INSTAR

CYBERSTAND.eu

indico GLOBAL

With the participation of our international partner TTA TTA

WORKSHOP

The EU's Impact on International Cybersecurity & eID Standardisation efforts

25 MARCH 2025
09:30-11:00 CET

Funded by the European Union

INSTAR CYBERSTAND.eu indico GLOBAL

WORKSHOP

The EU's Impact on International Cybersecurity & eID Standardisation efforts

Funded by the European Union

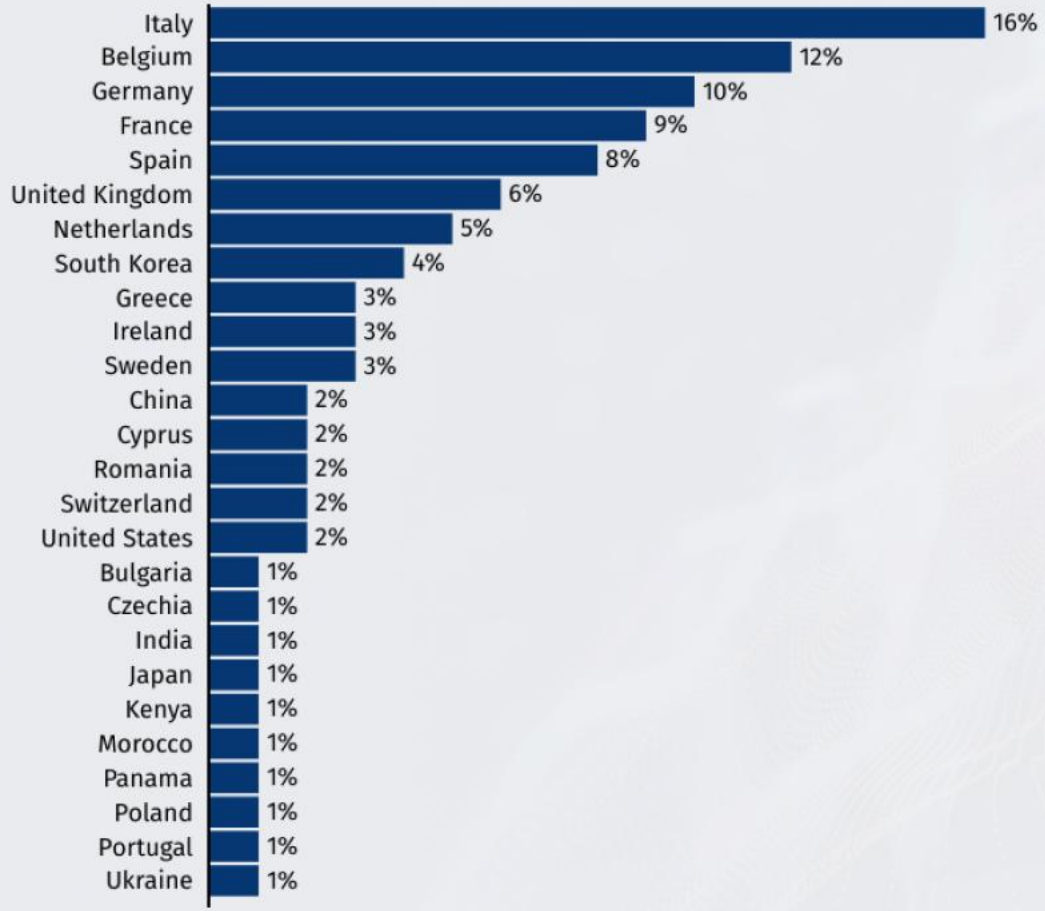
25 ETFs Members

100 Registrants

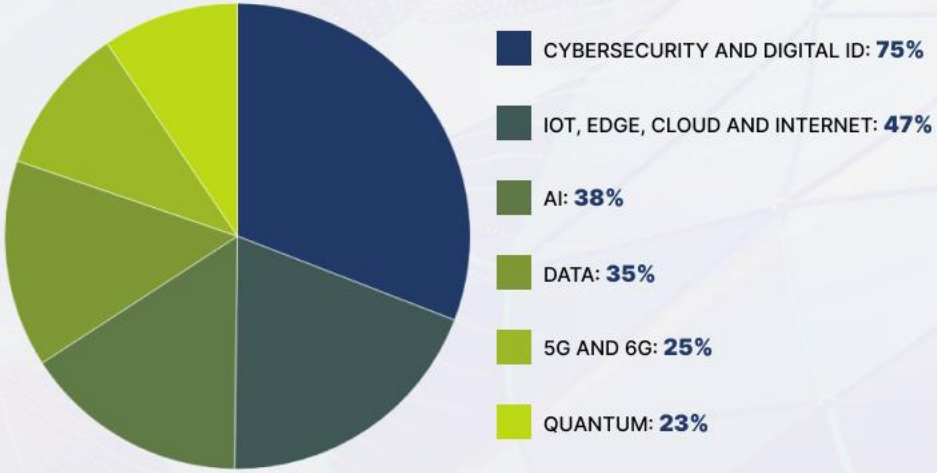
Gender

61% 19%

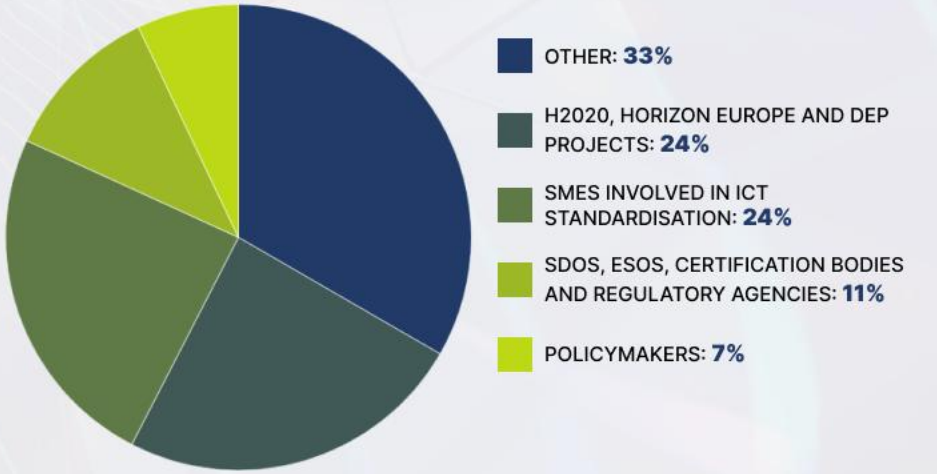
Participants by country



Participants by domain



Represented Stakeholders



INSTAR

OBJECTIVES

General Objective: To support the implementation of the EU Digital Partnerships and the EU-US TTC by working together with 7 international partners to drive international standards for 6 emerging technologies

