF is implementing the digital signature, but this needs to be expanded further to cover all levels of digital government services.
- **Implement a user-centric digital certificate** service: This is essential to enhancing the technical knowledge and capabilities required for security technology and system construction. It is necessary to be sensitive to current technological trends and apply the latest security technologies and standards to provide a high level of security.
- **Boost the capacity and awareness of digital certificates:** For efficient capacity building, it is necessary to establish a structure responsible for increasing government and public awareness of digital, including digital certificates and authentication.

1. Introduction

Lao PDR has pursued a growth model centered on its natural resources, driven by the aspirations of being "the landlocked country" and "the battery of Southeast Asia" (World Bank Group 2022). This vision has spurred significant investments in infrastructure, such as the Laos-China high-speed railway and the hydropower and mining industries. However, the resource-based economic model shows weaknesses, as it cannot support job creation and the development of value-added industries. This has led to issues in economic and social structures, such as rampant inflation, increasing inequality, under-education, and employment gaps.

Structural reforms are needed to stabilize the economic situation, support a more inclusive growth pattern, and overcome the "resource curse." Thus, the Laotian government has set the transition to the digital economy as a national strategy and established a plan for entering the digital economy. In this context, the Laotian government recognizes the importance of the digital certification system. Despite the government's efforts in developing digital certification, the Laotian digital certificate ecosystem is still nascent. There are several obstacles to the active usage of digital certificates, such as a lack of trust framework, limited interoperability, dominance of paper-based government processes, and lack of digital awareness and capacity.

To address these challenges, Lao PDR seeks to learn from the experiences of other countries, including Vietnam, Korea, and Estonia, to vitalize its digital certificate ecosystem. This has led to the current project, which aims to improve the policy environment for restructuring the national digital certification system and contribute to economic development through digital economy transformation. It is expected that upon completing this project, the Korean experts, in collaboration with Lao National Internet Center (LANIC), will develop realistic policy recommendations, a roadmap, and a To-Be model of the Laotian Digital Certification System. This report will become the blueprint of the new Digital Certification System and a guiding document for regulatory, policy, and capacity improvements.

2. Status Analysis

2.1. National Certification Policies and Legislation

2.1.1. Status Analysis Methodology and Structure

Progress has been made in conducting status analysis and advanced case studies of four pillar areas expected to impact the roadmap derivation for the Laos Digital Certification System. This includes an analysis of the status in Laos and advanced cases, followed by a gap analysis between advanced cases and the status in Laos to derive a roadmap for developing the Laos Digital Certification System.

Table 1.
Main Focuses of Status Analysis by Pillar

	Analysis Fields	Analysis Focus
Pillar 1	Policy and Legislation	Deriving improvements in digital government, policies, and legislation related to digital authentication is essential for activating digital authentication.
Pillar 2	Organization and Stakeholders	Improvement plans for digital government policies and certification-related organizational governance to activate digital government policies and certification.
Pillar 3	Technology and Standardization	Identifying new digital certification technologies and improving plans for standardization to advance digital certification technology.
Pillar 4	Capacity Development and Awareness Enhancement	Identifying capacity development and awareness enhancement plans for government and private sector digital government and certification.

2.1.2. Status Analysis and Improvement Directions Research

The analysis of Laos' digital certification status focuses on identifying and improving digital certification needs in government services (G2G, G2B, G2C) and private sector services like financial services. The research included both quantitative and qualitative aspects. More specific information on each research step is provided below.

Firstly, in terms of policies and legislation, an analysis covers the Lao government's top-level policies related to digital certification from 2021 until 2040, including the National Digital Economy Strategy (5-year policy, 10-year strategy, 20-year vision), as well as the ongoing Digital Government Master Plan being implemented by the Digital Government Center (DGC). The study examines digital certification policies' correlation and development direction under the Lao digital government's policy framework.

Furthermore, the study includes a survey of the legal status of digital certification policies, which form the basis of digital certification. This consists of assessing relevant laws such as the e-Transaction Law, a prominent law amended in 2022 concerning electronic signatures, and the Bank of the Lao PDR (BoL) Payment System established in the finance sector in 2018. Since no comprehensive legislation supports digital government policies, plans have been conducted to search for the right direction for legislative improvements.

Secondly, in the field of certification-related information systems and standardization, the study covers the status of services provided by the Lao government, which has been offering Public Key Infrastructure (PKI)-related systems supported by the Vietnamese government since 2023, in the forms of government services (GPKI) and private services (NPKI). The study examines the status and issues of digital government services, primarily focusing on e-Office and plans and policy directions for expanding government services using digital certification technology in areas such as Ministry of Finance (MoF)'s Government Financial Management System (GFIS), Tax Payment System (TaxRIS), Customs System (ASYCUDA), MoIC's Enterprise Registration System, among others. The study also identifies priorities for applying digital certification technology in government services and its direction.

Moreover, this research investigates the status of private financial services provided by institutions like BoL and commercial banks such as Banque Pour Le Commerce Exterieur Lao Public (BCEL), which hold over 70% of the financial transaction market share, and telecom operators like Lao Telecom offering M-Money services. Upon the assessment, the team presents recommendations regarding developing convenient certification technologies and applying PKI and Fast IDentity Online (FIDO) technologies.

Thirdly, from an organizational and stakeholder perspective, the study examines governance structures such as LANIC overseeing Root CA in the administrative sector and institutions involved in financial certification services like BoL, BCEL, Lao Telecom, etc. The research proposes improvements in integrating digital certification governance in the digital administration and finance sectors. Additionally, the Digital Transformation Committee – the overarching governing body for digital certification systems in the digital government domain – was formed in 2023 and is still in its early operational stage. As a result of the assessments, the team suggests future directions for further establishing subcommittees and working groups to activate digital certification.

Fourthly, regarding capacity building and awareness improvement activities related to digital certification by the Lao government, assessments based on the Digital Maturity Assessment conducted by UNDP in 2022 and the Digital Readiness Survey results illustrate a fundamental level of digital maturity with a score of 1.7 out of 5. This indicates a need to focus on capacity building and awareness improvement in digital government and digital literacy before specifically addressing digital certification.

Consequently, research has been completed on the Lao government's policies and plans regarding establishing training centers such as e-government Education (or Training) Centers to provide overall digital and ICT education to government officials, digital certification service personnel from other government agencies, and the public. This research serves as a basis for designing comprehensive digital government, digital certification, and digital capacity development education programs online and offline and exploring collaboration strategies with local governments.

Additionally, awareness improvement activities are being pursued to address the necessity and proliferation of digital certification. Committees, including digital certification subcommittees under the Digital Transformation Strategy Committee or Digital Transformation Task Forces, have been established in coordination with MTC-affiliated organizations such as DGC, MoF, Ministry of Industry and Commerce (MoIC), Lao Social Security Organization (LSSO), etc., to promote the spread of digital certification in inter-agency digital service activation. This research covers organizational structures, programs, and projects to enhance awareness and spread digital certification services between government agencies. Considering the overall low level of ICT utilization, programs to increase digital literacy among the public are deemed urgent. Collaboration with private entities, such as commercial banks and telecom operators centered around the BoL, is considered when proposing programs for enhancing digital literacy as a Universal Service of Telecom Carriers or incumbent ISPs.

2.2. Digital Certificate Ecosystem Status

2.2.1. Overview

From an ecosystem perspective, the elements appear fragmented. While the National Root Certificate Authority (NRCA) actively promotes PKI adoption, there is a lack of visible cooperation among identity credential providers, CAs, and verifiers such as banks and government organizations.

2.2.2. Supply and Demand Analysis

The team approached the in-depth digital certificate ecosystem analysis from the demand and supply perspective to more comprehensively delineate current developments and issues.

From the supply side, the LANIC and the Ministry of Technology and Communications (MTC) began the development of the Certificate Authority in 2017. The first step was establishing the Lao NRCA organization in collaboration with the Vietnamese NRCA.

The Lao NRCA is responsible for the overall implementation of CA, including Root CA management, standard & policy management, SubCA management and training, promotion, and international cooperation. NRCA issues USB Token and Soft key methods, but the current digital certificate system has limited functionality. The NRCA seeks system improvements, such as cross-connection between countries (Root-to-Root), to support the ICO 9303 standard.

Lao Certification Authority (LCA), also known as Wintech, issues and manages Public Certificates. LCA also cooperates with private Registration Authorities (RA) – Unitel, s-Tech, Datacom – to implement and promote digital certificate adoption. Although the LCA can issue both tokens and soft keys, only remote signs are issued, as hardware tokens are prone to loss and damage. LCA trained and authorized Unitel and LaoCom to manage digital certificates through an online system. However, some users still prefer to contact LCA for digital certificate issuance because of the quality of the service. RA users can enter the LCA portal to access certificate management functions, such as issuance, revocation, and statistics.

As for alternative digital authentication methods, most systems and services rely on Know Your Customer (KYC) and One Time Password (OTP) methods. Because there is no legal basis for enforcing a unified KYC system for all systems, Lao KYC is not a unique infrastructure. Thus, service providers like LOCA, M-money, and BCEL developed KYC modules to authenticate identity. KYC methods rely on the "3-gap" (three-step) method. The 3-gap rule implies a three-step verification: mobile number, photo of an ID document, and a photo of the account bearer with the given ID document. Without linkage to identity databases, this process creates an additional workload, hampers transaction security, and increases identity check error rates.

The Bank of Lao owns and operates the LaPASS system for bank transactions. It is based on the PKI infrastructure, so inter-bank transactions are encrypted. LaPASS has 43 participants (40 commercial banks, the Ministry of Finance, LAPnet Company, and Lao Securities Exchange). Most participating banks have not yet achieved Straight-Through Processing and rely on manual procedures to submit transactions to the Real-time gross settlement (RTGS).

2.2.3. Ecosystem Assessment

The team conducted an ecosystem assessment according to the Info-Tech Research Group framework to make the As-Is analysis results more objective and quantifiable and collaborated with the Laotian local consultants.

Figure 1.
Lao PDR Digital Certificate Ecosystem Assessment Results

Category	Readiness	Factors and Considerations
Public-Private Partnership (PPP)	77%	• Digital Certificates in Laos are implemented based on public-private partnership; most government solution development is outsourced to private companies • PPP Legal framework established by Law No. 624/GOV in 2020 • **It would be beneficial to explore some private-public funding options**
Security	70%	• MTC has recently established SOC under LaoCERT with assistance from Vietnam MOIC. • However, staffs and equipment are lacking; digital certificate risks are not clearly defined
Usability/ Services	50%	• LANIC identified some use cases and selected pioneer organizations (e.g., MOF) • Government-supported eKYC in place, but. no standardized process for all KYC • **E-Office is struggling to be the "killer application"**
Enterprise Governance	50%	• Roles and responsibilities on digital certificates are defined, **but there are some overlaps or mismatches in R&R** • Information and initiative silos within and outside the MTC
Compliance Framework	50%	• **General compliance provisions on digital certificates are in place, but more specific regulations required** • Each Lao Ministry also has its own regulations that often do not align with the digital certificate compliance provisions
Capacity and Awareness	50%	• **Low awareness on digital certificate in government organizations and among citizens** • The training and promotion attempts are sporadic, need a more systematic approach
Legislative Coverage	50%	• The legal framework on digital certificates exists to some extent. However, it lacks enforcement • **The legal framework lacks provisions on Digital ID** • No policies and plans on the promotion and expansion of digital certificates
Trust Framework	43%	• **Exclusion of MOHA, MOPS etc. credential holders** • **Lack of clearly defined and enforceable trust framework and standards** • Data Privacy Law is in place, but provisions on credential data privacy need work
Interoperability	30%	• **No integrated ID; separate ID data standards (e.g., MOPS, MOHA, MOFA)** • **Data exchange layer or interoperability framework not implemented**

Upon the assessment, the Laotian digital ecosystem is still nascent. The primary legal and policy framework is in place, but it lacks detail and enforcement. The lack of a digital transformation plan and overarching standards has also created siloed systems, and legal frameworks need further strengthening and detail. Interoperability and Trust framework are the weakest areas in the Laotian digital certificate ecosystem. First, the trust framework in Laos, which has appropriate standards and practices, is not yet established. Credential holders, such as Ministry of Public Security (MOPS) or Ministry of

