

Useful Guide to KOREA/KOREAN Security Evaluation and Procurement

Kwangwoo Lee

Security Architect

2025.10.16



October 16th, 2025



Useful Guide to KOREA/KOREAN Security Evaluation and Procurement

Kwangwoo Lee

Security Architect

2025.10.16



October 16th, 2025





Contents

National Cybersecurity Framework (NIS, NCSC)

Security Verification Scheme

Crypto Module Validation

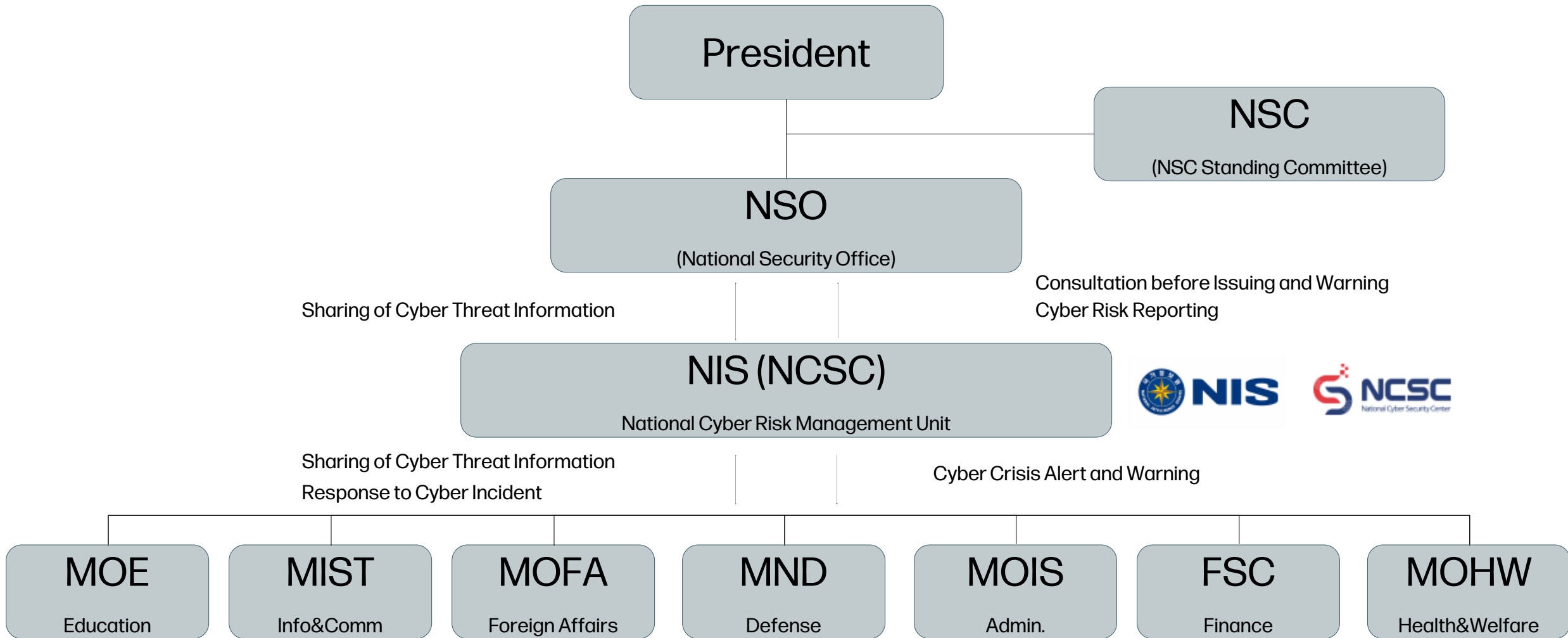
Cryptographic Algorithms Subject to Validation

Evaluation & Certification of Information Security Products (ITSCC)





National Cybersecurity Framework



Role and Responsibilities of the NIS

NIS – Cybersecurity Tasks

- Cybersecurity Intelligence
 - Collect, analyze, and share cyber threat intelligence as the national intelligence agency
- National Security Functions
 - Prevent and respond to cyberattacks targeting government and public sector
- Other Cybersecurity Missions
 - Additional roles defined by relevant laws and regulations