- Obj.1: Organise events to collect feedback to guide the activities of the EU Digital Partnerships & EU-US TTC
- Obj.2: Multilateral coordination with the 7 international partners on long-term common standardisation goals
- Obj.3: Create an EU standardisation priorities roadmap to guide the activities of the SDOs, EU Digital Partnerships and EU-US TTC

Community

- Coordination Board with SDO reps.
- 6 International Task Forces
- 1,000+ engaged community members across all Stakeholder Groups (SGs)

Key Exploitable Results

Synergies

- Signed MoUs with National, European, and Int'l organisations and initiatives
- Continuous engagement and exchanges on all ICT standards topics
- Regular interactions with relevant EC Offices & other: (Including. MSP, Sherpa Groups of the High-level standardisation office, STAIR
- Collaborations with targeted HE Standards projects:

HSbooster.eu · StandICT.eu · STAND4EU · EDU4Standards.eu · indico GLOBAL

Outreach

- 6 Workshops on results from the ETFs
- 6 Webinars on the roadmaps
- 1 Final INSTAR Impact event
- 8 newsletters
- 5 Professional Videos
- Visibility at 24 3rd party events
- Social media channel presence
- 10 Press Releases

Reports & other value-add info

- 6 Roadmaps (with digestable downloadable factsheet)
- Targeted blogposts in key technology areas
- 1 Report to assess SSH implications
- All Results published via zenodo
- Bi annual reports on each workstream

Technological scope

Geographical scope

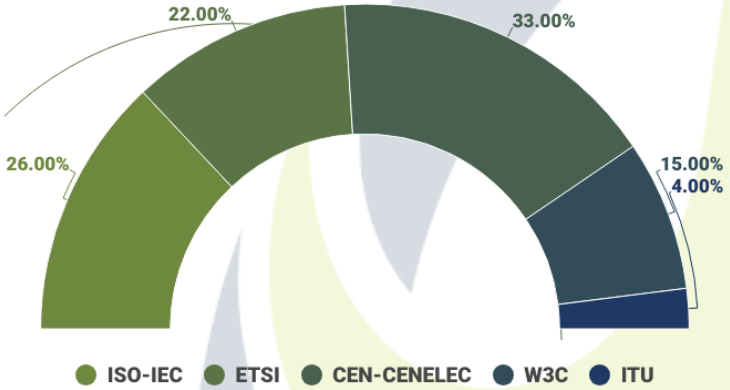
7

USA JAP
CAN ROK
SGP AUS
TWN

Coordinator: BluSpecs · Fraunhofer · fortiss · Alliance for IoT and Edge Computing Innovation · Trialog · TU Delft · Trust-iT services · COMMpla · AIT Austrian Institute of Technology · Demokritos

Cybersecurity/eID-ETF

- 16 experts.
- Experts participation in SDOs:
  - **ISO-IEC 33%** **ETSI 22%**
  - **CEN-CENELEC 26%** **W3C 4%**
  - **ITU 15%)**



What has been achieved so far:

- First **Roadmap Factsheet** published.
- 8 Cybersecurity and 8 eID standardisation priorities identified.
- 4 INSTAR Cyber/eID experts funded through the **CYBERSTAND Specific Service Procedure** to contribute to the development of harmonised standards for the Cyber Resilience Act.
- 7 INSTAR Cyber/eID experts funded through the **StandICT open calls**.

Recent activities

Joined 4 INSTAR events as speakers/participants

- **Shaping International Standards in Advanced ICT Tech Regulation**
- **INSTAR Roadmaps. Mapping future priority topics with our European Task Forces**.
- **Workshop on Cross-Domain Standardisation and Architecture for IoT and Edge Computing**.
- **EU – Canada alignment on digital credentials, identity and trust services**.

EU Cybersecurity/eID Standardisation Priorities

Cybersecurity:

- Adopt Quantum-Resistant Cryptography.
- Introduce a Cybersecurity Labeling Scheme.
- Develop Standards for Vulnerability Handling.
- Ensure IoT Product Security Conformity.
- Promote cross-border compliance with EU regulations.
- Develop Standards for Implementing a Zero-trust Architecture, including secure identity and access management, and multi-factor authentication (MFA).
- Develop a Decentralised Public Key Infrastructure (DPKI).
- Develop a standardised cybersecurity framework in alignment with existing regulations, such as the NIS2 Directive and the EU Cybersecurity Act.

Digital ID:

- Promote the European Digital Identity Wallet (EUDIW).
- Develop Digital ID Interoperability Framework that ensures the interoperability of national e-ID schemes and digital ID wallets across borders.
- Explore future cryptographic capabilities, e.g. privacy-enhancing ZKP.
- Align and Recognise Trust Services Across Borders.
- Ensure the Security of Digital Wallets.
- Integrate eIDAS into new initiatives like Digital Product Passport (ESPR Regulation).
- Integrate Privacy by Design in eID Wallets.
- Develop Trust Frameworks for Decentralised Identity.

CYBERSTAND.eu
Engaging & supporting EU experts in Cybersecurity Standardisation activities

Supporting EU experts in Cybersecurity standardisation activities for the Cyber Resilience Act

A 36 months (June 2024 – May 2027)
Coordination & Support Action with €2,999,999.09 budget with € 1,500,000 allocated to funding.

6 Specific Service procedures €1.5 million

APPLY HERE

25+ Experts funded

- Funding to contribute to standardisation activities related to the draft Cyber Resilience Act Standardisation Request topics. Funding types*
- 5th Specific Service Procedure
  Deadline: 11 April 2025 CoB.