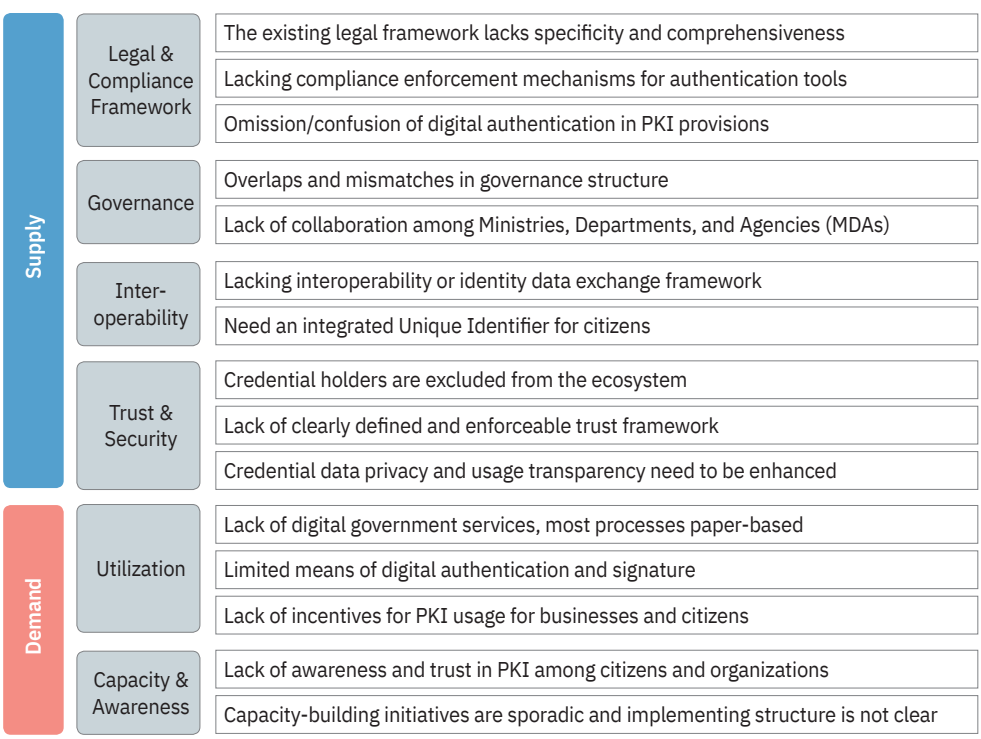
Home Affairs (MOHA), which are crucial for identity verification, are excluded from the ecosystem. Not only does this significantly reduce the reliability of digital certificates, but it also reduces the credibility of other authentication methods like KYC.

The LANIC shows effort in capacity building and awareness raising, such as training the NRCA in Viet Nam and awareness presentations in some Lao PDR regions. However, a comprehensive capacity-building plan that would include a spectrum of initiatives for different layers of the organization—from hands-on staff to policymakers—is needed.

2.2.4. Implications

Based on the Laos status analysis and readiness assessment, the team has drawn implications from the digital certificate environment and status from a supply versus demand perspective.

Figure 2.
Implications for Digital Certificate Ecosystem of Lao PDR by Area

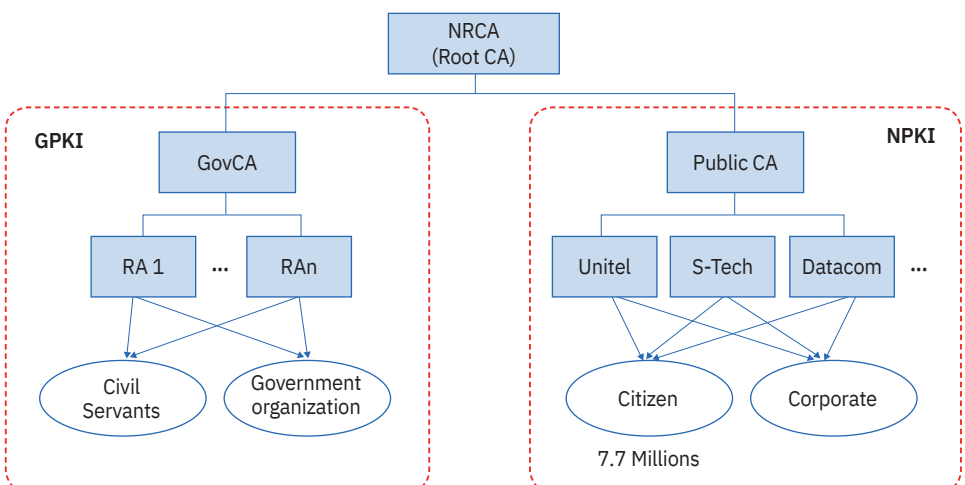


2.3. Digital Certificate Systems

The Lao NRCA is responsible for the overall implementation of CA, including Root CA management, standard & policy management, SubCA management and training, promotion, and international cooperation.

LCA, also known as Wintech, issues and manages Public Certificates. LCA also cooperates with private Registration Authorities (RA) – Unitel, s-Tech, Datacom – to implement and promote digital certificate adoption. Although the LCA has the authority to issue both tokens and soft keys, only remote signs are issued, as hardware tokens are prone to loss and damage.

Figure 3.
Laos Digital Certificate Model



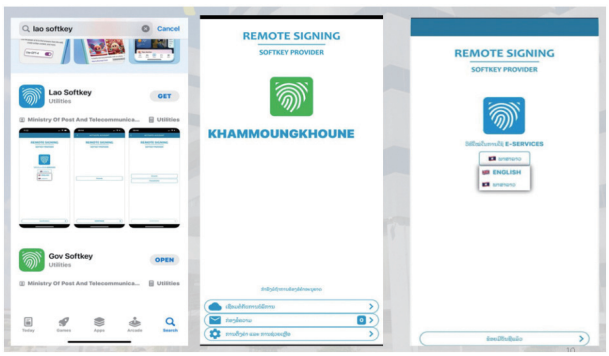
Source: compiled by the consulting team based on LANIC (2023).

The certification system is designed to ensure service continuity with hardware and software redundancy. While a disaster recovery center is not currently in place, plans for its establishment are being developed. LCA operates a remote signing service (RSSP) website, which allows users to purchase and download services like a personal digital signature, an enterprise digital signature, and a digital stamp. It also will enable renewals of personal certificate licenses and enterprise certificate licenses.

Remote Signing Service:

- Certificate Storage Location: Cloud
- Location of Electronic signature creation: Cloud
- User Authentication Method: ID/Password
- Mobile App: Lao Softkey

Figure 4.
Remote Signing App: Lao Softkey



Source: LANIC (2023).

The LANIC data center has obtained ISO27001 and Bureau Veritas certification. It has multi-factor authentication (ID card/fingerprint) access control, disaster preparedness equipment, temperature and humidity control, and UPS.

The certification system consists of the Root CA (Root Certificate Authority), GovCA (Government Certificate Authority), and Public CA (Public Certificate Authority). It is deployed across three separate racks inside steel cages within the data center, with hardware security modules, CCTV surveillance, and safes installed for added security.

Figure 5.
PKI Center in LANIC Data Center

The e-office system is the first system that the Laotian government attempted to integrate digital certification services with. Developed by the DGC of the MTC, it has been supplied to 17-18 ministries. Initially, digital certification was developed for senior government officials who relied on the USB token certification. However, Softkey has been added as an additional means for digital signatures.

Other applicable government digital services include MoIC's Business Registration System and MoF's TaxRIS (tax system), GFIS (financial management system), and ASYCUDA (customs system). In 2022, MTC and MoF ministers signed an Memorandum of Understanding (MoU) on activating digital government services through digital certification, thus boosting digital certificate-related cooperation between LANIC and MoF.

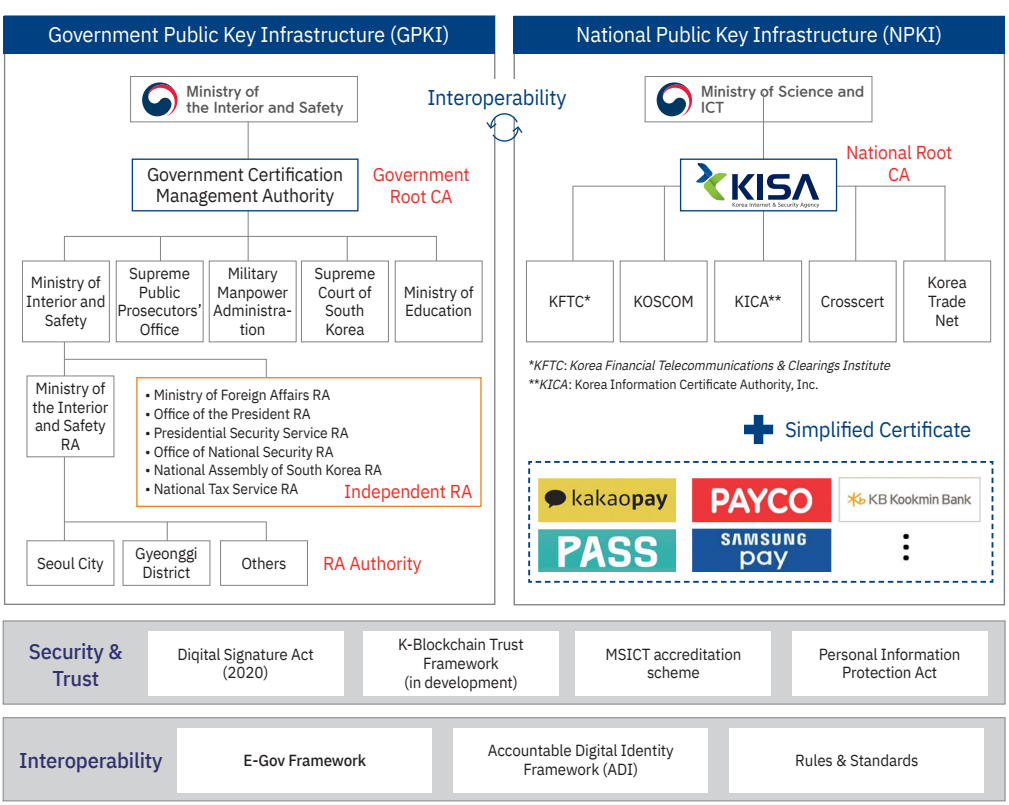
3. Case Studies

3.1. Korea

Korea's electronic signature system operates under two systems: Government Public Key Infrastructure (GPKI), which is built under the e-transaction law, and National Public Key Infrastructure (NPKI), which is built under the e-Signature Law. Importantly, E-Signature has the same legal effects as a hand-written signature.

In the case of GPKI, the Ministry of the Interior and Safety is the Root CA, and there are five certificate authorities (the Ministry of Interior and Safety, the Supreme Public Prosecutors' Office, the Military Manpower Administration, the Supreme Court, and the Ministry of Education). In the case of NPKI, the Korea Internet & Security Agency (KISA) is the Root CA, and five organizations are the representative certificate authorities: the Korea Financial Telecommunications & Clearings Institute (KFTC), KOSCOM, the Korea Information Certificate Authority (KICA), Crosscert, and the Korea Trade Network (KTNET).

Figure 6.
Korean Digital Certificate Ecosystem



Source: All that Digital Gov. KOREA (2021).

