APKIC ASIA DIGITAL TRUST SUMMIT 2026

Vietnam’s PKI and Trust Services

National Electronic Authentication Centre (NEAC)
Ministry of Science and Technology, Vietnam

PKI

DIGITAL TRUST INFRASTRUCTURE

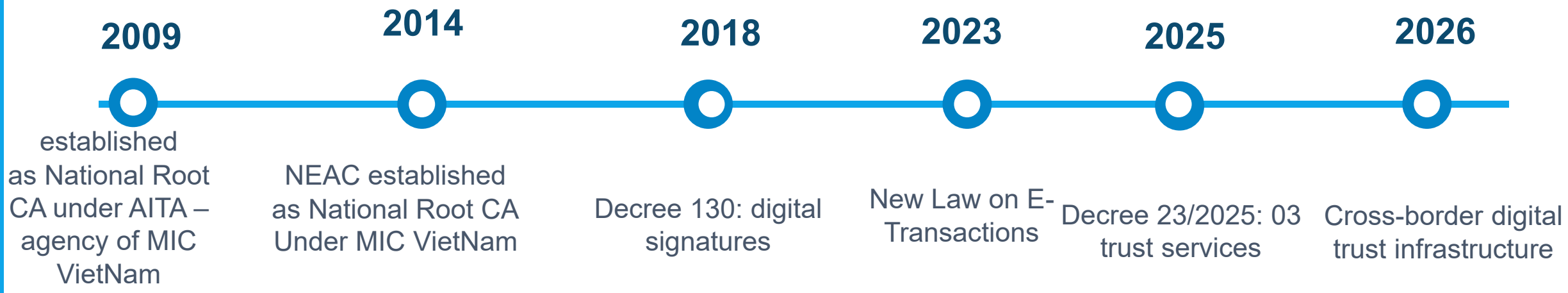
AGENDA

Present Contents

1. Introdution PKI in Vietnam
2. Statistics and Implementation Status
3. Applications
4. Conclusion and Recommendations

SECTION 01

VN PKI Path & NEAC's Road (2009–2026)



Key focus of NEAC's journey

Building a complete national digital trust foundation - from Root CA operations and trust services regulation to cross-border recognition mechanisms that enable seamless electronic transactions across borders.

SECTION 01

Legal and Regulatory Framework

1 New categories of trust services:

- Digital signatute,
- TSA,
- ectronic data message authentication.

2 Continuing the standardization process:

Issuing 5 circulars that specify technical requirements for digital signature software, digital signature verification software, connection gateways, and digital certificate formats

3 Simplify:

This November, the Government has directed the completion of the rollout of free digital signatures via VNeID. Citizens can sign documents digitally directly on their phones, without the need for any separate hardware..

4 Esure legal security

- The national digital signature authentication infrastructure is secured in accordance with information security levels and international standards
- Decree No. 174/2026/ND-CP stipulates penalties for the act of providing false information in order to obtain a digital signature.