NCSC

- Established in 2004 under the National Intelligence Service (NIS)
- Mission: Develop response technologies with R&D centers to counter new cyber threats and enhance national defense capability
- Origin: Triggered by Slammer Worm attack (Jan 25, 2003) which disrupted ROK Internet networks for hours
- Renamed from National Cybersafety Center → NCSC on Jan 1, 2021 with NIS Act amendments



Role and Responsibilities of the NCSC

Information sharing & cooperation

- Share the information about domestic/overseas cyberthreats and countermeasures
- Raise public awareness and establish domestic/overseas cooperation channels

Policy establishment & consultation

- Establish cybersecurity policies and guidelines
- Provide security diagnosis evaluation and consultations for information network systems

Threat detection & response

- Constantly monitor major information networks
- Timely detect cyber attacks and issue an alert

Accident investigation & damage recovery

- Investigate cyber incidents and make attribution of the attack

- Provide support to minimize damages and prevent the recurrence of the campaign

Security Verification Scheme

Purpose: Strengthen security of national/public networks & defend against external threats

History & Evolution:

- 2001: Initial security review
- 2006: Renamed to “Security Verification Scheme”; CC certification required for public sector products
- 2014: Network equipment added
- 2016: Accredited labs validate products against national standards





Security Verification Scheme

Pre-Verification Policy (2020–2022): Critical products (e.g., network equipment, secure USBs, DLP, data transfer solutions) must be pre-verified before adoption

Security-Validated Products List: Published by NIS for simplified adoption (CC-certified, VSFT, performance-evaluated products)

Vulnerability Response Framework (2022): 4-level system for addressing product vulnerabilities (Levels 3–4 require immediate remediation or exclusion)

Policy Update (2022):

- Over 30,000 institutions grouped into A/B/C with tailored requirements
- Rapid Verification System introduced for new/converged technologies

Crypto Module Validation

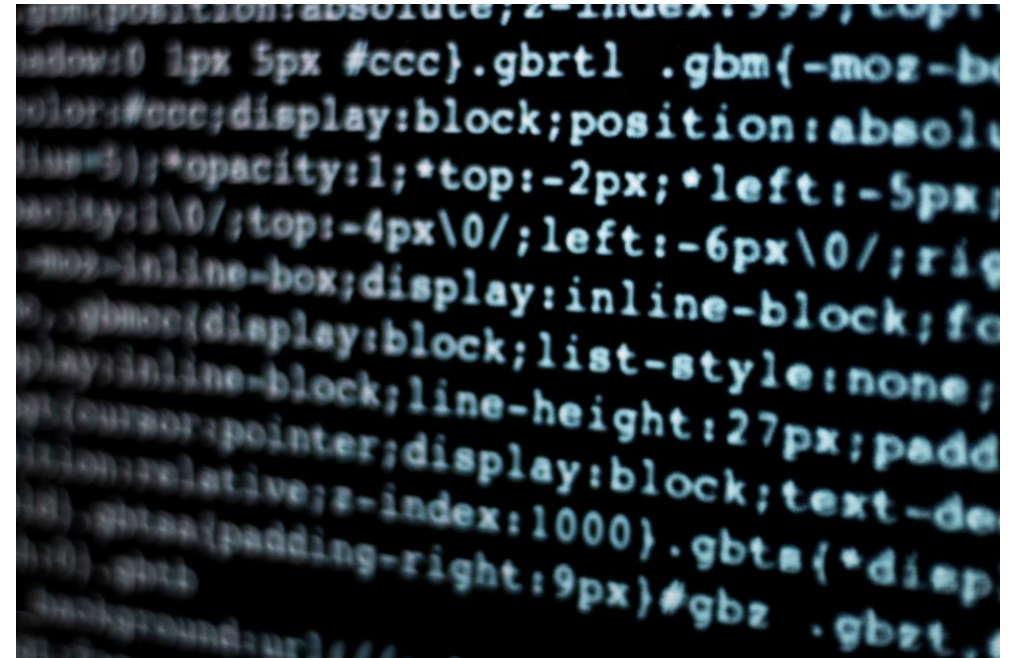
Scope: Validation of crypto modules (SW, HW, FW) protecting non-classified government data

Standards:

- KS X ISO/IEC 19790:2015 (Security Requirements), KS X ISO/IEC 24759:2015 (Testing Requirements)

Timeline:

- 2005: Program launched (NSR test lab)
- 2015-16: Revised standards adopted
- 2018: KISA designated
- 2024: First private lab (Korea System Assurance)