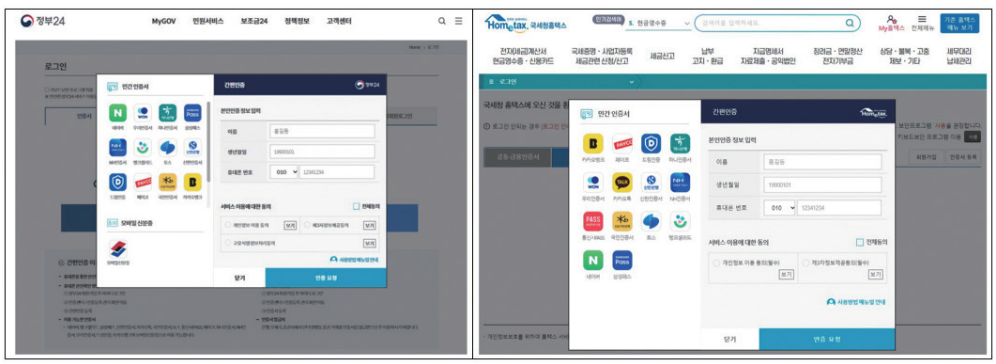
In 2020, after the revision of the Digital Signature Act, in addition to the five accredited certificate authorities, the 'private certificate' market was introduced with the participation of various mobile operators, financial companies, e-commerce, and fintech companies. This amendment was crucial, as it not only diversified the market but also enhanced the quality and accessibility of the digital certificate service. Digital signature and authentication services are essential for financial services, and synergy effects with fourth industrial revolution technologies such as big data, blockchain, and IoT are expected.

Technically, Korea's mobile authentication is linked to a web server-based e-government framework and follows the Accountable Digital Identity (ADI) framework developed by the Decentralizaed IDentity (DID) Alliance. The e-Government Standard Framework is a standardized development framework for each platform in Korea's public sector informatization project. The development framework supports efficient application construction by creating and providing the functions and architecture necessary for information system development in advance. Regarding the trust framework, Korea adheres to WebTrust, a system that verifies whether the certificate authority is issuing certificates through a transparent and reliable process. If it passes WebTrust, it is registered as a trusted authority by most operating systems and web browsers. In Korea, the Ministry of Interior and Safety, the Ministry of Education, and KISA have been certified by WebTrust and have followed Secure Sockets Layer (SSL) security since 2015.

In Korea, most e-government and e-commerce services are secured by electronic signatures to ensure authentication, integrity, and non-repudiation. E-authentication is actively used in e-government services such as e-taxation, e-civil services, and e-procurement and e-commerce services such as Internet banking, Cyber stock, and e-shopping malls.

Korea National Tax Service has been providing Home Tax Service (HTS), which allows people to make tax payments at home without visiting a tax office. By improving user convenience, such as Web Accessibility, the use rate of HTS is higher than in the U.S. (57%) and England (33%). Also, people can obtain birth, family relationships, tax, and land certificates through the 'Government 24' online portal by logging in with e-authentication. Bidding documents are submitted after being digitally signed and enveloped two times. An e-procurement system, KONEPS, checks the integrity of the bidding documents and stores the enveloped documents in the Database until the bid opening date. On the bid opening date, all the enveloped documents will be decrypted, and the integrity of the documents will be verified by digital signature.

Figure 7.
PKI Enabled E-Government Service in Korea



E-Government Portal Home Tax Service

- **Improved Convenience:** Allow citizens to access government services anytime, anywhere, which is especially beneficial for those living in rural areas
- **Time and Cost Savings:** The time required for document preparation, submission, and processing has been significantly reduced.
- **Increased Transparency:** Electronic signature enhances data transparency and improves information accessibility.
- **Reduced Environmental Impact:** Decreasing paper use helps conserve natural resources.
- **Enhanced Administrative Efficiency:** Automated processes reduce administrative errors and speed up processing.
- **Enhanced Security:** Provide authentication, non-repudiation, integrity, and confidentiality to protect personal information and data security.
- **Increased Reliability:** Enable users to securely log into government websites and services and boost the reliability of e-government services.
- **Strengthened Legal Validity:** Provide legal validity to electronic documents and digital signatures.

3.1.1. Lessons Learned

South Korea's official certification system began with the Electronic Signature Act, enacted in 1999 to promote e-commerce. At the time, Korea's E-Signature Law created an "electronic seal certificate" by adding the owner's information to the PKI because there was no way to verify the other transaction party. Although the digital certificates were mandatory and thus ubiquitous, several concerns have been voiced: the fact that PKI-based authentication technology was used only in a few countries, a possible monopoly on the market, increased limitations on people's right to choose

authentication methods, and obstacles to technology and service innovation.

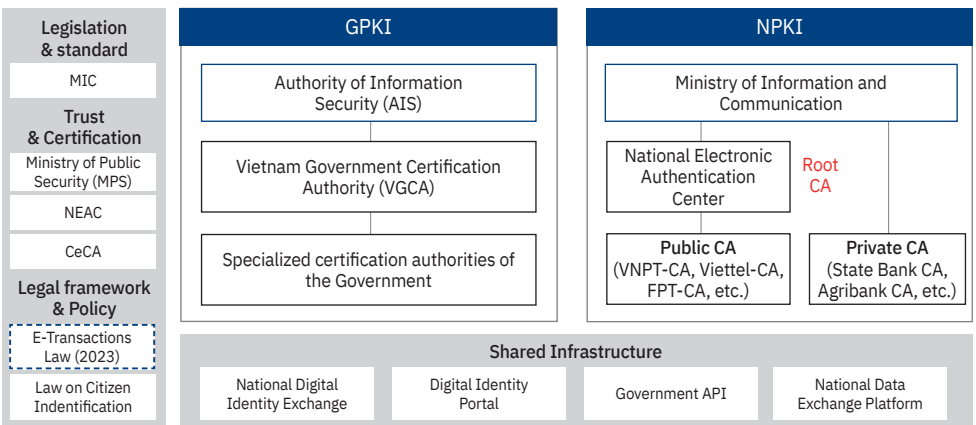
In particular, the public certificate was operated as an 'Active X' plug-in-based service, and its use was restricted to operating systems (OS) and browsers other than Microsoft Windows and Internet Explorer (IE). Users began to feel the inconvenience of having to install 'Active X' and dozens of security programs when using public certificates and renewing them every year.

To respond to the changing digital service landscape and consumer demands, with the passage of the amendment to the Electronic Transactions Act in 2014, the provision on the mandatory use of certificates was removed. However, since the authentication system legally granted by the government was already established for most users, the influence of public certificates continued until 2020, when the Digital Signature Act was amended to eliminate the monopoly of public certificates. Transitioning the certificate to the KFTC cloud and setting the renewal period to three years solved storage and renewal difficulties. Plus, abolishing obligatory government certificates allowed the selection and use of certificates from private CAs, such as Kakao, Naver, Kookmin Bank, and Toss.

3.2. Viet Nam

Similar to Korea, Viet Nam has a twofold digital certificate governance structure. Thus, the Viet Nam Authority of Information Security is responsible for the GPKI insurance, whereas the Ministry of Information and Communication (MIC) is responsible for NPKI. Vietnamese structure also includes trust and certification authorities, such as the Ministry of Public Security as a credential holder, the National Electronic Authentication Center (NEAC) as the Root CA, and Electronic Contract Development Axis (CeCA). According to the NEAC, as of 2020, approximately 30,000 certificates were issued to Vietnamese government ministries and 60,000 certificates to local governments. Public CAs often include telecom companies. As of February 2024, there are 25 digital certificate providers, with Vietnam Posts and Telecommunications Group (VNPT) being the most significant player (270,000 certificates issued in 2022). There are also six Private CAs – primarily banks – licensed by the MIC.

Figure 8.
Viet Nam Digital Certificate Governance Model



Source: compiled by the consulting team based on NEAC (2023).

In general, Viet Nam's regulatory framework fully recognizes the legitimacy of e-signature, which satisfies the requirements specified in the Law on Transactions 2023. Notably, this law follows the UNCITRAL Model Law, which ensures the Vietnamese legal framework's adherence to global standards. The law applies to all areas of transactions, potentially facilitating the adoption of digital signatures (Vu, 2023).

The electronic identification specified in Decree 59/2022/ND-CP can replace traditional paper documents and identify citizens in the digital environment. Digital signatures are also officially recognized as replacing traditional signatures in business and banking transactions. However, as only about 30% of the government services in Viet Nam are digitalized, the scope of digital certificate applications is somewhat limited and focused on G2B services. Currently, Viet Nam enabled digital certificate usage for some of the investment commercial matters:

Table 2.
Examples of Services Allowing Digital Certificate Use: Viet Nam

Authority	Process
Ministry of Planning and Investment	Business Registration/Incorporation via the National Business Registration Portal
Tax Authority	Declare and pay taxes via the E-Tax website
Viet Nam Social Security	Register for online public services on the Portal

Source: Hoang (2022).

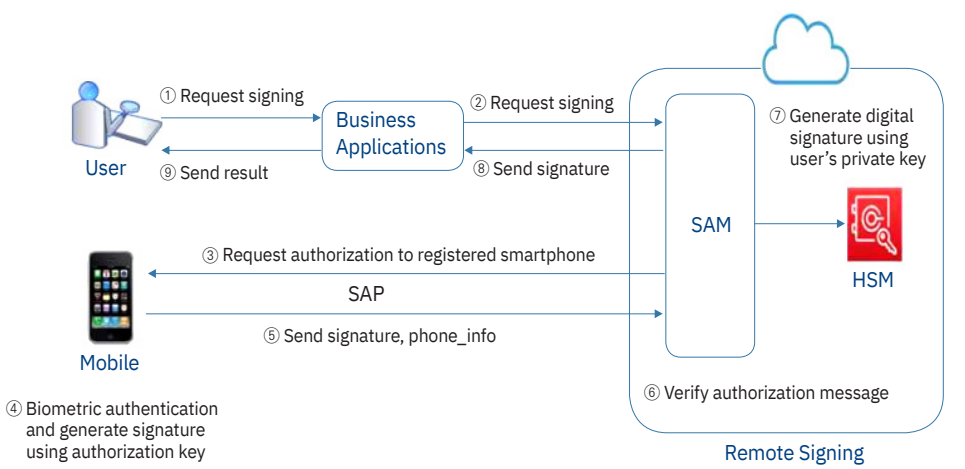
According to NEAC, 100 percent of enterprises have used digital signatures in transactions, mostly tax declarations, customs, and social insurance. Nevertheless, the number of people having personal digital certificates remains modest, as the ratio of

individual certificates did not exceed 23 out of 2.1 million active public digital certificates in 2023. These certificates are often used in tax reports, payments, and social security services.

To facilitate the certificate uptake, NEAC has provided digital certificates under the remote signing model, which is expected to be integrated into payment platforms and apps. As of the end of 2022, MIC had granted licenses to provide digital signature service under the remote signing model to seven public CAs and SIMPKI (Subscriber Identity Module Public Key Infrastructure) to two public CAs.

Remote signing is a service that provides digital signature services using subscriber private keys and certificates safely stored in the cloud. It must meet the European Union's eIDAS (Electronic Identification, Authentication, and Trust Services) regulations and be licensed separately from the existing certification authority license. As of August 2023, ten agencies were designated remote signature service providers.

Figure 9.
Process of Remote Signing



Note: SAM (Signature Activation Module)
SAP (Signature Activation Protocol)
HSM (Hardware Security Module)
Source: compiled by the consulting team based on MySign Service of Viettel-CA.