Multi-stakeholder dialogue around the CRA

JOIN NOW

60+ members

- Identify and provide recommendations on key priority areas for standardisation activities;
- Awareness and outreach to ensure standardisation is understood and aligned with the market;
- Support the drafting of guidelines and recommendations.

VISIT CYBERSTAND.EU

*Applicants individuals or natural persons residing in European Member States and Associate countries.

Trust-iTservices communicating to markets · COMMpla Communication Platforms and Online Solutions · ECSO · European DIGITAL SME Alliance · ETSI · CEN · CENELEC

InDiCo-Global:
Promoting EU digital policies & standards globally

Catalyst for collaboration between EU and partner countries on **ICT standardization**

Build bridges and **foster capacity building** with partner countries in the area of Digital

Help EU and partners understand each other's **regulatory frameworks** and **standardization models**

Promote **inclusive** and **cooperative** processes for the development of **global ICT standards** supporting and **embedding EU values**

A 36 months action with 2.5M€ budget, starting Jan. 24
40% of budget allocated to third party funding (FSTP)

Priority topics
European Standardisation System, NLF, AI, 5G and beyond, IoT and its security aspects, internet, cybersecurity, data, eID, quantum, distributed ledger technologies (DLT), circular economy or smart cities), Data Protection

Scope of activities
Studies, capacity and awareness building, workshops & technical events, funded projects through FSTP

Geographical scope
India, China, Southeast Asia, African Union, Latin America and Caribbean (LAC), Western Balkans and Eastern Partnership

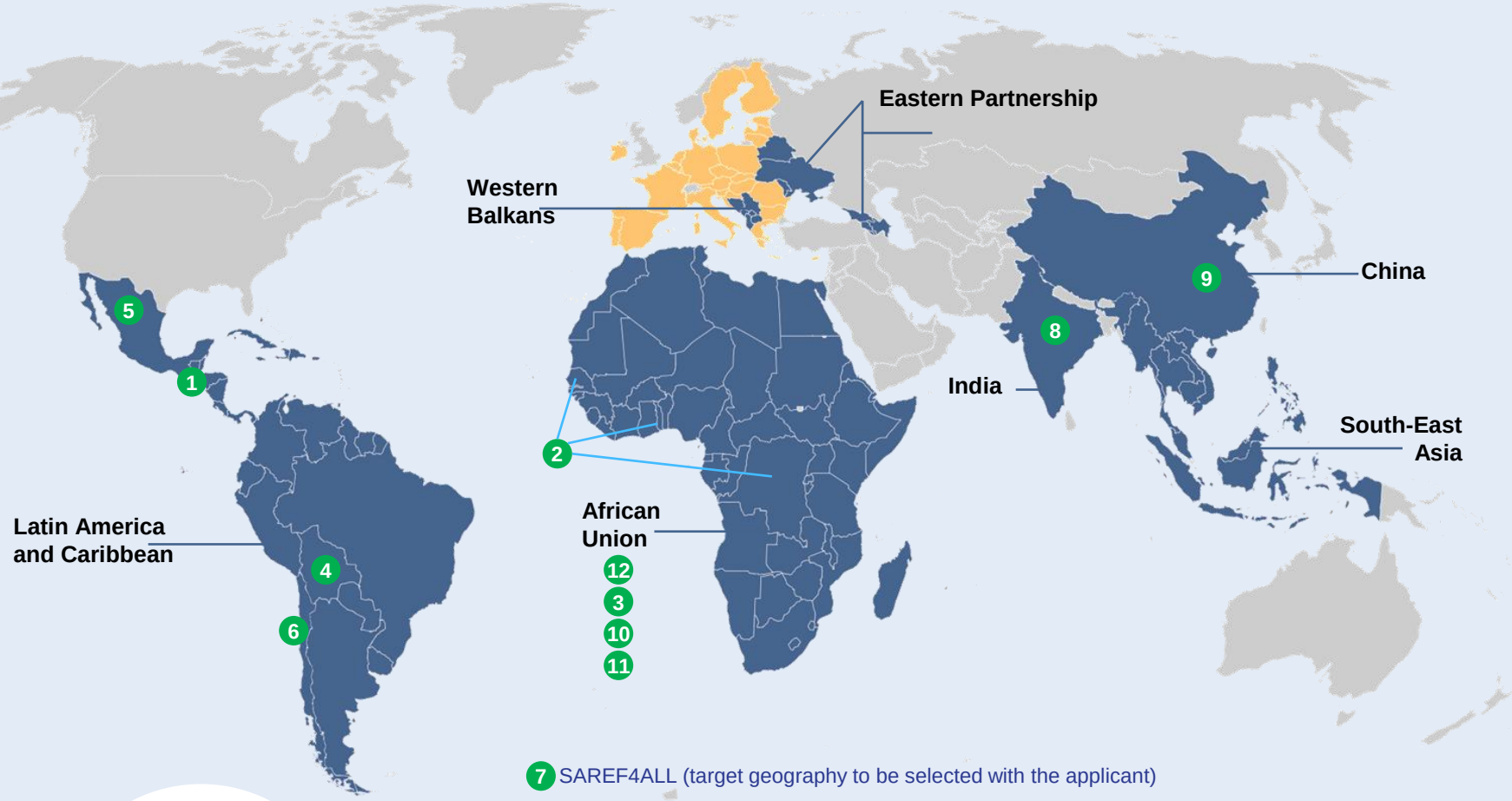
indico GLOBAL

Implemented by ETSI CEN CENELEC MARTEL innovate Trust-iT COMMpla

Funded by the European Union

www.indico-global.eu

Projects funded following Open Call #1



1. Enhancing Digital Government in Guatemala through European Standards
2. Use of AI systems in online content moderation, review and remedies in EU and in OHADA regions
3. Accessiblity Standards/EAA in Africa
4. Fostering data protection and responsible IA compliance in Bolivia
5. Bridging the Gap Between European and Mexican ICT Standards in Open Data
6. High Impact Workshops for Knowledge Exchange Between Chile and Europe on Standardisation Initiatives
7. SAREF4ALL
8. Artificial Intelligence, Landscaping analyses/ studies
9. Geopolitics of Semiconductor Standards & High-Performance Computing Chips: De-Risking China Project
10. Advancing AI Policy Development in Africa: Harmonizing with EU Standards for Sustainable Innovation
11. Developing Guidelines on Common Denominators for Security Levels of Digital Identity Wallets
12. Understanding EU Climate Fintech: Legal and Regulatory Perspectives