Crypto Module Validation

Enhancements:

- RNG testing methodology (2021 → adopted 2022)
- From 2025: Minimum 128-bit security strength required

Private Sector Transition: 2023 guideline amendment → more private labs designated

Guidance & Services:

- Operational/Implementation Guides (2022 - 24)
- Pre-Validation & Validation Management Services (with KISA, 2023)

Public platform: kcmvp.or.kr

Global Alignment: AES adoption announced (CSK 2024), validation starts Jan 2026





Cryptographic Algorithms Subject to Validation

Selection Criteria: Security strength, efficiency, standards trends, policy, interoperability, IPR

Categories (8, 23 types):

- Block ciphers, Hash functions, MACs, RNGs
- Key establishment, Public-key encryption, e-Signatures, KDFs

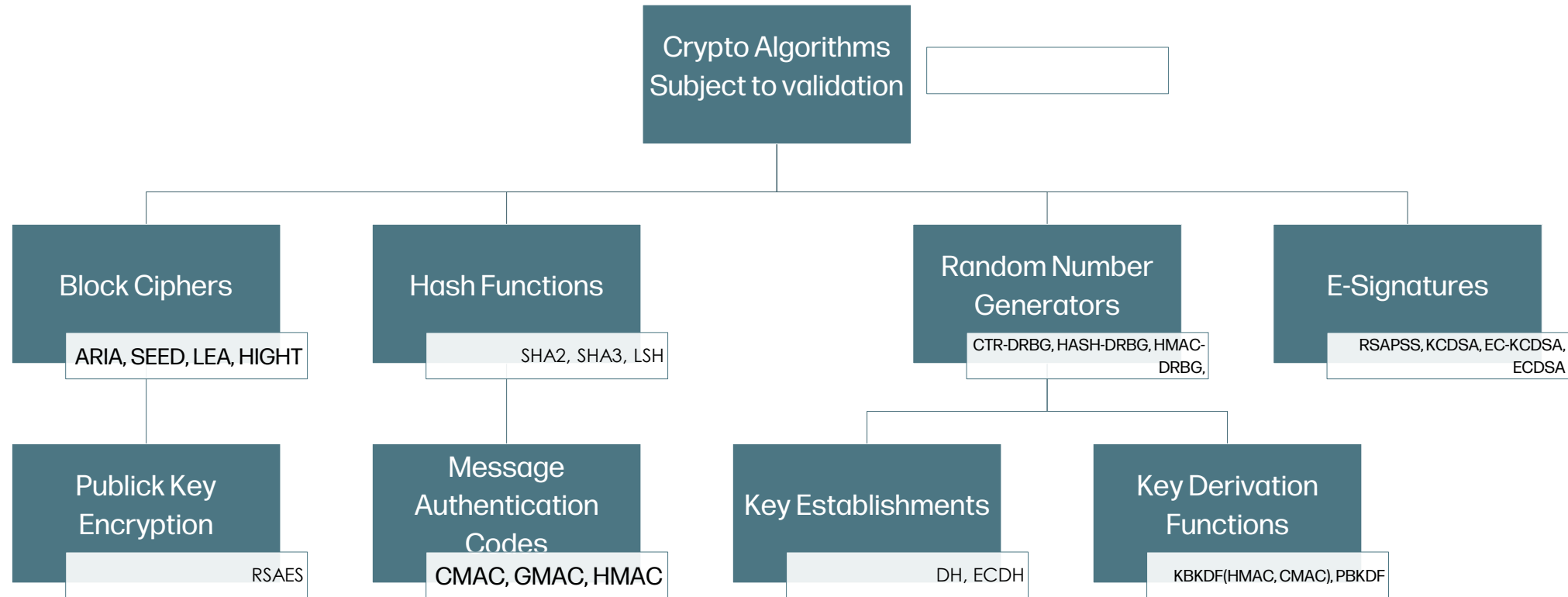
Security Strength:

- Minimum 112-bit for all algorithms
- From Jan 2025 → At least one algorithm ≥ 128 -bit required in modules

Update:

- From 2026 → AES officially included in validation scope

Cryptographic Algorithms Subject to Validation



Transition to Post-Quantum Cryptography (PQC)

Challenge: Quantum computers threaten existing public-key crypto

Initiatives:

- 2021: Launch of KpqC consortium (industry-academia-research)
- National PQC Competition → 4 Korean algorithms selected as national candidates