3.2.1. Lessons Learned

Despite being regulated by Vietnamese laws, E-Signatures are not as frequently and widely used in transactions and documentation signing in Viet Nam. This is due to their limited scope and usage benefits presently in Viet Nam. With only around 30% of public services digitalized, citizens and businesses may feel discouraged from adopting a new technology. Also, there is still a persistent paper-based culture, so it will take some time before Viet Nam becomes accustomed to being completely digital. Moreover, as

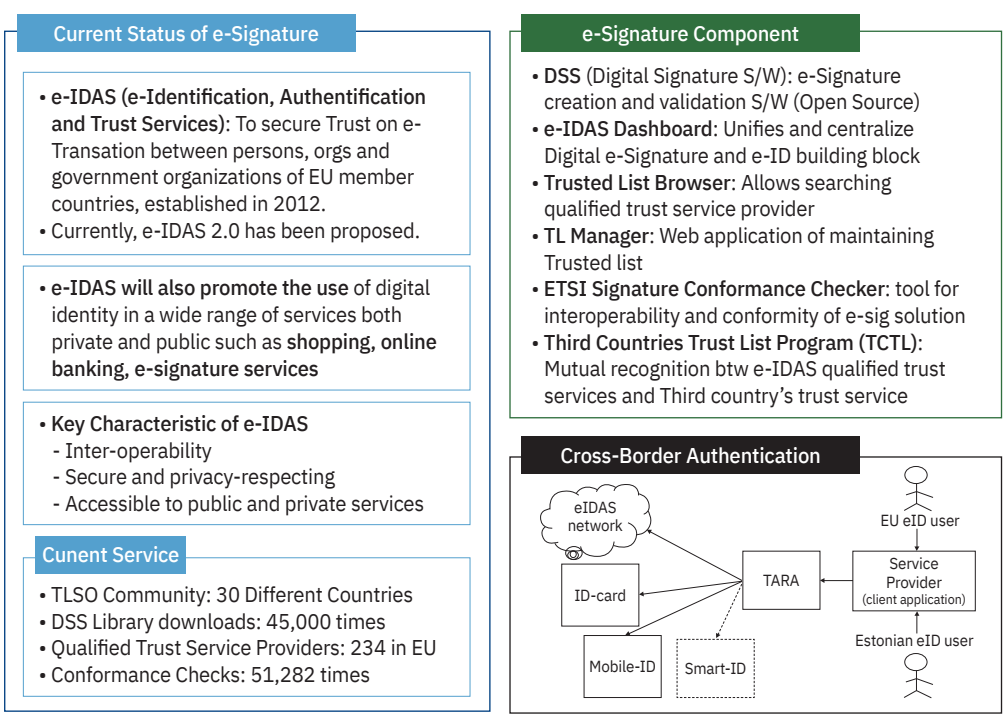
mentioned before, digital certificates come with a cost, which is often prohibitive for small companies and individuals.

In the past few years, Viet Nam has seen significant developments in digital certificates, particularly the recent recognition and rollout of eIDs. Moreover, Viet Nam followed best practices by establishing a data exchange infrastructure and integrated identification databases, which are core factors in the trust and usability of digital certificates. Despite certain limitations, Viet Nam has seen decent government and private organizations issuance numbers. With more standardization, capacity building, and funding solutions, Viet Nam will likely succeed in full-scale digital certificate adoption.

3.3. EU and ASEAN

3.3.1. Digital Certificate System in the European Union

Figure 10.
EU Case Study



Source: compiled by the consulting team based on e-IDAS regulation from the European Commission Web Site and State Authentication Service (TARA) Technical description.

e-IDAS, established in Europe in 2012, is a regulation for "e-ID authentication trust services," initially proposed by Estonia. According to this regulation, Estonia provides

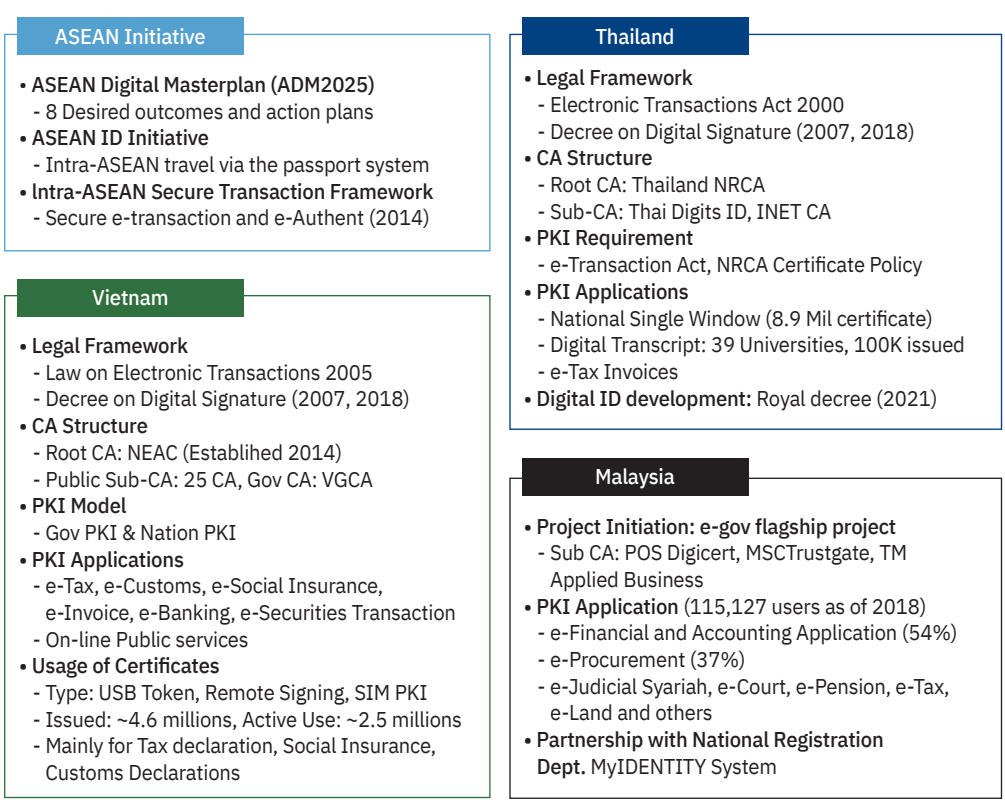
authentication services across EU member states' borders. To ensure seamless authentication services among EU countries, even for newly admitted EU member states, service providers must comply with the e-IDAS regulation and be included in the Trusted List (TL).

Key digital authentication services under the e-IDAS regulation are utilized for electronic signature services such as shopping and online banking across EU member states, primarily in Estonia. These services are accredited in over 30 countries, with 235 service providers across the EU meeting the e-IDAS authentication standards. The number of certifications is increasing rapidly, with over 50,000 assessments completed, indicating a growing trend of digital services meeting these authentication standards.

For example, Estonia's e-government services include TARA, an electronic authentication service. Individuals can use various methods such as ID cards, mobile IDs, Smart IDs, and EU e-IDs for electronic authentication to access multiple e-government services.

3.3.2. Digital Certificate System in ASEAN member countries

Figure 11.
ASEAN Case Study



Source: Compiled by the consulting team, based on International Symposium Materials from ASIA PKI Consortium and Government Public Key Infrastructure of Malaysia.

Based on the literature review, we analyzed the status of national digital authentication usage in major ASEAN countries.

As a shared feature for all ASEAN countries, the ASEAN Digital Master Plan (ADM 2025) has been undertaken as a fundamental digital policy, including digital trust-related goals among its eight significant objectives. In addition, ASEAN rolled out an ASEAN ID Initiative to explore using passport authentication for cross-border movement.

In Viet Nam, the e-Transaction Law was enacted in 2005 and revised in 2023, with the Digital Signature Decree supporting the law. Organized efforts have led to establishing the NEAC as the Root CA in 2014, currently operating 25 Sub-CAs. Digital authentication services are primarily utilized in e-tax, e-customs, social insurance, banking, securities trading, and other public services. Authentication certificate types include USB tokens, remote signature authentication, and SIM PKI certificates, with over 4.6 million certificates issued and approximately 2.5 million actively used.

Thailand enacted the e-Transaction Law in 2000, and NRCA and two sub-CAs were established organizationally. Authentication certificates are predominantly used in government portals such as the National Single Window and e-Tax systems and for issuing academic transcripts in many universities.

Malaysia has pursued digital authentication as a key initiative under its e-government Flagship Program, with approximately two sub-CAs established. Digital authentication is applied in e-finance, e-tax, e-procurement, and digital administrative services in judicial bodies and pension systems, contributing to its active utilization.

3.4. Gap Analysis

Table 3.
Gap Analysis

Pillar	Sub-Component	Laos	Advanced Cases	Note
Policies & Legal Framework	Digital signature law	○	○	
	Digital government law	X	○	
	Digital payment law	○	○	
	Digital signature-related policy	○	○	Laos Digital Vision, Strategy, Plan
	Sectoral legal revision for digital administerial environment	△	○	
	Digital government policies related to digital signature development	○	○	UNDP Digital Government Strategy & Masterplan
	Mandatory use policy of digital signature should be expanded to MDAs when building application	X	○	Need to confirm with Decree for details

Table 3. Continued

Pillar	Sub-Component	Laos	Advanced Cases	Note
Technology & Standard	Digital signature certificate system	○	○	
	Number of issued certificates	Low	High	
	Remote signing	X	○	
	Simple authentication	○	○	
	Bio-based identification	Middle	High	
	Block-chain-based digital ID	X	○	
Organization & Stakeholder	Government-wide Digital Government steering committee	△	○	Launched in 2023
	Digital signature dedicated organization	○	○	
	Application systems supported by digital signature	Scarcely	Plenty	
	Regular meetings for inter-MDA digital government development	X	○	
	Inter-government cooperation between MDAs	Low	High	
Capacity-building & Awareness	Dedicated government training center	X	○	
	Training program for digital signature operators	Low	High	
	Training program for government officers	Low	High	
	Training program for citizens	X	○	
	Budget for capacity building	Low	High	
	Inter-MDA training program or plan for other MDAs	X	○	

Table 3 presents the results of a gap analysis conducted through surveys of the status in Laos and advanced/similar case studies. The main implications of the gap analysis are listed below.

1. Policy and Legal Aspect: Efforts are underway to formulate digital e-government policies and legislation by 2040. However, substantial support in the form of detailed regulations, including decrees and sub-regulations, is needed to supplement this. The enactment of fundamental laws such as the Electronic Government Law is crucial for significant advancements in digital certification.
2. Technological/Standardization Aspect: While Laos has initiated digital certification services based on a PKI system supported by government backing, their utilization remains minimal. The dependence on face-to-face certificate issuance and the lack of widespread adoption pose challenges. Financial sector certification services primarily center on the BoL but are dominated by service providers like BCEL and M-Money. Standardization efforts are lagging, with no integrated

technical standards in place. The e-NID initiative, developed in collaboration with Huawei over a decade ago, lacks widespread adoption due to incomplete regional dissemination and the absence of IC chips.

3. Digital Government Organization & Stakeholders: Forming key bodies, such as the Digital Government Transformation Committee, chaired by the President, is a critical step. However, concrete discussions and collaboration on specific agendas have not yet materialized. A robust e-government governance framework is deemed necessary to prioritize inter-agency cooperation and establish digital government services effectively. Close collaboration between LANIC and DGC and the formation of internal working committees within MTC are essential for digital service expansion and certification proliferation. Setting up a dedicated committee under the Digital Government Working-level Committee to prioritize applying digital certification technology in services like TaxRIS and ASYCUDA is necessary.
4. Digital Literacy: Given Laos' low digital literacy level (1.8/5), initiatives to enhance the digital literacy of government officials and citizens are crucial. Establishing dedicated e-government training centers for government personnel and conducting e-government education through these platforms is necessary. Evaluation of e-government levels among ministries to foster healthy competition and improve digital literacy is recommended. Activating education on digital certification and e-government services within this category is seen as beneficial in activating digital certification.

4. Policy Implications

This project reviewed and analyzed the current state of the digital certificate ecosystem, including policies, legal framework, governance, services, and infrastructure. The KSP research team developed three groups of recommendations based on the analysis of the Laotian As-Is status and case studies.

4.1. Legal Framework Improvement Plan

Although Lao PDR established a basic legal framework for digital certificates, several weaknesses need addressing. Hence, the team developed suggestions on the legal framework as follows:

4.1.1. Promulgate the Digital Government Framework Act

Currently, Laos has several acts on different components of digital government, such as electronic transactions, electronic signatures, e-commerce, and information protection. However, the Digital Government Act (DGA) is still under development. The Lao Digital Transformation Masterplan Draft (2022) includes enacting this act as one of the action items. While the Act does not usually directly address digital certificate adoption, it can facilitate the implementation of digital certificates in several ways. First, by recognizing digital as the basis for internal and external government processes, the DGA promotes digitalizing government records and transactions. Organizations inevitably use digital certificates to ensure the authenticity and integrity of electronic documents and transactions. Second, the DGA may include provisions or requirements for government agencies to implement robust security measures, which could involve using digital certificates to authenticate users and secure data transmissions. Third, the DGA should include interoperability among government systems as one of its goals. As digital certificates are crucial in securing data exchange between organizations, nudging interoperability can also encourage the adoption of standardized digital certificate formats and protocols.