7 SAREF4ALL (target geography to be selected with the applicant)

Global ID Standardization

2025-25-Mar

Kyeong Hee OH, TCA services

khoh@tcaservices.kr

International Standardization Organizations

IdM roadmap (https://www.itu.int/en/ITU-T/studygroups/com17/ict/Pages/ict-part06.aspx)

- DID WG
- VC WG
- CCG

- SC 27
  WG5

JTC 1/Open ID std

- TC 307
  JWG4

- SG 17
  Q10
  Q11
  Q14

OpenWallet Forum

International Standardization Organizations

IdM roadmap (https://www.itu.int/en/ITU-T/studygroups/com17/ict/Pages/ict-part06.aspx)

- DID WG
- VC WG
- CCG

- SC 27 WG5

JTC 1/Open ID std

ISO/IEC 26131:2024 Information technology — OpenID connect — OpenID connect core 1.0 incorporating errata set 2

ISO/IEC 26132:2024 Information technology — OpenID connect — OpenID connect discovery 1.0 incorporating errata set 2

ISO/IEC 26133:2024 Information technology — OpenID connect — OpenID connect dynamic client registration 1.0 incorporating errata set 2

ISO/IEC 26134:2024 Information technology — OpenID connect — OpenID connect RP-initiated logout 1.0

ISO/IEC 26135:2024 Information technology — OpenID connect — OpenID connect session management 1.0

OpenWallet Forum

Save the date
for the launch of the

Global Digital Collaboration

to foster wallets, credentials and trusted infrastructure
for the benefit of all humans

July 1-2, 2025
CICG Geneva, Switzerland

Hosted by the Swiss Confederation

ID standardization in Korea

- TTA (21 standards)
  - PG 502 Personal Information Protection/ID Management, Blockchain Security
  - PG 1006 Blockchain-based Technology Project Group
    - mobile driver's license standards based on decentralized identifiers
- DLTSF
  - DID standardization based on DLT
- DID Forum
  - Policy, technology, standardization

Interoperability between standards

- Mobile Identification - Part 1: DID based Mobile Driver's License (2023)

- ISO/IEC 18013-5:2021 Personal identification — ISO-compliant driving licence Part 5: Mobile driving licence (mDL) application
- ISO/IEC TS 18013-7:2024 Personal identification — ISO-compliant driving licence Part 7: Mobile driving licence (mDL) add-on functions

Issues

- Different standards, duplicated efforts in several SDOs
- Do we have a common understanding?
  - Digital ID? e-ID?
  - Decentralized ID vs Conventional ID in centralized & Federated IDM
  - Big ecosystem and components are there
- Can we develop a single one std for all?
  - Bottom-up vs. top-down
  - Interoperable digital ID or interoperable digital passport?
- Policy decision of the relying party
  - Will DPKI succeed?
- Collaboration: How, where and on what?

INSTAR Presentation

RED Art 3.3 cybersecurity

Octavian Popescu, consultant EUCOMREG SRL

Radio Equipment Directive (RED) delegated regulation on cybersecurity Overview

- Radio equipment placed on the EU single market must comply with the essential requirements of the RED. The RED was adopted in 2014.

- European Commission (EC) adopted the RED Delegated Regulation 2022/30 on cybersecurity through which RED Articles 3(3) d, e, f essential requirements are activated and will be enforced from 1 Aug. 2025. This is the first time products will have to comply with cybersecurity essential requirements.

- The aim of the EC is an overall improvement of the network cybersecurity and related features protecting personal data and privacy of the user. In this spirit, manufacturers of wireless devices will now have to include technical features to improve the level of cybersecurity of such devices before placing them on the European market.

- There are several ways to demonstrate compliance with the essential requirements, the two most used are the Notified Body (NB) route and harmonised standards conferring a presumption of conformity with Directive 2014/53/EU.

- Cyber Resilience Act (CRA) will repeal RED Art. 3.3 d, e, f. The transition from RED Art 3.3 d, e, f to CRA will be done quickly and the vast majority of equipment will fall in the basic CRA compliance category.

Harmonised standards for cybersecurity under the RED delegated regulation Current status

- The RED Delegated Regulation 2022/30 imposes essential requirements, formulated in general terms as objectives to be achieved, that are deemed necessary for ensuring an adequate level of cybersecurity, personal data protection and privacy.

- By Implementing Decision C(2022)5637, the EC addressed a Standardisation Request to two of the European Standardisation Organisations: CEN and CENELEC in order to develop harmonised standards in support of this legislation.

- Harmonised standards EN 18031-1:2024, EN 18031-2:2024 and EN 18031-3:2024 were developed with the participation of the European stakeholders including industry, and were assessed by the Commission against the essential requirements laid down by the EU legal framework.

- The standards were cited in the OJEU, with restrictions as clarified in EC Implementing Decision (EU) 2025/138 of 28 January 2025 amending Implementing Decision (EU) 2022/2191.

- The restrictions not conferring a presumption of conformity are given in the Annex of the Implementing Decision 2025/138, and refer to the rationale and guidance not being applicable, situations when the user might not set a password, and opportunities for not ensuring the parental or guardian access control.

How standards for the RED delegated regulation can be used to support the development standards for CRA

- The Cyber Resilience Act (CRA) was adopted as Regulation (EU) 2024/2847 of the European Parliament and of the Council, on horizontal cybersecurity requirements for products with digital elements.

- The CRA mentions that its essential cybersecurity requirements are aligned with the objectives of the requirements included in the RED SR and therefore the work carried out under this SR should be taken into account.

- Using the EN 18031-X:2024 Harmonised Standards, manufacturers may be able to make an assessment of their product based on a decision tree. Such an assessment is divided in: conceptual assessment, functional completeness assessment, functional sufficiency assessment. These concepts should be useful when producing standardisation deliverables for the CRA SR.

How the Cyber Resilience Act will impact international cybersecurity standards

International cybersecurity standards in which Korea is involved

2025.03.25

Heebong Choi
hhbchoi@gmail.com

What is EU-CRA?