Transition to Post-Quantum Cryptography (PQC)

Master Plan (Jul 2023): 3-phase roadmap (goal: nationwide PQC infra by 2035)

- Mid-to-long-term crypto policy action plans
- Technical & institutional foundations for PQC transition
- Nationwide PQC adoption & secure environment by 2035

Future Directions:

- Long-term roadmap for cryptographic module validation with PQC
- Select PQC algorithms for validation via domestic/international standardization



Validated Cryptographic Modules

List of Validated Cryptographic Modules

- Available on NCSC website
- Includes: name, type, validation date, expiration, security level, policy docs, configuration data

As of Dec 2024 - Total: 100 modules

- 80 software
- 10 firmware
- 2 hybrid firmware
- 8 hardware





ITSCC

IT Security Certification Center (ITSCC) is Certification Body responsible for carrying out certification and overseeing the day-to-day operation of an evaluation and certification scheme.





Evaluation & Certification of Information Security Products

History:

1998: K Criteria launched (IPS, IDS, VPN, OS security, biometrics, smart cards)

2005: Transition to **Common Criteria (CC)** → All product types included

2006: K Criteria abolished

K/CC





Evaluation & Certification of Information Security Products

Evolution:

2007: Split into international & domestic tracks → reduced SME burden

2010: Simplified domestic evaluation

2011 – 2013: Expanded to 28 categories (incl. mobile, source code tools)

2012: National security requirements & 3-year certificate validity introduced

2014: Policy oversight transferred to MSIT

2017: Reflected updated **CCRA agreements**, 7 new PPs developed

Evaluation & Certification of Information Security Products

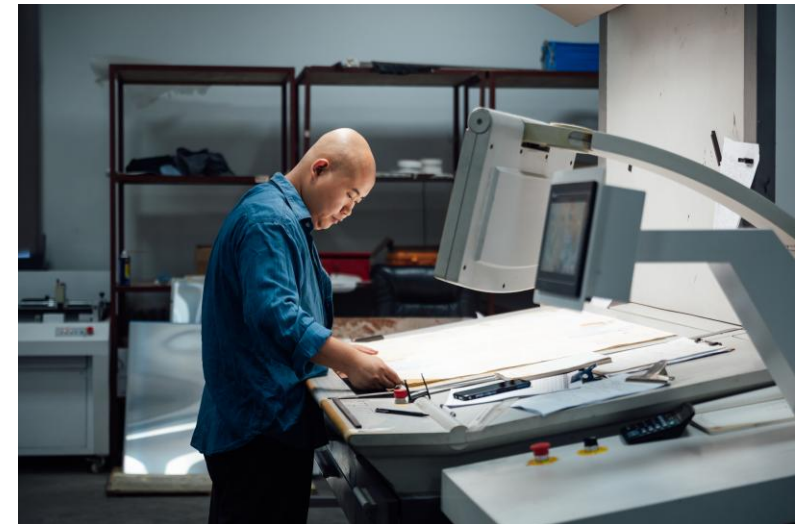
Recent Updates:

2020: Secure USBs with VSFT cert allowed without CC; CC scope reduced to 18

2018-2024: Development & adoption of **HCD cPP** for public procurement

2021: National Security Requirements v3.0 → 27 product categories, incl. quantum devices & video surveillance

By 2024: 17 national PPs published





Evaluation & Certification of Information Security Products

Supportive Policy:

2019: Enforcement Decree amended → CC-certified products meeting national security requirements eligible for sole-source procurement

What does ITSCC do? (1/2)

- Establishes and implements Korea IT Security Evaluation and Certification Regulation, guidelines and procedures related to evaluation and certification.
- Produces certification reports and issues certificates.
- Manages certified products including publication of the certified products list.
- Establishes and implements the internal rules and regulations regarding the operation of the certification body, and qualifies certifiers.
- Approves, suspends, and cancels the license of evaluation facilities, and qualifies evaluators.



What does ITSCC do? (2/2)

- Oversees the evaluation facility's evaluation activities and investigates the evaluation facility's security management conditions.
- Participates in the technical competency assessment of the accreditation body for accrediting the accredited testing laboratory.
- Mediates disputes between the sponsor and the evaluation facility.
- Takes part in activities related to Common Criteria Recognition Arrangement (CCRA).
- Registers and manages the certified PPs.