4.1.2. Adopt a detailed legal framework for digital certification that includes digital authentication

Laos's digital certification legal framework is expressed in e-transactions and e-signature laws, but detailed regulations are lacking. Many articles define only general

features of the law subject, but there are few provisions on the scope of application and enforcement, violation criteria, and relevant punishment. A legal framework that requires the adoption of digital certificates is needed.

Existing e-transaction and e-signature laws in Laos typically lack implementation assessment and monitoring provisions, which weakens law enforcement. Thus, it is essential to incorporate articles allowing digital certification implementation monitoring as a means of enforcement. To vitalize the digital certificate ecosystem, Laos needs a legal framework that recognizes digital authentication based on PKI and describes its scope of application. Digital certificates, such as KYC, should become a basis for all simplified digital authentication.

Overarching laws for digital certificates may not be enough to enforce the adoption of this technology, as the wet-ink culture is still dominant. Ministerial-level regulations that recognize and even require the digitalization of government processes will substantially affect separate organizations and thus act as supporting pillars for existing framework acts.

4.1.3. Enhance terms and provisions on user data privacy, utilization, and sharing

Although Lao PDR has a Law on Electronic Data Protection in place since 2017, there is still little enforcement regarding data protection and usage transparency. These issues are critical when dealing with digital certificates and identity, as these services require information on the most crucial individual details. The Laotian Electronic Data Protection Law has no data protection officer. The law also needs to provide additional identification possibilities as a criterion for Data Ownership.

By law, all data requires consent from the Information Owner to be collected, and many services in Laos, including the digital certificate system, do not collect users' consent.

Furthermore, the Law could be improved by specifying the exact nature of the "other acts that violate the law." The law should provide more specific details on the measures for educating, warning, disciplining, fining, or penalizing violators.

4.1.4. Develop specific compliance and trust regulations with redress mechanisms

There is a lack of compliance and trust regulations for digital certificates in Laos. The legal framework should further define and enforce certificate issuance and management policies. This includes specifying approved CAs, crypto standards, certificate lifetimes, and trust levels. The legal framework should consist of minimum

criteria for the CAs.

To install the trust framework for digital certificates, Laos must adopt principles and standards that organizations can adhere to in digital certificate implementation. These rules shall assure organizations that they all work in an aligned and trusted way and that they can trust credentials presented by a user. These rules must be supported by redress and infringement prevention mechanisms to ensure enforcement. Given the potential risks of digital authentication and certification infringement, it is necessary to install a robust penalty framework; however, a separate redress mechanism is needed to ensure that ecosystem participants can solve the issues collectively.

4.1.5. Review current regulations to include audit and reporting mechanisms

The legal framework on e-signatures, including CA regulations, does not include any auditing provisions. Thus, it is necessary to supplement the existing legal framework with an auditing mechanism that oversees the ecosystem members and ensures that every organization adheres to the given laws and standards.

The framework laws should mention the auditing and reporting mechanisms, whereas by-laws, instructions, and guidelines can describe specific auditing mechanisms. A certified auditor can carry out audits to ensure transparency and objectivity.

It is useful to refer to the international standards for implementing such audit frameworks. For example, eIDAS introduced a six-step audit process involving the organization's internal preparation, auditor selection, audit process, and certification. The audit usually includes examining the organization's systems, policies, and procedures to ensure they comply with eIDAS regulations. The auditor also checks the technical and organizational measures implemented to secure electronic identification and trust services. All these procedures should have a regulatory basis.

4.2. Digital Authentication Ecosystem Improvement Suggestions

In addition to specific law and policy recommendations, the team developed action items to vitalize the Laotian digital certificate ecosystem. We derived eight actionable tasks that cover governance, trust framework, interoperability, capacity, and service delivery areas. The figure below represents a target To-Be model of the Laotian ecosystem. However, achieving this model is not a short-term feat: it requires careful planning and extensive collaboration across organizations and sectors. Similarly, the tasks below provide only general guiding points and will need elaboration.

4.2.1. Establish a centralized and collaborative governance

The current Laotian digital certificate governance structure is far from optimal: there is little collaboration between departments and organizations and a lack of a cohesive digital development plan. As a result, digital initiatives are often implemented in silos. Without prominent data and system standards, this leads to fragmentation in digital authentication: every system virtually relies on a separate identification solution. Moreover, governance of the digital certificate itself needs refinement, such as clarifying roles and responsibilities and reinforcing the LANIC as the trust anchor. A centralized and collaborative governance structure must be implemented to tackle this issue, motivated by cooperation and dialogue rather than competition. A significant step in this direction was the recent establishment of the inter-departmental Digital Transformation Committee. This entity has excellent potential to coordinate and enforce overall government digital development, but it needs to secure its authority by legal and structural means. Furthermore, there is a need for a working-level group that will ensure the implementation of all policies and initiatives designed by the High-level digital committee. Next, it is necessary to strengthen digital certificate governance. An initial step to enhance digital certificate governance is establishing a temporary Digital Certificate Service Secretariat under the Digital Transformation Committee.

4.2.2. Adopt a data exchange framework

Currently, Laos has no national or international standards for digital government systems. Standards for data gathering and management are also lacking. In addition, there is no technical basis for exchanging data among government agencies, especially credential holders. This causes several issues in current identity verification tools' credibility, digital certificate usability, data silos, and obstacles to digital identity implementation. To solve these issues, it is necessary to consider a framework that would allow seamless data exchange among organizations. National implementation is the most typical way to adopt a data exchange framework.

The data exchange framework will also help with data exchange security, thus enhancing trust in digital services. During the process, the identity of each organization and technical access point is verified using certificates issued by a trusted CA. This measure enhances the security of the data exchange and the usability of digital certificates.

Streamlining the exchange of identity data through a standardized framework will reduce administrative overhead and eliminate the need for redundant data entry or verification processes.

4.2.3. Adopt a Unique Identifier to Enhance Trust

Organizations must trust the data and credentials for digital identity to be accepted across borders and sectors. Without general acceptance, the value of the digital certificates significantly diminishes. To embed trust in ecosystems, Laos should adopt the correct frameworks that allow organizations to operate according to rules and standards. One such rule is adopting a unique citizen ID and its connection to various digital authentication methods.

Currently, all credential holders have different standards for their identity data. There is no unique identifier per se because citizen identification data holders (MOHA, MOPS, LSSO) use different identifier standards, and identification data interoperability is limited. Closing gaps in citizen ID information for digital certificates to operate at total capacity is essential. Digital Transformation Committee's new digital master plan includes adopting unique identification numbers. The number will be assigned based on the birth certificate, thus making MOHA the central credential holder. However, this transfer shall be made step-by-step and align with existing regulations, policies, and standards.

4.2.4. Promote pan-government systems and solutions

Even though LANIC succeeded in identifying pioneer use cases for digital certificates (such as MOF systems), it is only a start in adopting the pan-governmental digital certificate system. Although Laos does not have services used across all government institutions, the most promising system is the e-Office, which currently has 18 users from government entities. The e-Office already integrated a digital certification for digital signatures. However, the government still must put effort into propelling this system across all public organizations and departments. Currently, several organizations are running their internal systems that follow different standards from e-Office and often require additional operations to include a digital certificate module. What is more, big organizations like MOF have different teams for different internal systems, which only exacerbates system silos and procedural inefficiencies. On the other hand, implementing digital signatures in the MOF systems will pave the way for digital document circulation in different ministries, as financial tasks are ubiquitously paper-based.

Based on the Korean case analysis, it will be helpful to implement a set of measures and incentives for system usage, such as including e-office and digital certificate usage into the government organization assessment levels. The MTC will have to conduct extensive awareness campaigns to explain that e-Office would tackle the existing system issues. It is also necessary to actively support recently onboarded organizations

(e.g., LSSO) by providing training and technical assistance. The scope of digital certificate usage within e-Office should be expanded.

4.2.5. Improve the digital certification system to ensure user-centricity

System adoption and usage success depend primarily on user-centricity (EPAM, 2023). In the case of digital certificates and authentication, this means diversifying authentication devices and methods. Laos previously implemented a token but switched to softkey technology, which presumes PC usage and requires installing SoftKey modules. This means that some populations will be inevitably excluded from digital certificate usage. To tackle this problem, it is necessary to provide all citizens with a chip-enabled ID that would be the base technology for authentication and signatures. This measure will also ensure that citizens with limited internet access can access the necessary services without extra paperwork. User-centricity also means that users should have choices not only in authentication means but also in data processing. The users should be informed on how, by whom, and where their data will be used. Lastly, it may be necessary to simplify the process of verifying the authenticity of digital certificates. However, to balance service security with simplicity, LANIC needs to ensure its encryption methods and data protection measures are robust.

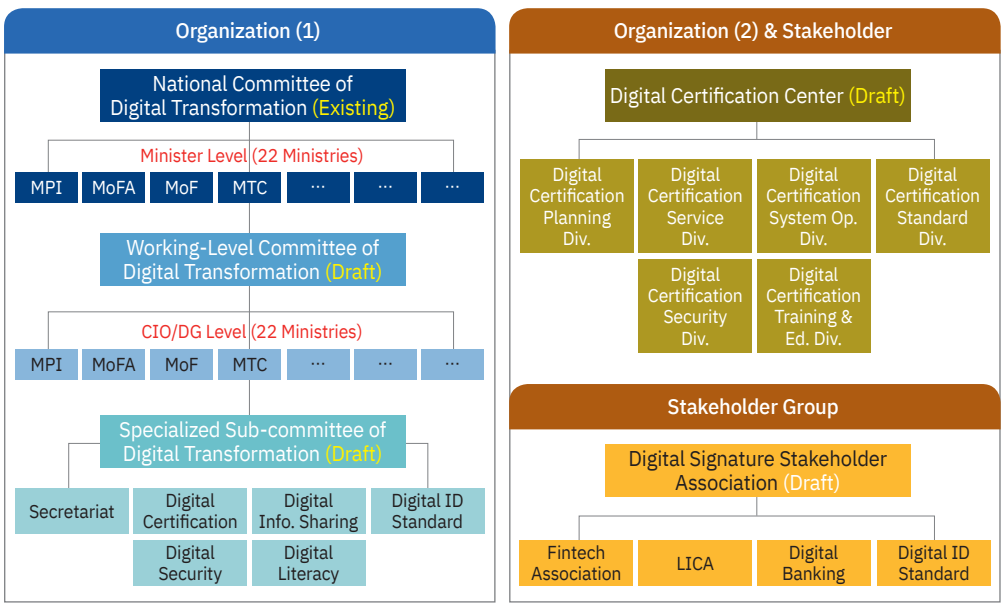
4.2.6. Utilize and strengthen existing public-private partnerships

Achieving success in digital certificate implementation is hard without collaboration among sectors, institutions, and industries. Laos has a good case of public-private cooperation: most government system development is outsourced to private developers. In addition, LANIC assigned Wintech/LCA as the Public CA, making it responsible for distributing and promoting public certificates. However, there is room for growth in private-public partnerships, which can be filled by consolidating and structuring the partnership.

Schemes driven by a public-private ecosystem will combine the private sector's strengths, such as innovation, digitization, and resources, with those of the public sector, such as standardization and regulation. Public-private collaboration can take different forms, such as policy advising and promotion of digital services, where private companies form an official Association that communicates regularly with the public sector on the digital certificate industry development question.

4.3. Enhancement of Organization and Governance Structure

Figure 12.
Enhancement of Direction of Governance Structure



Note: CIO (Chief Information Officer)

4.3.1. Inception of the Digital Transformation Governance System

The National Digital Transformation Committee needs a three-layer structure with working-level and sub-committees to support its initiatives. Formed in 2023, the lack of working-level committees hinders the expansion of digital certification. A digital government working committee and specialized subcommittees are necessary to coordinate digital authentication across government agencies. Each agency should appoint a Digital Government Chief Information Officer (DG CIO) to enhance digital capabilities. This will improve digital services for staff, petitioners, NGOs, and civil organizations.