- Aim
  - Improve cybersecurity for **digital products and services** across the European Union
  - ensure that hardware and software products meet cybersecurity requirements throughout their lifecycle

Korea ACT

- Act on Promotion of Information and Communications Network Utilization and Information Protection (**Information and Communications Network Act**)
  - focuses on protecting personal information and ensuring the security of information and communications networks
- **Personal Information Protection Act** (PIPA)
  - Focuses on protecting the privacy rights of individuals by regulating the collection, use, and management of personal information.
- South Korea has established a **national strategy** to bolster cybersecurity across various sectors, aiming to protect critical infrastructure and respond effectively to cyber threats from North Korea
  - Korea does not have a specific law titled "Cyber Resilience Act" similar to the European Union's Cyber Resilience Act (CRA)

Global Regulatory Alignment

- **International standardization activities** can contribute to global regulatory alignment.

- Korea's "Act on Promotion of Information and Communications Network Utilization and Information Protection" regulation **can be** aligned with the EU's "Cyber Resilience Act" through **international standardization efforts**.

International standards organizations for cybersecurity

- ISO/IEC JTC 1 SC 27 Information security, cybersecurity and privacy protection
- ISO/IEC TC 307 Blockchain and distributed ledger technologies
- ITU-T SG 17 Security

- **The Korean government provides significant support for international standardization activities.**
  - **International cybersecurity standards have influenced Korean solutions, products, or regulatory frameworks**

SC 27 Structure

Information security, cybersecurity and privacy protection

SC 27 Plenary

Chairmanship
Chair: Andreas WOLF (DIN)
Support: Laura LINDSAY (ANSI)

Secretariat
Committee Manager: Sobhi MAHMOUD (DIN)

CAG
Convenor: Andreas WOLF (DIN)
Support: Laura LINDSAY (ANSI)

JAG IEC/TC 65 - JTC 1/SC 27
Co-Convenor: Ingo WEBER (IEC/TC 65)
Co-Convenor: Andreas WOLF (SC 27)

AHG 1 Resolution Drafting
Convenor: Sobhi Mahmoud (DIN)

WG 1 Information Security Management Systems
Convenor: Edward HUMPHREYS (BSI)
Support: Pablo CORONA (DGN)

WG 2 Cryptography and Security Mechanisms
Convenor: Hirotaka YOSHIDA (JISC)
Support: Takeshi CHIKAZAWA (JISC)

WG 3 Security Evaluation, Testing and Specification
Convenor: Miguel BAÑÓN (UNE)
Support: Naruki KAI (JISC)

WG 4 Security Controls and Services
Convenor: Faud KHAN (SCC)
Support: vacant

WG 5 Identity Management and Privacy Technologies
Convenor: Kai RANNENBERG (DIN)
Support: Jan SCHALLABÖCK (DIN)

JWG 4 Security, privacy and identity for Blockchain and DLT
Co-Convenor: Julien BRINGER (AFNOR) (TC 307)
Co-Convenor: Sal FRANCOMACARO (SC 27)

JWG 7 Cybersecurity testing and evaluation of biometrics
Co-Convenor: Julien BRINGER (AFNOR) (SC 27)
Co-Convenor: Ambika SUMAN (SC 37)

AG 2 Trustworthiness
Convenor: Ricardo VILLALON FONSECA (INTECO)

AG 5 Strategy
Convenor: Jean-Pierre QUEMARD (AFNOR)
Support: Kai CHEN (SAC)

AG 6 Operations
Convenor: Qin QIU (SAC)

AG 7 Communications and Outreach
Convenor: Edward HUMPHREYS (BSI)
Support: Taewan PARK (KATS)

AG 8 Conformity Assessment Advisory Group
Convenor: Edward HUMPHREYS (BSI)

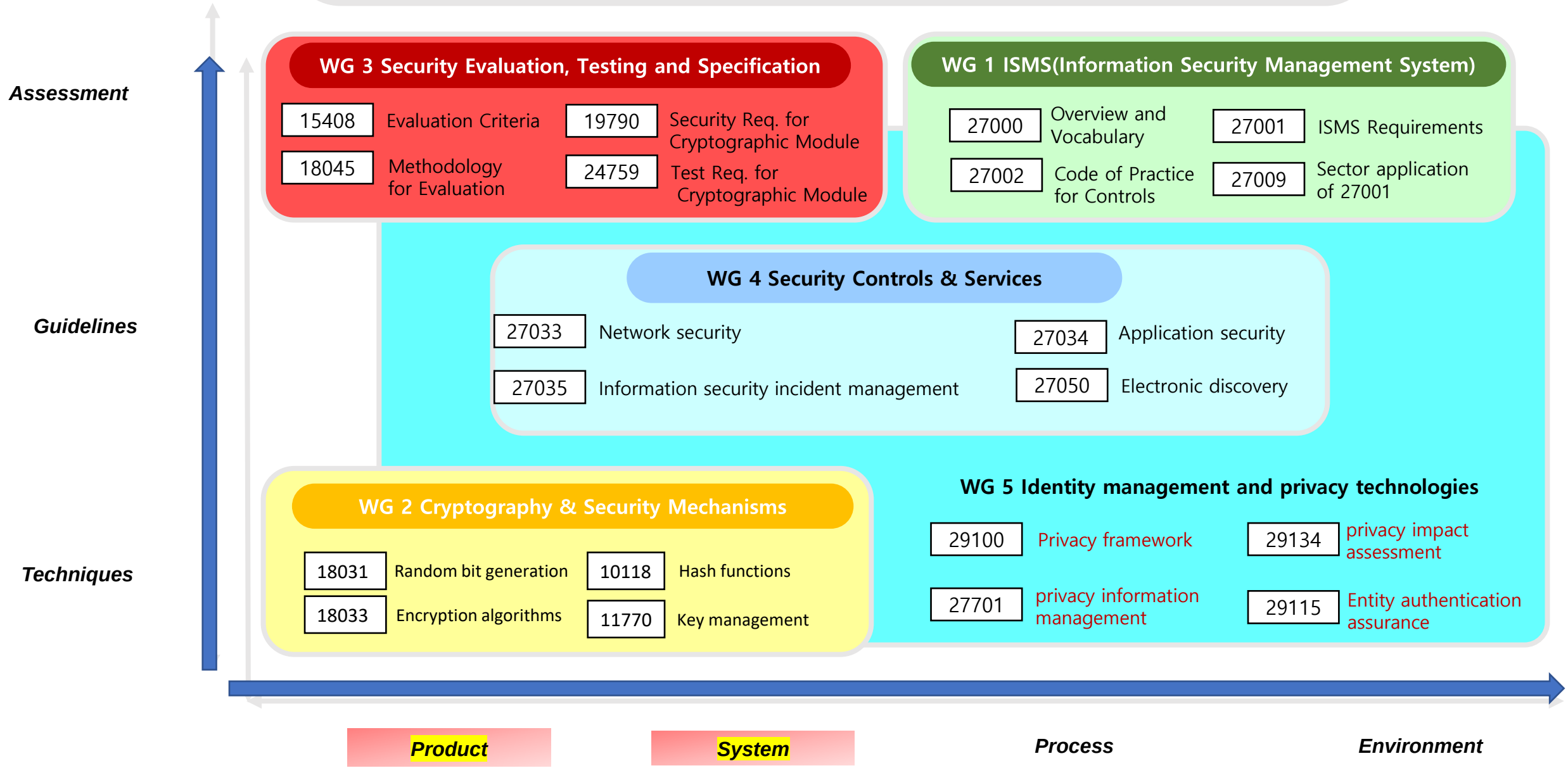
AG 9 Diversity
Convenor: Gargi KEENI (BIS)