IT Security Evaluation and Certification Scheme

Basic Objectives

- To achieve global reliability of an IT security product
- To enhance the information security level of the national communication network and the competitiveness of an IT security product

Legal Grounds

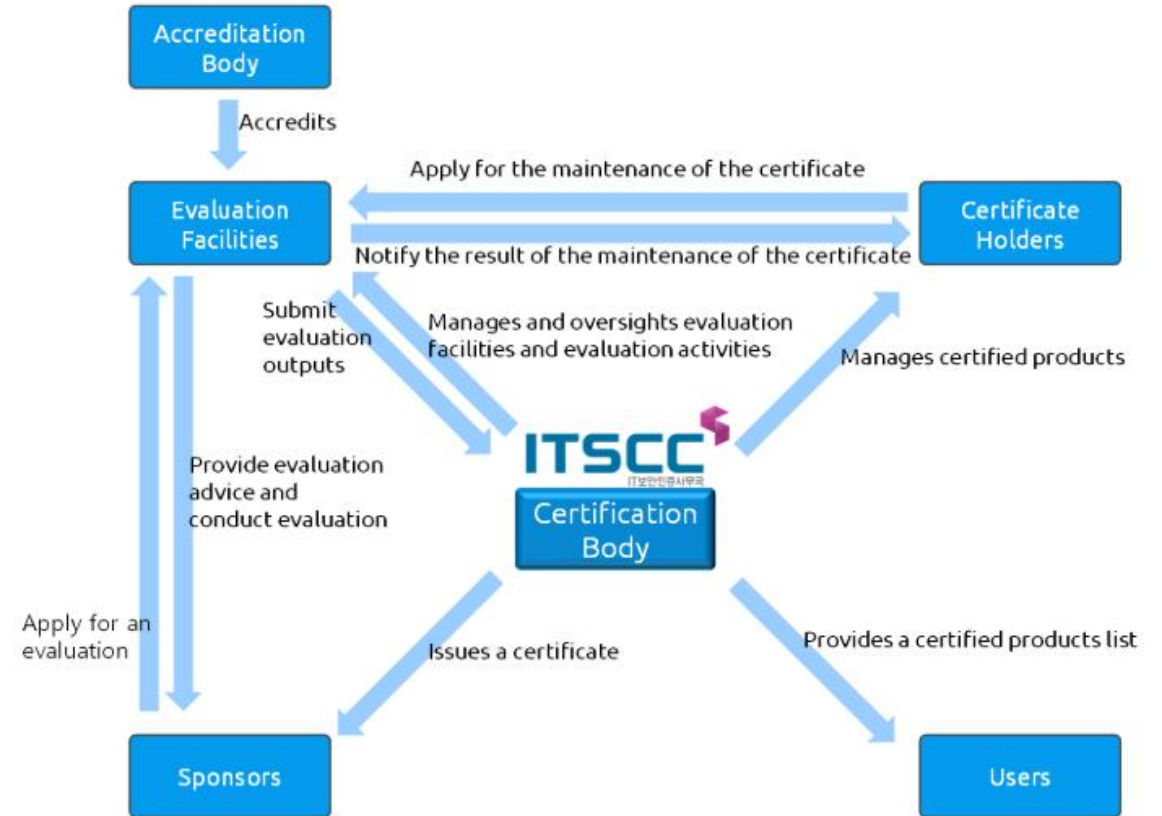
- FRAMEWORK ACT ON INTELLIGENT INFORMATIZATION, Article 58 (Public Notice of Standards for Information Protection Systems)
- ENFORCEMENT DECREE OF FRAMEWORK ACT ON INTELLIGENT INFORMATIZATION, Article 51 (Public Notice of Standards for Information Protection Systems)
- Common Criteria for Information Technology Security Evaluation (Ministry of Science, ICT and Future Planning Notice No. 2013-51)
- Korea IT Security Evaluation and Certification Guidelines (Ministry of Science and ICT Guidance No. 2022-61)

Regulations

- Korea IT Security Evaluation and Certification Regulation (Ministry of Science and ICT-ITSCC, May 17, 2021)

Evaluation and Certification Scheme

The evaluation and certification system of information security products is divided into four distinct entities based on roles and responsibilities: policy authority, certification authority, evaluation laboratories, and accreditation body.