4.3.2. Establishment of an Independent Integrated Digital Certification Center

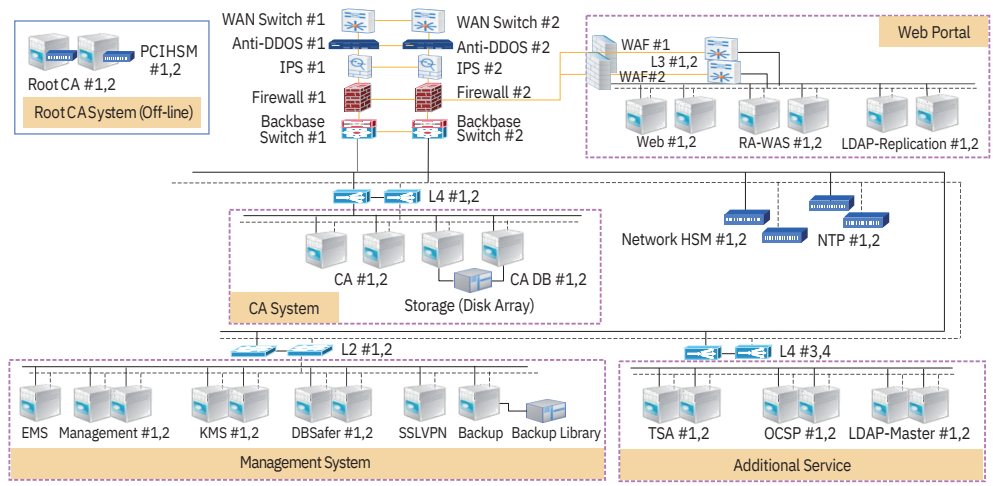
To meet the growing demand for digital certification, an independent digital certification center with six departments should be established. The government should support stakeholder groups for each certification area to foster industry and technology development. Beyond GPKI and NPKI, an integrated digital certification center is needed for policy and legislative matters related to simple payment, e-NID, and e-KYC. This center should promote digital certification services for government officials and the public.

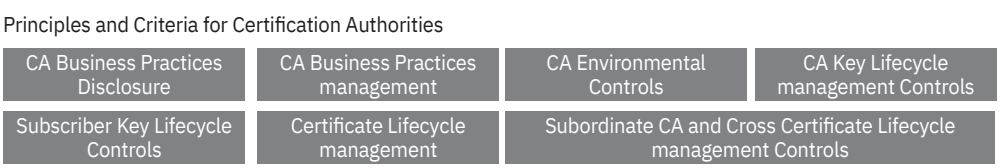
4.4. Design of an Advanced National Certification System

4.4.1. Advanced National Certification System

The Laos Advanced National Certification System should be configured to meet the 'WebTrust Principles and Criteria for Certification Authorities' to achieve internationally recognized WebTrust certification.

Figure 13.
Configuration of Advanced National Certification System





- **Certificate Issuance Regulations:** Laos' certification authorities must adhere to the certificate issuance regulations outlined by WebTrust. These include rules for issuing, renewing, and revoking certificates.
- **Certificate Validation:** Laos' certification authorities should implement a process to validate the validity of issued certificates. This enables clients to verify the identity of websites.
- **Privacy Protection:** WebTrust places a high emphasis on privacy protection, and Laos' authentication system should be capable of securely protecting users' personal information. This includes safeguarding the authentication process and related data.
- **Security Enhancement:** Laos' authentication system should take measures to enhance security. This includes using encryption technologies, complying with

security protocols, and improving network security.

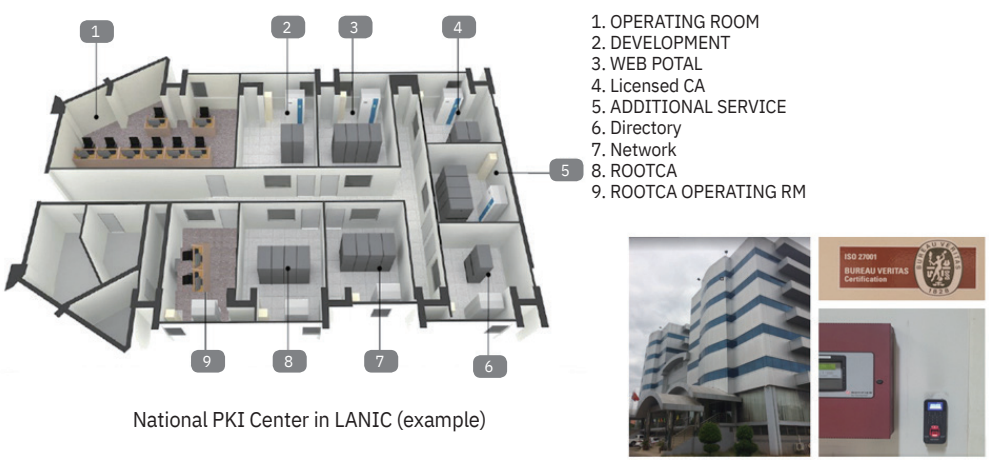
- **Auditing and Review:** Laos' WebTrust authentication system should undergo regular audits and reviews to ensure security. This helps address security threats and keeps the system up-to-date.

4.4.2. Certification Center

The certification center must be configured independently. Access control in both physical and information security involves selectively restricting room access. Operators cannot have simultaneous access permissions to all rooms.

- Different core component systems, such as CA/RA, OCSP/TSA, and DS, must be installed separately in different rooms.
- Each system should operate independently of the others.
- Physical access to these rooms must be strictly controlled.
- Measures should be implemented to mitigate damage from fire or flooding.

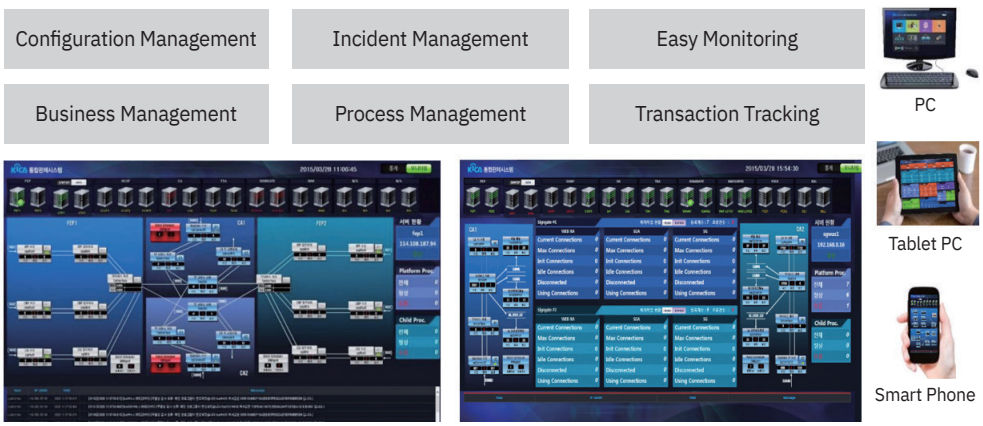
Figure 14.
National PKI Center



National PKI Center in LANIC (example)

System Management Software (SMS) monitors and manages system failures, performance, and applications. Network Management Software (NMS) includes hardware and software monitoring and managing computer networks. NMS and SMS are essential for efficiently and reliably monitoring and controlling the certification center. However, despite all these efforts, most problems arise due to operator errors or lack of experience among staff. Therefore, the most crucial factor lies in the secure operation of well-trained operators according to appropriate policies.

Figure 15.
Operation and Monitoring



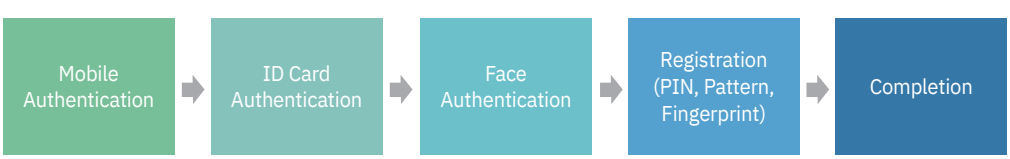
4.4.3. Digital Certificate

Laos Advanced National Certification System should incorporate non-face-to-face identity verification technologies equivalent to face-to-face methods, enabling users to quickly obtain digital certificates for electronic signatures and other business purposes.

The recommended non-face-to-face identity verification procedure is as follows:

1. Mobile Authentication (with LANIC)
2. ID Card Authentication (OCR)
3. Face Authentication (with Liveness Check)
4. Registration
   a. Certificate PIN (6-digits)
   b. Certificate Pattern
   c. Biometric Information for the Certificate (Fingerprint)
5. Completion of Financial Certificate Issuance

Figure 16.
Certificate Issuance Process with non-face-to-face authentication

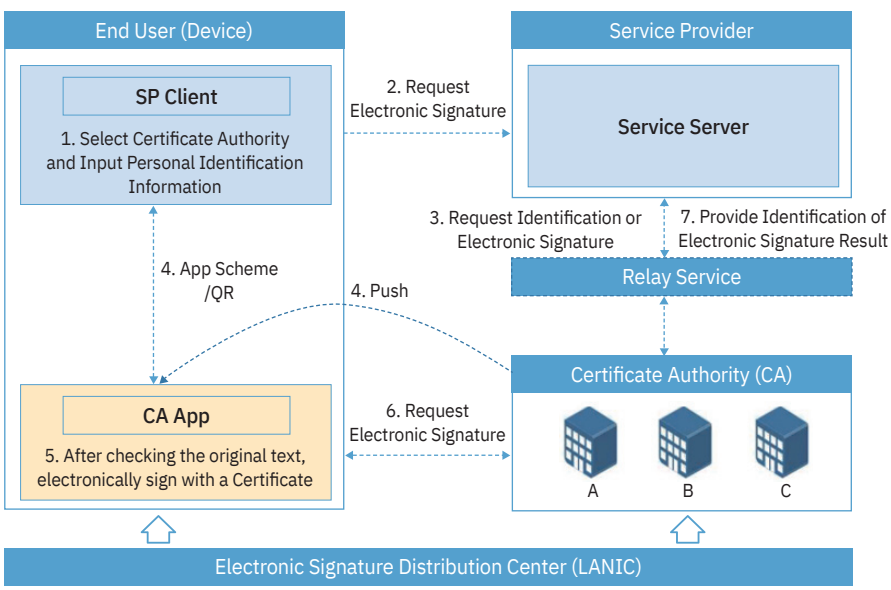


4.4.4. Securing Application

Applying certificate-based electronic signatures to e-government services enhances security, authenticity, integrity, and efficiency in digital transactions and interactions between citizens, businesses, and government entities.

Standardized interfaces enable easy access to electronic signature services across various applications, such as public services, telecommunications, and finance. By providing standardized interfaces for electronic signature services, Laos can facilitate the widespread adoption of electronic signatures across various sectors, improving efficiency and convenience for businesses and individuals.

Figure 17.
Authentication and Signature Procedure

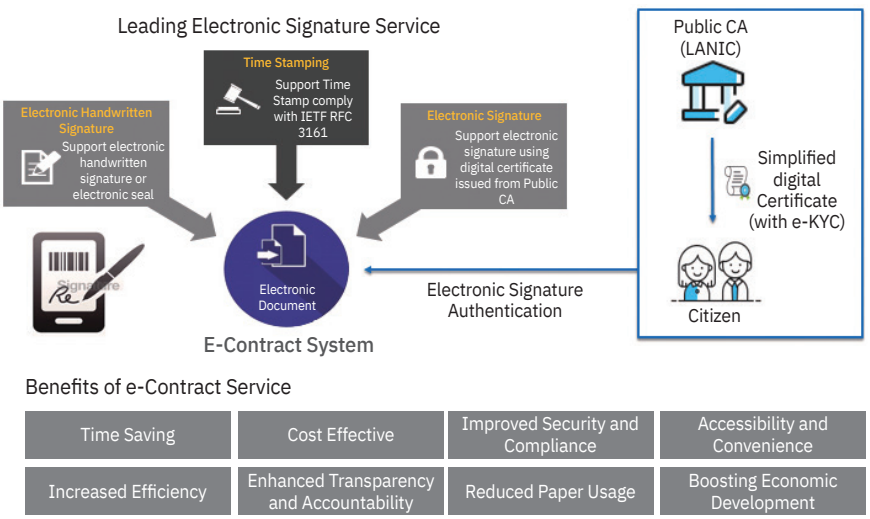


Source: KISA Homepage (2024).