AHG 3 Security and privacy in AI and Big Data
Convenor: François LOREK (AFNOR)
Support: Kai CHEN (SAC)

Korea Mirror committee for SC 27

- Supervising Organization
  - KATS (Korean Agency for Technology and Standards
  - RRA (National Radio Research Agency)
- Secretariat Organization
  - TTA (Telecommunications Technology Association)
- It involves experts from government, academia, and industry.
- Korea effectively contributes to international cybersecurity standards while reflecting national security policies and industry needs.

Overview of the SC27 Standards Collection



Overview of SC27 WG1 Standards Collection

Working Group 1: Information Security Management System

Information Security Management System

ISMS Core

- 27000 Overview and Vocaburaly
- 27001 Information Security Management System - Requriements
- 27002 Code of practice for information security controls

ISMS Support

- 27003 ISMS Guidance
- 27004 Monitoring, measurement, analysis and evaluation
- 27005 Information security risk management
- 27014 Governance of information security
- 27016 Organizational economics
- 27021 Competence requirements for ISMS Professionals

ISMS Sector Application

- 27009 Sector specific application of ISO/IEC 27001 Requirements
- 27010 Information security management for inter-sector and inter-organizational communications
- 27011 Code of practice for information security controls based on ISO/IEC 27002 for telecommunications organizations
- 27013 Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
- 27017 Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- 27018 Code of practice for protection of personally identifiable information (PII) in public clouds acting PII processors
- 27019 Information security controls for the energy utilities industry

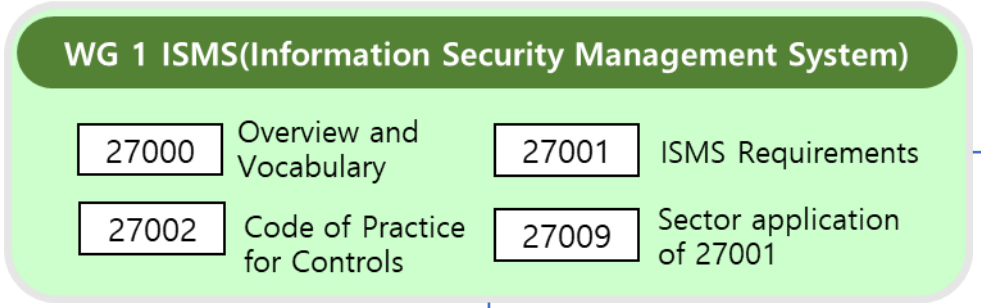
Accreditation/Certification

- 27006 Requirements for bodies providing audit and certification of Information Security Management System
- 27007 Guidelines for Information Security Management Systems Auditing
- 27008 Guidelines for the assessment of information security controls

Cybersecurity

- 27100 Overview and Concepts
- 27101 Cybersecurity framework development guidelines
- 27102 Guidelines for cyber-insurance
- 27103 Cybersecurity and ISO and IEC standards

Specific example of how international cybersecurity standards (ISO/IEC) have influenced Korean solutions, products, or regulatory frameworks



ISO/IEC 27000 family have been **adopted** and are in use in 13 countries

ISO/IEC 27000 family have been **referenced** in Korean Regulation on Certification of Information Security Management System and Personal Information Protection Management System

Korean Expert
Park Taehwan as a co-editor for ISO/IEC 27000 family

Overview of SC27 WG2 Standards Collection

Working Group 2: Cryptography and Security Mechanisms

Cryptographic Primitives

Fundamental cryptography

- 18031 Random bit generation
- 18032 Prime number generation
- 15946 Cryptographic techniques based on elliptic curves
- 11770 Key management
- 10118 Hash functions

Encryption

- 18033 Encryption algorithms
- 10116 Modes of operation

Lightweight cryptography

- 29192 Lightweight cryptography

Cryptographic Mechanisms

authentication

- 9797 Message authentication codes
- 7064 Check character system
- 9798 Entity authentication
- 20009 Anonymous entity authentication

Digital signature

- 14888 Digital signatures with appendix
- 9796 Digital signature schemes giving message recovery
- 18370 Blind digital signature
- 20008 Anonymous digital signatures
- 23264 Redaction of authentic data

Hybrid mechanisms

- 19772 Authenticated encryption
- 29150 Signcryption

Cryptographic Protocols

Cryptographic protocols

- 13888 Non-repudiation
- 19592 Secret sharing
- 18014 Time stamping services and protocol
- 4922 Secure multiparty computation