Scheme Authorities

Organization

- Ministry of Science and ICT (MSIT)

Duties

- Enactment and amendment of the laws related to the evaluation and certification scheme
- Establishment of the evaluation and certification scheme
- Securing budgets for the evaluation and certification scheme



Ministry of Science and ICT



Certification Body

Organization

- IT Security Certification Center (ITSCC) of National Security Research Institute (NSR)

Duties

- Approval of evaluation results and issuance of certificates
- Licensing and management of evaluation facilities and support on CC certification policy establishment
- International activities such as CCRA



Evaluation Facilities

Evaluation Facilities

- KISA(1998), KOSYAS(2007), KSEL(2009), TTA(2009),KTR(2010), KOIST(2014), KTC(2014)

Duties

- Operation of the evaluation facility based on the quality manual as accredited testing laboratory by KOLAS (Korea Laboratory Accreditation Scheme)
- Evaluation of products including examination of evaluation deliverables, testing and vulnerability analysis
- Education and training of evaluators
- Site visit of developers

Accreditation body

Organization

- Korean Agency for Technology and Standards (KATS)

Duties

- accredits laboratories seeking recognition as information security product evaluation laboratories by the certification authority
- Ensuring compliance with international testing and calibration standards





Status of Evaluation and Certification

Total Certifications: 1,311

- 1,110 domestic; 201 international
 - Includes revoked/expired certificates

Domestic Certifications

- Over half are network security devices (IPS, IDS, ACS)

International Certifications

- Over half are smart card solutions (e-passports, OS) and digital MFPs
- 2016-2017: Expanded to smart TV security software
- Since 2018: Cryptographic products (document & DB encryption, integrated authentication)

Recent Trend

- Since 2020: ~70 certifications annually
 - 57 domestic, 13 international



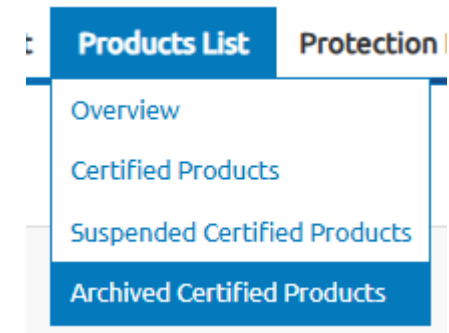


Overview

IT Security Certification Center publishes the security target (ST), the certificate, and the certification report of the certified product in the Certified Products List (CPL).

The CPL is categorized as follows.

- Certified products
 - Lists currently valid certified products.
- Suspended certified products
 - Lists products whose certificate validity was suspended for a determined period.
- Archived certified products
 - Lists products whose certificate validity period is expired.





Reports

Certification report

- A document produced by the certification body that summarizes the results to conduct the certification.

Maintenance Report

- A document produced by the certification body in case of changes that give minor affects to the assurance of the certified product.





Certified Products

Product	Certification No.	Certificate Holder	EAL	Type of Product	Date of Certification
KCOS e-Passport Version 5.1 - SAC, EAC and AA on S3D384E	KECS-ISIS-1372-2025	KOMSCO	EAL5+	e-Passport	2025-09-30
KCOS e-Passport Version 5.1 - BAC and AA on S3D384E	KECS-ISIS-1371-2025	KOMSCO	EAL4+	e-Passport	2025-09-30
KOMSCO JK62 V1.1	KECS-ISIS-1370-2025	KOMSCO	EAL5+	Java card platform	2025-09-30
Alpha DBGuard V2.1	KECS-CISS-1368-2025	Alphabit Co.,Ltd.	PP Compliant	DB Encryption	2025-09-25
eXSignOn V4.0	KECS-CISS-1366-2025	tomatosystem	PP Compliant	SSO	2025-09-12
PrivacyDB V3.0	KECS-CISS-1345-2025	OWL Systems Inc.	PP Compliant	DB Encryption	2025-05-26
KSignAccess V5.0	KECS-CISS-1342-2025	KSign Co., LTD.	PP Compliant	SSO	2025-03-07
DocuRay x v3.5	KECS-CISS-1341-2025	BlueMoonSoft Inc.	PP Compliant	Electronic Document Encryption	2025-03-04
Sindoh MF2000, MF3000, MF4000, N630 Series	KECS-CISS-1334-2024	Sindoh Co., Ltd.	EAL2	Digital Multifunction Printer	2024-11-13
D'Guard v5.0	KECS-CISS-1333-2024	INEB Inc.	PP Compliant	DB Encryption	2024-10-25