4.4.5. Leading Electronic Service (e-Contract)

The Laotian government has enacted an electronic signature law to confer legal validity to electronically signed documents. Electronic contract services are online contracts utilized when exchanging documents requiring electronic signatures and seals. LANIC, a government agency in Laos, can construct a cloud-based electronic contract service. Initially, this service will be provided for approximately 500 contracts annually signed by the MTC, with plans for gradual expansion to other key government agencies such as the Ministry of Finance and the Customs Department.

Figure 18.
E-Contract System



4.5. Establishment of a Capacity Building Plan

To enhance the capabilities of the Laos National Certification System and improve awareness, it is necessary to differentiate target groups and devise strategies tailored to each group when crafting policies and programs. Strengthening the capabilities of the national certification system in Laos also entails incorporating capacity-building programs into digital literacy education efforts.

- **Manager Group:** This course focuses on establishing tailored PKI policies. Participants will learn how to develop, implement, and manage PKI policies specific to their organization's needs. Topics covered may include PKI governance, policy development, legal and regulatory compliance, risk management, and best practices in PKI management.
- **Operator Group:** This training is aimed at individuals tasked with maintaining the stable operation of a PKI center. Participants will gain knowledge and skills related to PKI infrastructure management, including server administration, backup and recovery procedures, performance monitoring, and ensuring the security and availability of PKI services.
- **Application Developer Group:** This course targets application developers. Participants will learn to integrate PKI functionalities into their applications, including digital signature verification, certificate validation, and secure communication protocols. Topics may also include API integration, coding best practices, and troubleshooting PKI-related issues within applications.

By offering these tailored PKI training courses, organizations can ensure that each relevant group receives the necessary knowledge and skills to manage and utilize within their respective roles effectively. Enhancing the capabilities of experts responsible for operating and maintaining security infrastructure ensures the long-term success of the Laos National Certification System.

4.6. Cost and Budget Planning

The project for Laos Advanced National Certification System consists of the following components:

- **Implementation of Certification System:** This includes developing and implementing the certification system.
- **Development of PKI Enabled Service:** Developing leading electronic signature services, ensuring they are robust and user-friendly.
- **PKI Awareness:** Activities to raise awareness about Public Key Infrastructure (PKI), its importance, and its applications.
- **Invitation Training:** Hosting educational events to invite participation and provide training on PKI-related topics in Korea

Table 4.
Scope of Advanced National Certification System

Category	Tasks	No	Activities
Phase I	Implementation of National PKI System	1	• Field Research
		2	• Master Plan for National PKI
		3	• Facillities and Equipment Installation (NPIKI)
		4	• Implementation of PKI Certification System
		5	• System Operation Training
		6	• PKI Enabled Application Development (E-Government Services)
		7	• WebTrust CA & AATL
Phase II	Implementation of PKI enabled services	1	• Requirement Analysis & Design/Master Planning
		2	• Facilities and Equipment Installation (PKI enabled services)
		3	• Implementation of e-Contract Service
PKI Awareness (Laos)		1	• On-site Training
		2	• PKI Seminar & Workshop
Invitation Training (Korea)		1	• High-level Administrator course
		2	• Manager/Operator/Developer Course

The budget for the implementation of the Laos Advanced National Certification System is a total of 8 million dollars, and the detailed breakdown is as follows:

Table 5.
Cost and Budget Planning: Phase I

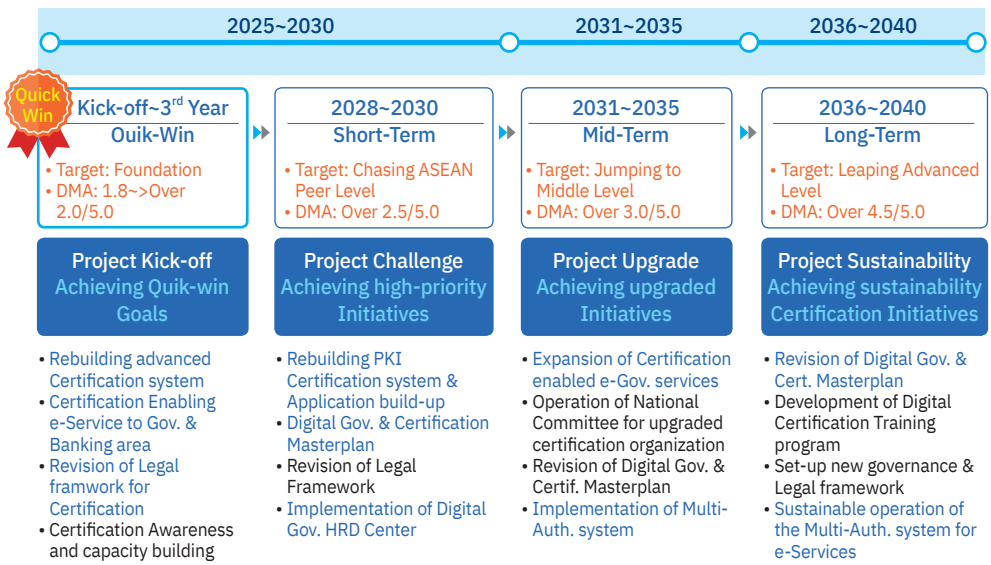
Classification	Item	Cost (USD)	Remarks
Provision and Equipment (HW/NW/SW)	Root CA	350,000	Including DR
	Public CA	2,500,000	
	Government CA	2,000,000	
Expert Dispatch (Direct Expense & Labor)	Field Research	12,000	3 Persons * 1 week
	Master Plan Establishment	312,000	5 Persons * 6 Months
	Setup & Training (HW/NW)	24,000	3 Persons * 2 weeks
	Installation & Training (SW)	24,000	3 Persons * 2 weeks
	PKI Enabled Application Dev.	30,000	2 Persons * 4 weeks
Trust Certificate	Obtain WebTrust CA /AATL	500,000	5 Persons * 9 Months
PKI Awareness (Laos)	On-site Training	14,000	3 Persons * 1 week
	PKI Seminar & Workshop	40,000	3 Persons * 2 weeks
Invitation Training (Korea)	High-level Officials	10,000	4 Person * 1 week
	Working level Officials	20,000	7 Person * 1 week
	Total Cost	**5,836,000**	

Table 6.
Cost and Budget Planning: Phase II

Classification	Item	Cost (USD)	Remarks
Provision and Equipment	E-Contract System (HW & SW)	1,630,000	Including DR
	Development (Localization)	120,000	4 Persons * 3 Months
Expert Dispatch (Direct Expense & Labor)	Requirement Analysis & Design / Master Planning	312,000	5 Persons * 6 Months
	Setup & Training (HW/NW)	24,000	2 Persons * 2 weeks
	Installation & Training (SW)	24,000	3 Persons * 2 weeks
PKI Awareness	PKI Seminar & Workshop	40,000	3 Persons * 2 weeks
Invitation Training (Korea)	Working level Officials	14,000	5 Persons * 1 week
	Total Cost	**2,164,000**	

4.7. Digital Certification Improvement Roadmap in Lao PDR

Figure 19.
Phased Roadmap of Digital Certification



The development roadmap for the digital certification in Laos, broken down into short-term, mid-term, and long-term phases, is as follows:

First, in the short-term roadmap, the initial phase, a few Quick Win tasks to be accomplished within approximately three years, will be implemented right after the commencement of the digital certification project. This period will serve as the foundation-building stage for the digital certification project. The goal is to advance from the current digital maturity level of 1.8 to the early 2.0s, as diagnosed by the UNDP's Digital Maturity Assessment (DMA). Details of the Quick Win tasks will be explained in the following slides.

Subsequently, during the short-term roadmap, including the period of executing the Quick Win tasks, the project will aim to catch up with ASEAN peer countries such as Vietnam and Thailand. By implementing the roadmap's action plan, the DMA score is expected to improve to around 2.5 out of 5.0. Significant achievements in the digital certification field are anticipated to be realized during this short-term roadmap period.

Next, the mid-term roadmap aims for an intermediate level of development compared to other countries' digital certification projects. Finally, the long-term roadmap sets the goal of challenging toward an advanced level in the digital certification field by 2040, matching that of developed countries.

Figure 20.
Sectoral Detailed Roadmap

2025~2030 | 2031~2035 | 2036~2040

	Short-Term		Mid-Term	Long-Term
	2025~2027	2028~2030	2031~2035	2036~2040
Policy & Legal Framework	• Digital Gov. Masterplan • Digital Gov. enactment • Digital Signature Decree & Regulation Revision • Individual Admin. Law requiring digital Certification	• Digital Certification Masterplan	• (Revison) Digital Government Masterplan v2.0 • (Revison) Digital Certification Masterplan v2.0	• (Revison) Digital Government Masterplan v3.0 • (Revison) Digital Certification Masterplan v2.0
Org. & Stakeholder	• Establishment of working-level committee of Digital Transformation • Establishment of Specialized Sub-committee of Digital Transformation	• Establishment of 'Digital Certification Center'	• Operation of National Committee of 3-layer digital transformation Committee	• Operation of National Committee of 3-layer digital transformation Committee
Technology & Standard	• PKI Certification system build-up (1) • Application build-up based on PKI certification • Establishment of public CA standard	• PKI Certification system build-up (2) • Application build-up based on PKI certification • Builidng of Simple Auth. Platform	• Implementation of Distributed Digital ID platform • Application build-up based on multi-auth certification and operation • Implementation of digital Information Sharing Common Platform and Op.	• Application build-up based on multi-auth certification • Expansion of digital Information Sharing Common Platform and Op.
Capacity Building & Awareness	• Establishment of Digital Capacity Building masterplan and training system, fostering teacher, ToT • Building ICT Training & Literacy Center (USF) • Digital Certification Awareness Diagnosis and Consulting	• Implementation of Digital Government HRD Center • Building ICT Training & Literacy Center (USF) • Appointment of DG CIO at MDA	• Development of Digital Certification Training Program and ToT Program • Fostering Digital literacy and Certification teacher at individual MDA • Digital Certification Sub-Committee Operation • Advancement of DG CIO at MDA	• Development of Digital Certification Training Program and ToT Program • Fostering Digital literacy and Certification teacher at individual MDA • Digital Certification Sub-Committee Operation • Advancement of DG CIO at MDA

We propose the following sectoral action items by pillars for the digital certification improvement roadmap:

4.7.1. Policy

- Establish specific policy frameworks such as a Digital Government Master Plan and a Digital Certification Master Plan.
- Finalize the Digital Government Master Plan as a national agenda on top of the current digital economy policy framework. Additionally, the government must prioritize the development of a Digital Certification Master Plan covering all aspects of digital certification services.

4.7.2. Legal Framework

- Add legislation for individual tasks related to the equivalent effectiveness of digital documents compared to paper documents, necessitating amendments to specific laws.
- Amend individual laws to ensure that documents and tasks verified through digital certification services have the same legal validity as paper documents.
- Adopt intra-agency digital information-sharing services to promote digital certification. The legal framework for information-sharing center functionalities must be established to facilitate this.
- Promulgate the Digital Government Act as a foundational document for digital government operations.

4.7.3. Digital Certification Related Governance System

- Establish a three-layer organizational structure within the National Digital Transformation Committee. This structure should include working-level committees to support the high-level Digital Transformation Committee and specialized subcommittees.
- Each MDA should appoint a Digital Government Chief Information Officer (DG CIO) to enhance digital capabilities within the ministry and among stakeholders such as petitioners, NGOs, and civil organizations and to activate related policies and initiatives.
- Establish an independent Digital Certification Center of six departments to meet the increasing demand for digital certification in various sectors. This center should aim to activate digital certification services for government officials and the public.