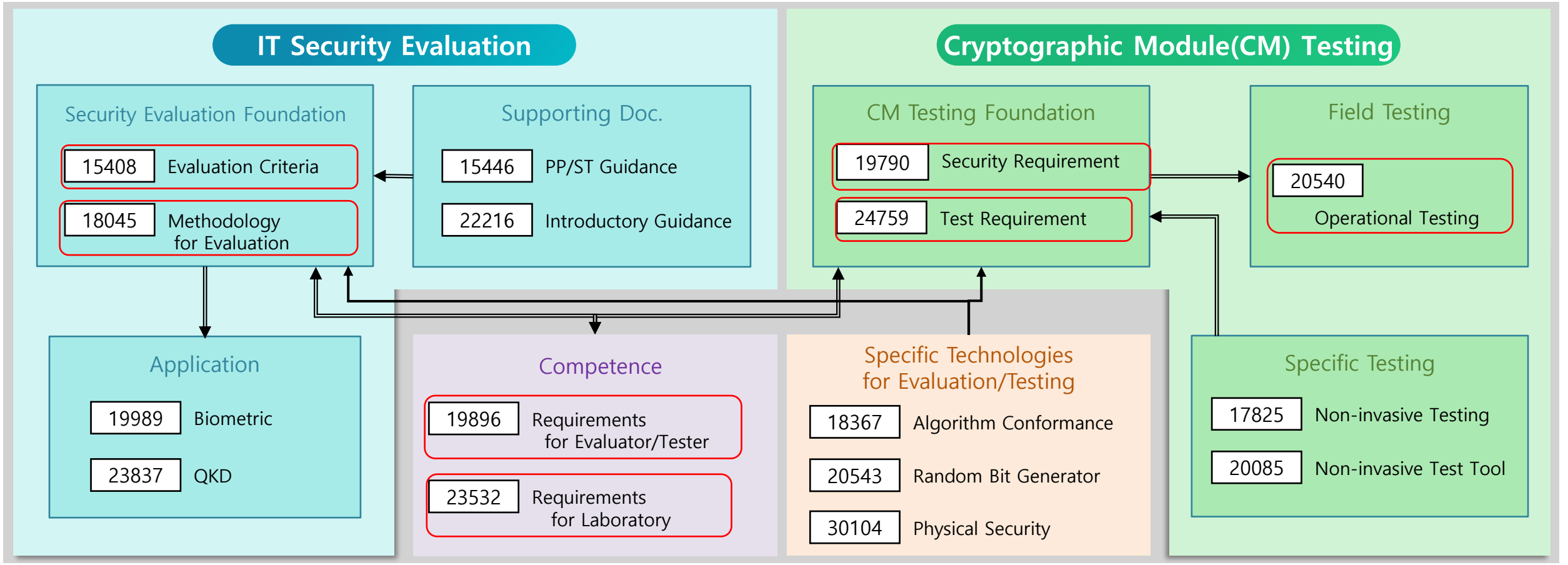
Specific example of how international cybersecurity standards (ISO/IEC) have influenced Korean solutions, products, or regulatory frameworks

Many international standard cryptographic algorithms are approved and used under the KCMVP (Korea Cryptographic Module Validation Program).

Korean Experts
CHO Jihoon as an editor for ISO/IEC 25330-1,2,3 and a co-editor for ISO/IEC 11770-4 and ISO/IEC 25330-1,2,3
SON Yongha as an editor for ISO/IEC 25330-1,2,3 and co-editor for ISO/IEC 25330-1,2,3
ROH Dongyoung as an editor for ISO/IEC ISO/IEC 9797-2/COR1
KWON Daesung as a co-editor for ISO/IEC ISO/IEC 9797-2/COR1

Overview of the SC27 WG3 Standards Collection

Working Group 3: Security Evaluation, Testing and Specification



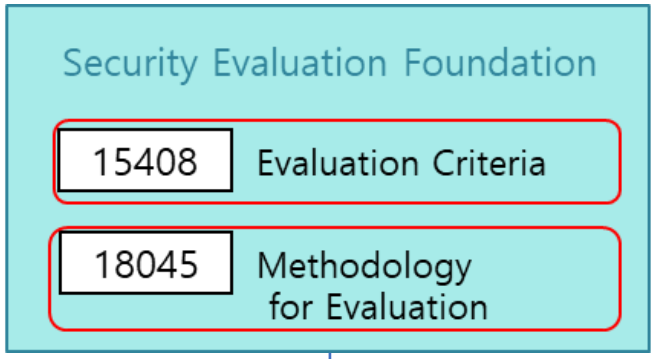
Assurance and Process for General System

- 30111 Vul. Disclose
- 29147 Vul. Handling
- 15443 IT Security Assurance
- 19791 Operational System
- 21827 SSE-CMM
- 19249 Secure System Design
- 19792 Biometric Security

Specific Technologies

- 24485 WBC
- 20897 PUF
- 29128 Crypto Protocol Verification
- 19608 Privacy Security
- 20004 S/W Vulnerability

Specific example of how international cybersecurity standards (ISO/IEC) have influenced Korean solutions, products, or regulatory frameworks



- The **IT Security Certification Center (ITSCC)** is an organization responsible for the **evaluation and certification of IT security products** under **article 58 of the Intelligent Informatization Basic Act** from Korea

- **EU-CC (European Common Criteria)** is a **cybersecurity certification scheme** introduced by the **European Union (EU)** as part of the **EU Cybersecurity Act**.
- It aims to establish a **unified, EU-wide Common Criteria (CC) certification framework** for **IT security products**, ensuring higher security assurance and mutual recognition across EU member states.

Korean Expert
Choi Heebong as an editor for 15408-5
Lee Kwangwoo as an editor for 15408-2 and co-editor for 18045

ISO/IEC 15408 Part 1: Introduction and general model

- This document establishes the general concepts and principles of IT security evaluation and specifies the general model of evaluation given by various parts of the standard which in its entirety is meant to be used as the basis for evaluation of security properties of IT products.
- This document provides an overview of all parts of the ISO/IEC 15408 series.
- It describes the various parts of the ISO/IEC 15408 series;
  - defines the terms and abbreviations to be used in all parts of the standard;
  - establishes the core concept of a Target of Evaluation (TOE);
  - describes the evaluation context and describes the audience to which the evaluation criteria is addressed.
- An introduction to the basic security concepts necessary for evaluation of IT products is given.