Search Options

 [KOREAN](#) | [Site Map](#) 

[About](#) [Products List](#) [Protection Profiles](#) [External Links](#)

Certified Products

Search Options 

Product name	<input type="text" value="Product name"/>
Certification No.	<input type="text" value="Certification No."/>
Certificate holder	<input type="text" value="Certificate holder"/>
EAL	<input type="text" value="Select an EAL"/> ▼
Type of product	<input type="text" value="Select a type of product"/> ▼
Year of certification	<input type="text" value="Year of certification"/>
Evaluation facility	<input type="text" value="Select an evaluation facility"/> ▼





Archived Certified Products



KOREAN | Site Map

Search this site



About

Products List

Protection Profiles

External Links

Archived Certified Products

Search Options



Product	Certification No.	Certificate Holder	EAL	Type of Product	Date of Certification
Smart TV Security Solution V5.0 for Samsung Knox	KECS-CISS-1047-2020	Samsung Electronics Co., Ltd.	EAL1	Smart TV Security Solution	2020-10-08
EdgeDB v4.0	KECS-CISS-1046-2020	SECUCEN	PP Compliant	DB Encryption	2020-10-06
MagicDBPlus v2.0	KECS-CISS-1042-2020	Dreamsecurity	PP Compliant	DB Encryption	2020-09-08
Samsung Multifunction MultiXpress K4250, K4300, K4350, K401, X4220, X4250, X4300, X401, X400, K7400, K7500, K7600, X7400, X7500, X7600, X704, X706, K705, K706 Series	KECS-CISS-1035-2020	HP Inc.	EAL2+	Digital Multifunction Printer	2020-08-26
KOMSCO JK62 V1.0	KECS-ISIS-1031-2020	KOMSCO	EAL5+	Java card platform	2020-08-04





Protection Profile

Protection Profile	Certification No.	EAL	Type of Product	Date of Certification
Korean National Protection Profile for Wireless LAN Authentication V3.0	KECS-PP-1353-2025	EAL1+	Wireless LAN Authentication	2025-06-27
Korean National Protection Profile for Network Access Control V3.0	KECS-PP-1352-2025	EAL1+	NAC	2025-06-27
Korean National Protection Profile for Mobile Device Management V3.0	KECS-PP-1351-2025	EAL1+	MDM	2025-06-27
Korean National Protection Profile for Database Encryption V3.1	KECS-PP-1350-2025	EAL1+	DB Encryption	2025-06-27
Korean National Protection Profile for Electronic Document Encryption V3.1	KECS-PP-1349-2025	EAL1+	Electronic Document Encryption	2025-06-27
Korean National Protection Profile for Single Sign On V3.1	KECS-PP-1348-2025	EAL1+	SSO	2025-06-27
Korean National Protection Profile for Database Access Control V3.0	KECS-PP-1316-2024	EAL1+	DB Access Control	2024-06-28
Korean National Protection Profile for Wireless Intrusion Prevention System V3.0	KECS-PP-1315-2024	EAL1+	WIPS	2024-06-28
Korean National Protection Profile for Voice over IP Firewall V3.0	KECS-PP-1314-2024	EAL1+	VoIP Firewall	2024-06-28
Korean National Protection Profile for Intrusion Prevention System V3.0	KECS-PP-1313-2024	EAL1+	IPS	2024-06-28

Protection Profile	Certification No.	EAL	Type of Product	Date of Certification
Korean National Protection Profile for Firewall V3.0	KECS-PP-1312-2024	EAL1+	FW	2024-06-28
Korean National Protection Profile for Enterprise Security Management V3.0	KECS-PP-1311-2024	EAL1+	ESM	2024-06-28
Korean National Protection Profile for Virtual Private Network V3.0	KECS-PP-1310-2024	EAL1+	VPN	2024-06-28
Korean National Protection Profile for Web Application Firewall V3.0	KECS-PP-1234-2023	EAL1+	Web Application Firewall	2023-04-27
Korean National Protection Profile for Access Control in Operating System V3.0	KECS-PP-1233-2023	EAL1+	Access Control in OS	2023-04-27
Korean National Protection Profile for Database Encryption V3.0	KECS-PP-1232-2023	EAL1+	DB Encryption	2023-04-27
Korean National Protection Profile for Electronic Document Encryption V3.0	KECS-PP-1231-2023	EAL1+	Electronic Document Encryption	2023-04-27
Korean National Protection Profile for Single Sign On V3.0	KECS-PP-1230-2023	EAL1+	SSO	2023-04-27
ePassport Protection Profile V2.0	KECS-PP-0163-2009	EAL4+	e-Passport	2009-05-06
Smart Card Open Platform Protection Profile V2.0	KECS-PP-0097-2008	EAL4+	Smartcard	2008-04-24