4.7.4. Advancement of the digital certification system and its application

- Improve current PKI systems: upgrades, redundancy, and security reinforcement are necessary.
- Develop and provide a Software Development Kit (SDK) and libraries targeting the most in-demand administrative services to activate PKI-based digital certification services.
- Establish a government-wide standard framework to prevent lock-in to specific software and to support pilot testing centers for government-wide digital service support.
- Conduct feasibility studies on digital certification services to assess their suitability for prominent G2G services (e.g., e-office) and expand these services to other areas of digital government services. Ensuring the stability and functionality of the current PKI digital authentication system within government services and activating private sector participation (NPKI) will require discussions with financial entities on the applicability of PKI authentication services in banking services. Additionally, enhancing the functionality and stability of PKI authentication systems is necessary.
- Efforts to identify pan-government services where digital authentication can be applied must be undertaken in collaboration with other ministries and the Digital Transformation Committee. Collaborative development, testing, and technology operation among ministries may be required.
- The government needs to gather capabilities to provide various digital certification services in diverse competitive environments through subcommittees under the National Digital Transformation Committee. This includes standardizing the Public Certification Authority (CA), simplified payment standardization platforms, distributed DID platforms, and other related areas.

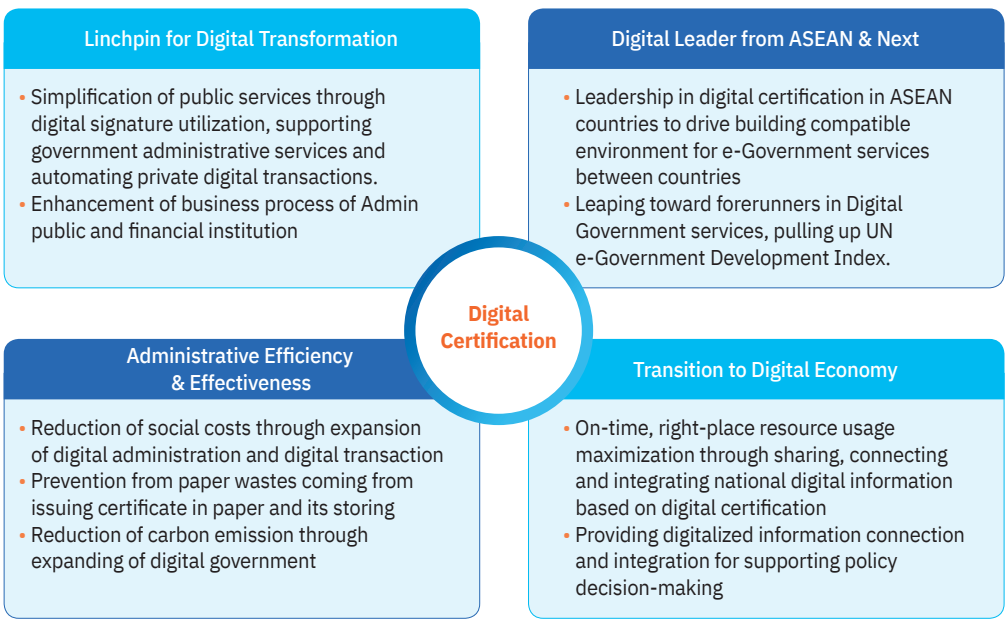
4.7.5. Capacity Building and Awareness Improvement

- Establish a master plan for policy formulation regarding digital capacity building to formulate a comprehensive policy. It shall include aspects such as digital governance, policies related to digital certification, legislation, organizational structures for capacity building, the establishment of capacity building centers, and capacity enhancement programs.
- Redefine each institution's roles and responsibilities (R&R) in providing existing digital education services and re-establishing the governance system.
- Develop and implement regular digital government education programs tailored to specific fields.

- Establish a cross-government Digital Government Human Resource Development (HRD) Center, which is essential for the revised digital government governance system. This center will facilitate the development of digital literacy and capacity building for digital authentication services on a government-wide scale.
- The proposed "Digital Certification Center" shall include a "Digital Certification Education Department" under its organization. This department will serve as the focal point for providing consulting services tailored to each ministry's digital literacy and Certification needs.
- Support the operation of Departmental Chief Information Officers (CIOs) to enhance digital literacy and digital certification capabilities across departments; provide training for departmental experts (including ToT) in digital government and digital certification.
- Organize information technology competitions among government departments to stimulate competition and promote the development of digital government services. Performance management can foster capacity development and awareness improvement regarding digital government and certification.

5. Conclusion: Expected Effects

Figure 21.
Expected Effects of Digital Certification System



The team expects the following effects from the implementation of the policy recommendations and roadmap prescribed by this report:

Quick-win Phase

- In the first stage of the short-term roadmap, after initiating the digital certification business, about three years will be dedicated to pursuing Quick Win projects, laying the foundation for the digital certification business. The goal during this period is to advance from the current DMA score of 1.8~2.0 to the early 2.0s.

Short-term Roadmap

- The short-term roadmap, including the duration of Quick Win project implementation, will involve tracking ASEAN peer countries such as Vietnam and Thailand, aiming to catch up with them. By executing action plans in the roadmap, the goal is to elevate the DMA development effect to around 2.5 out of 5.0. It is anticipated

that significant achievements in the digital authentication field will be made during this short-term roadmap period.

Mid-term Roadmap

- The mid-term roadmap aims to achieve a development level comparable to other countries' digital certification businesses, reaching a middle-level standard.

Long-term Roadmap

- The subsequent long-term roadmap has been designed to catch up with advanced countries in the digital certification field by 2040.

References

ASEAN. (2021). *ASEAN digital masterplan (ADM 2025).* ASEAN. https://asean.org/book/asean-digital-masterplan-2025

Asian Development Bank. (2023). Lao PDR: Economy. *Asian Development Bank.* https://www.adb.org/where-we-work/lao-pdr/economy

ASIA PKI Consortium. *Presentation material (Viet Nam, Thailand, Malaysia)*. www.Asiapki.org (Accessed date not available).

Vongdara, B. (2023). Digital transformation in Lao PDR. *United Nations Development Programme (UNDP),* 12–22.

Luanglath, C. (2021). Digital transformation in Lao PDR. *Ministry of Technology and Communications.* https://www.mtc.gov.la

European Commission. (2021). e-IDAS Regulation. European Commission. https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation

Euroopa Uhendamise Rahastu. (n.d.). *State authentication service (TARA) technical description.* https://e-gov.github.io/TARA-Doku/TehnilineKirjeldus#9-erasektori-asutuse-erisused

Deloitte Anjin LLC. (2024). *Services.* Deloitte. https://www.deloitte.com/kr

Gelb, A., & Diofasi Metz, A. (2018). *Identification revolution: Can digital ID be harnessed for development?* https://muse.jhu.edu/chapter/2059040/pdf

Goode Intelligence. (2020). *An introduction to GADI – the global architecture for digital identity.* https://www.goodeintelligence.com/report/an-introduction-to-gadi-the-global-architecture-for-digital-identity

Government of Lao PDR. (2012). *Law on electronic transactions No. 20/NA.* Lao Official Gazette. https://laoofficialgazette.gov.la/kcfinder/upload/files/Law%20on%20Electronic%20Transactions%20.pdf

Government of Lao PDR. (2017a). *Laos information protection law No. 25/NA.*

Government of Lao PDR. (2017b). *Law on payment systems No. 292/P.* https://www.bol.gov.la/en/fileupload/14-06-2019_1560480775.pdf

Government of Lao PDR. (2018). *Law on e-signatures No. 59/NA.*

Government of Lao PDR. (2021). *Decree on E-Commerce No. 296/GOV.*

Government of Lao PDR. (2022). *Law on electronic transactions (2022 Draft).*

Government of Lao PDR. (2023). *Digital government strategy and masterplan (Draft).*

Info-Tech Research Group. (2020). *Navigate the digital ID ecosystem to enhance customer experience.* https://www.infotech.com/research/ss/navigate-the-digital-id-ecosystem-to-enhance-customer-experience

Jabatan Pekhidmatan Awam. (n.d.). *Government public key infrastructure (GPKI).* https://docs.jpa.gov.my/sme/penulisan/Pengurusan_Teknologi_Maklumat/1b.pdf

Kemp, S. (2023). *Digital 2023: Laos.* DataReportal – Global Digital Insights. https://datareportal.com/reports/digital-2023-laos

Soulivong, K. (n.d.). ICT & e-Government in Laos. Deputy Director General of e-Government Center, Ministry of Posts and Telecommunication. Email: kesone@mpt.gov.la.

KOICA Office in Lao PDR. (2017). *Korea's country partnership strategy for Lao PDR.*

Korea Information Certificate Authority. (2024). *Service introduction.* https://signok.com

Korea Internet & Security Agency. (2024a). *Simple authentication interface guideline.*

Korea Internet & Security Agency. (2024b). *Digital safety.* https://www.kisa.or.kr

LANIC. (2023, November). *Lao PDR NRCA introduction materials.* Slide show.

Lao News Agency. (2023, August). *President appoints new committee for country's digital transformation. Newsletter.*

McKinsey Global Institute. (2019). *Digital identification: A key to inclusive growth.* https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20identification%20A%20key%20to%20inclusive%20growth/MGI-Digital-identification-Report.ashx

Ministry of the Interior and Safety, NIA. (2021). *All that digital gov. KOREA.*

National Electronic Authentication Center. (2024). *Statistics.* https://neac.gov.vn/en

Khammoungkhoune, N. (2023). Lao national root certificate authority. Ministry of Technology and Communications Lao National Internet Center.

Peace Independence Democracy Unity Prosperity. (2021a). *20-year NDE vision, 10-year NDE strategy, 5-year NDE plan.* Lao People's Democratic Republic.

Peace Independence Democracy Unity Prosperity. (2021b). *9th 5-year national socio-economic development plan (2021-2025).* Lao People's Democratic Republic.

SGLab Co., Ltd. (2021, September 30). *국제 전자서명 동향 및 평가제도 연구 [Research on international electronic signature trends and evaluation systems]*. https://www.kisa.or.kr/201/form?postSeq=12052&page=1

United Nations Development Programme (UNDP). (2023). *Digital government strategy and masterplan,* 12–22.

United Nations Population Fund (UNFPA). (2022). *MOHA, LSB and partners working to make everyone visible in Lao PDR.* https://lao.unfpa.org/en/news/moha-lsb-and-partners-working-make-everyone-visible-lao-pdr

World Bank Group. (2022). *Lao PDR systematic country diagnostic 2021 update brief.* https://www.worldbank.org/en/country/lao/brief/lao-pdr-systematic-country-diagnostic-2021-update-brief

World Economic Forum. (2021). *Digital identity ecosystems: Unlocking new value.* https://www3.weforum.org/docs/WEF_Guide_Digital_Identity_Ecosystems_2021.pdf

2023/24 Knowledge Sharing Program

This publication summarizes the key findings of the Knowledge Sharing Program (KSP), funded by the Ministry of Economy and Finance (MOEF) of the Republic of Korea. The views expressed are those of the authors.
The KSP is a policy-oriented development cooperation program designed to share Korea's development experience and knowledge. Its goal is to support the institutional and capacity building of partner countries through collaborative research, policy consultations, and technical assistance on key policy issues.

For more information:
https://www.ksp.go.kr

Ministry of Economy and Finance (MOEF)
Sejong Government Complex, Doeuom 6-Ro, 42, Republic of Korea
Tel. 82-44-215-7742
www.moef.go.kr

Korea Development Institute (KDI)
Namsejong-ro, 263, Sejong-si 30149, Republic of Korea
Tel. 82-44-550-4114
www.kdi.re.kr

IGB & Company Co., Ltd.
12F, 33, Gukjegeumyung-ro 6-gil, Yeongdeungpo-gu,
Seoul 07331, Republic of Korea
Tel. 82-2-2088-8432

Korea Information Certificate Authority Inc.
6F, 69, Geumto-ro, Sujeong-gu, Seongnam-si,
Gyeonggi-do, 13453, Republic of Korea
Tel. 82-2-360-3215

Knowledge Sharing Program (KSP)
www.ksp.go.kr

9 791159 328954 94320
ISBN 979-11-5932-895-4
ISBN 979-11-5932-904-3 (set)