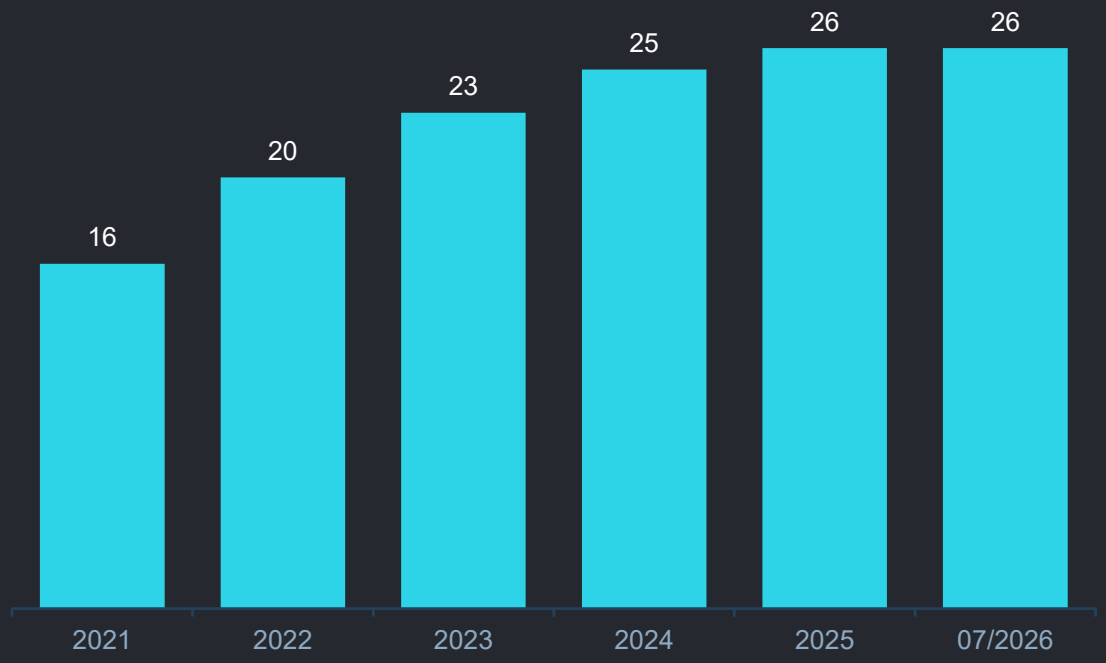
TCVN Standards in The Field of Trust Services 2026

1 Electronic Transactions - Operational and Control Requirements for Public Digital Signature Certification Service Providers	**2** Electronic Transactions - Operational and Control Requirements for Public Digital Signature Certification Service Providers under the Remote Signing Model	**3** Electronic Transactions - Operational and Control Requirements for Time-Stamping Service Providers	**4** Electronic Transactions - Operational and Control Requirements for Registered Electronic Delivery Service Providers
5 Electronic Transactions - Operational and Control Requirements for Providers of Data Message Preservation and Integrity Validation Services	**6** Electronic Transactions - Requirements for Data Message Certification Services	**7** Electronic Transactions - Requirements for Digital Signatures on Data Messages for Long-Term Preservation	**8** Electronic Transactions - Digital Signature Creation Protocol for the Remote Signing Model
9 Electronic Transactions - Requirements for Signature Creation Software and Signature Validation Software	**10** Electronic Transactions - Signature Activation Application for the Remote Signing Model	**11** Electronic Transactions - Requirements for Signature Creation Modules for the Remote Signing Model	**12** Electronic Transactions - Functional and Business Requirements for the Mobile PKI Model
13 Electronic Transactions - Requirements for Roaming Specifications for the Mobile PKI Model	**14** Electronic Transactions - Time-Stamping Protocol for Trust Services	**15** Electronic Transactions - Requirements for Web Service Interfaces for the Mobile PKI Model	**16** Electronic Transactions - Requirements for the Security Framework for the Mobile PKI Model

SECTION 02

Statistics and Implementation Status

Growth of Licensed Public CAs (2021 – 07/2026)



26	licensed public CAs (Jul 2026)
25	CAs providing token signing
14	CAs providing remote signing
3	CAs providing SIM PKI services
7	CAs providing timestamp services

**Some CAs provide more than one type of service.*

Public Digital Signature Certification Service

Activities & Technology

Certificate Issuance

Identity verification via VNeID; issuance of Digital Signature Certificates binding the public key to subscriber identification information.

Lifecycle Management

Renewal, suspension, restoration, revocation of certificates; maintenance of CRL and OCSP online 24/7.

03 Digital Signing Models

USB Token (25/26 CAs) - Remote Signing (14/26 CAs) - SIM PKI (03/26 CAs)

26

Licensed public CAs

36M

Cumulative Digital Signature Certificates issued as of 10/2026

52.26%

of the adult population now have a digital signature

SECTION 03

Applications & eSign Gateway

Digital signatures applied across key sectors, connected nationwide through the eSign Gateway.