Archived Protection Profile

Protection Profile	Certification No.	EAL	Type of Product	Date of Certification
Protection Profile for Network Data Loss Prevention V1.0	KECS-PP-1206-2022	EAL1+	DLP	2022-12-15
Protection Profile for Host Data Loss Prevention V1.0	KECS-PP-1205-2022	EAL1+	DLP	2022-12-15
Korean National Protection Profile for Web Application Firewall V1.0	KECS-PP-0982-2019	EAL1+	Web Application Firewall	2019-12-11
Korean National Protection Profile for Access Control in Operating System V1.0	KECS-PP-0960-2019	EAL1+	Access Control in OS	2019-08-30
Korean National Protection Profile for Enterprise Security Management V1.0	KECS-PP-0959-2019	EAL1+	ESM	2019-08-30
Protection Profile for Network Device V1.0	KECS-PP-0946-2019	EAL1+	Network Device	2019-07-11
Korean National Protection Profile for Network Access Control V1.0	KECS-PP-0933-2019	EAL1+	NAC	2019-05-31
Korean National Protection Profile for Database Access Control V1.0	KECS-PP-0905-2018	EAL1+	DB Access Control	2018-11-23
Korean National Protection Profile for Mobile Device Management V1.0	KECS-PP-0904-2018	EAL1+	MDM	2018-11-23
Korean National Protection Profile for Single Sign On V1.0	KECS-PP-0822-2017	EAL1+	SSO	2017-08-18

Protection Profile	Certification No.	EAL	Type of Product	Date of Certification
Korean National Protection Profile for Electronic Document Encryption V1.0	KECS-PP-0821-2017	EAL1+	Electronic Document Encryption	2017-08-18
Korean National Protection Profile for Database Encryption V1.0	KECS-PP-0820-2017	EAL1+	DB Encryption	2017-08-18
Korean National Protection Profile for Wireless Intrusion Prevention System V1.0	KECS-PP-0819-2017	EAL1+	WIPS	2017-08-18
Korean National Protection Profile for Network Data Loss Prevention V1.0	KECS-PP-0805-2017	EAL1+	DLP	2017-07-07
Korean National Protection Profile for Host Data Loss Prevention V1.0	KECS-PP-0804-2017	EAL1+	DLP	2017-07-07
Korean National Protection Profile for Intrusion Prevention System V1.0	KECS-PP-0803-2017	EAL1+	IPS	2017-07-07
Korean National Protection Profile for Wireless LAN Authentication V1.0	KECS-PP-0718-2016	EAL1+	Wireless LAN Authentication	2016-06-10
Korean National Protection Profile for Voice over IP Firewall V1.0	KECS-PP-0717-2016	EAL1+	VoIP Firewall	2016-06-10
Korean National Protection Profile for Virtual Private Network V1.0	KECS-PP-0716-2016	EAL1+	VPN	2016-06-10
Korean National Protection Profile for Firewall V1.0	KECS-PP-0715-2016	EAL1+	FW	2016-06-10

Protection Profile	Certification No.	EAL	Type of Product	Date of Certification
Korean National Protection Profile for Network Device V1.0	KECS-PP-0714-2016	EAL1+	Network Device	2016-06-10
Firewall Protection Profile V2.0	KECS-PP-0093-2008	EAL4	FW	2008-04-24
ePassport Protection Profile V1.0	KECS-PP-0084-2008	EAL4+	e-Passport	2008-01-04



Evaluation Facilities

- Korea Internet & Security Agency (KISA)
- Korea System Assurance, Inc. (KOSYAS)
- Korea Security Evaluation Laboratory (KSEL)
- Telecommunications Technology Association (TTA)
- Korea Information Security Technology (KOIST)
- Korea Testing Certification (KTC)
- Korea Testing & Research Institute (KTR)



Thank you