Taxation
5 B
Electronically signed e-invoices

Banking
46 M
Electronic banking customers

Customs
57,7 M
Electronic clearance transactions

Social Insurance
81,5 M
Successfully processed record

State treasury
188M
Dossiers and vouchers (100%)

E-Commerce
16,2 M
Electronic Contracts

Electronic Contract (NEW): 21M

eSign Gateway

- Centralized access to service information and usage statistics.
- Technical support and solution integration for signature applications.
- Simple, transparent connection model and procedures.
- Secure and interoperable signing with all licensed public CAs.

RESULTS

34 / 34
Successfully connected to all provincial public service portals nationwide.

50M+
Access requests recorded, demonstrating strong demand and effective integration.

NEAC connects all CAs to the eSign Gateway

Digital Signature in Healthcare, Education and Public administrative services

HEALTHCARE

- Preferential pricing for Digital Signature for hospitals & nationwide healthcare facilities
- Integration of digital signing for electronic prescriptions (HIS) - paperless
- Digital signatures are integrated into electronic medical records

EDUCATION

- Digital signatures in verifying academic transcripts, tuition fees and online enrollment
- Electronic diploma and transcript with the principal's digital signature and timestamp
- Digital signatures for teachers and students are linked to the VNeID identifier

PUBLIC ADMINISTRATIVE SERVICES

- Mandatory personal digital signatures in level 4 administrative procedures
- Digital signatures are applicable to electronic notarization
- Digital signatures applied to electronic document management

Time-Stamping Service

Concept:

Attaches a timestamp (date, hour, minute, second) to electronic data messages - the moment the service provider receives the data, synchronized with the national standard time source. The timestamp proves that the data existed at that point in time and has not been altered afterward.

Time-Stamping Issuance Process (RFC 3161)

1. Calculate hash of the data
2. Send TSQ (Time Stamp Request)
3. TSA synchronizes with national standard time
4. TSA signs → Timestamp Token
5. Returns Token to the user

Practical Applications:

Litigation & Legal

Proof of signing/submission time for electronic documents

Electronic Contracts

Confirms signing time with legal validity

Finance - Securities

Order execution, electronic banking transactions

State Document Archiving

Ensures long-term legal validity of government documents

SECTION 02:

Data Message Authentication Service

Confirms the integrity and origin of electronic data messages. Provides irrefutable proof of transaction content - combining Digital Signature Certification + Timestamp + Event Log storage.

COMPARISON WITH DIGITAL SIGNATURE CERTIFICATION SERVICE:

Aspect	SVC01-Digital Signature Certification	SVC03-Data Message Authentication
Object of Certification	Signer's identity (Certificate)	Content of the data message
Time of Certification	At the time of certificate issuance	At the time of sending/receiving the message
Evidence Provided	Digital Signature Certificates & Digital Signature	Event log, Data Message integrity code
Storage Requirements	Subscriber information	Content + metadata of data message + event log

Applications: Electronic Commercial Contracts | Electronic Litigation | Online submission of dossiers to State agencies | Electronic Bidding | CeCA Platform (16,2M contracts, 250K enterprises)

SECTION 04

Conclusion and Recommendations

Conclusion

- Vietnam has advanced in nationwide deployment of digital signature and trust services.
- A complete legal framework supports trust services and cross-border recognition.
- eSign Gateway ensures secure, interoperable, and legally valid digital transactions.

Development Orientation

- Expand digital signature applications in digital government, economy, and society.
- Establish cross-border interoperability and mutual recognition mechanisms.
- Promote international cooperation in standards, recognition, and conformity assessment.

Proposed Cooperation

- Exchange information and share management and technical standards.
- Conduct interoperability testing and mutual CA recognition.
- Post Quantum Cryptography Migration
- PKI for AI (AI Agents)

Thank you!

Xin cảm ơn!

National Electronic Authentication Centre (NEAC)
Ministry of Science and Technology, Vietnam