ISO/IEC 15408 Part 2: Security functional components

- This document defines the required structure and content of security functional components for the purpose of security evaluation.
- It includes a catalogue of functional components that meets the common security functionality requirements of many IT products.

ISO/IEC 15408 Part 3: Security assurance components

- This document defines the assurance requirements of the ISO/IEC 15408 series.
- It includes the individual assurance components from which the evaluation assurance levels and other packages contained in ISO/IEC 15408-5 are composed, and the criteria for evaluation of Protection Profiles (PPs), PP-Configurations, PP-Modules, and Security Targets (STs).

ISO/IEC 15408 Part 4: Framework for the specification of evaluation methods and activities

- This document provides a standardized framework for specifying objective, repeatable and reproducible evaluation methods and evaluation activities.
- This document does not specify how to evaluate, adopt, or maintain evaluation methods and evaluation activities.
- These aspects are a matter for those originating the evaluation methods and evaluation activities in their particular area of interest.

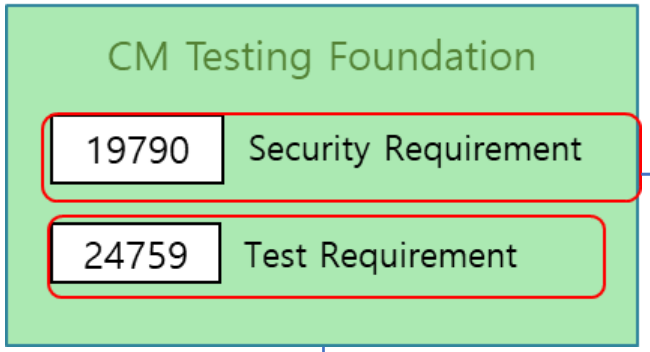
ISO/IEC 15408 Part 5: Pre-defined packages of security requirements

- This document provides packages of security assurance and security functional requirements that have been identified as useful in support of common usage by stakeholders.

ISO/IEC 18045 Evaluation criteria for IT security — Methodology for IT security evaluation

- This document defines the minimum actions to be performed by an evaluator in order to conduct an ISO/IEC 15408 series evaluation, using the criteria and evaluation evidence defined in the ISO/IEC 15408 series.
- This document defines the minimum actions to be performed by an evaluator in order to conduct an ISO/IEC 15408 series evaluation, using the criteria and evaluation evidence defined in the ISO/IEC 15408 series.

Specific example of how international cybersecurity standards (ISO/IEC) have influenced Korean solutions, products, or regulatory frameworks



KCMVP (Korea Cryptographic Module Validation Program) is a validation program that validates cryptographic modules **introduced** in national public departments based on **Article 9 of the Cybersecurity Operational Regulations** and **Article 69 of the Enforcement Decree of the Electronic Government Act under** ISO/IEC 19790 and ISO/IEC 24759.

US, Canada and Japan are operating CMVP and JCMVP under ISO/IEC 19790 and ISO/IEC 24759

Korean Expert
Choi Heebong as an editor for ISO/IEC 24759 and co-editor for ISO/IEC 19790.
This both document were published in February, 2025

ISO/IEC 19790 Security requirements for cryptographic modules

- This document specifies the security requirements for a cryptographic module utilized within a security system protecting sensitive information in Information and Communication Technologies (ICT).
- It defines four security levels for cryptographic modules to provide for a wide spectrum of data sensitivity and a diversity of application environments.
- This document specifies up to four security levels for each of the 11 requirement areas with each security level increasing security over the preceding level.

ISO/IEC 24759 Test requirements for cryptographic modules

- This document specifies the methods to be used by testing laboratories to test whether the cryptographic module conforms to the requirements specified in ISO/IEC 19790:2025.
- The methods are developed to provide a high degree of objectivity during the testing process and to ensure consistency across the testing laboratories.
- This document also specifies the information that vendors are required to provide testing laboratories as supporting evidence to demonstrate their cryptographic modules' conformity to the requirements specified in ISO/IEC 19790:2025.
- Vendors can also use this document to verify whether their cryptographic modules satisfy the requirements specified in ISO/IEC 19790:2025 before applying to a testing laboratory for testing.

Other standards in WG 3

- Other standards in which Korean experts are actively participating as a co-editor include:
  - ISO/IEC TR Transition Guide for ISO/IEC 19790 and ISO/IEC 24759
  - New concepts and changes in ISO/IEC 15408:2022 and ISO/IEC 18045:2022
  - PWI Revision of ISO/IEC Cryptographic algorithms and security mechanisms conformance testing (18367)
  - ISO/IEC 19896-1, 2 Requirements for the competence of IT security conformance assessment body personnel
  - ISO/IEC NP Application of attack potential to deep learning-based technology (WG3 N2873)
  - ISO/IEC NP Enhancing the ISO/IEC 15408 series and ISO/IEC 18045 for the Evaluation of Artificial Intelligence (AI) Functionality (WG3 N2895)
  - ISO/IEC PWI Evaluation of AI-based Technology

Overview of SC27 WG4 Standards Collection

Working Group 4: Security controls and services

Internet security

Cyber security

- 27032 — Guidelines for cybersecurity
- 24392 — Security reference model for Industrial Internet Platform (IIP)

Big data & privacy

- 27045 — Processes
- 27046 — Implementation guidelines
- 20547 — Security and privacy

IoT security Privacy

- 27030 — Guidelines for security and privacy in Internet of Things (IoT)
- 24391 — Guidelines for IoT-domotics

Incident management

- 27035-1 — Principles of incident management
- 27035-2 — Plan and Prepare
- 27035-3 — incident response operations

Network & System security

Network

- 27033 — Network security overview and concepts, threats, design techniques and control, etc.
- 27039 — Selection, deployment and operation of intrusion detection and prevention systems (IDPS)

System

- 15945 — Specification of TTP services to support the application of digital signatures
- 27071 — Security recommendations for establishing trusted connection between device and service

Forensic

- 27037 — Guidelines for identification, collection, acquisition and preservation of digital evidence
- 27041 — Guidance on assuring suitability and adequacy of incident investigative method

Storage security

- 27040 — Storage security

Service and Application security

Cloud

- 19086 — Service level agreement (SLA) framework
- 21878 — Security guidelines for design and implementation of virtualized servers

Application

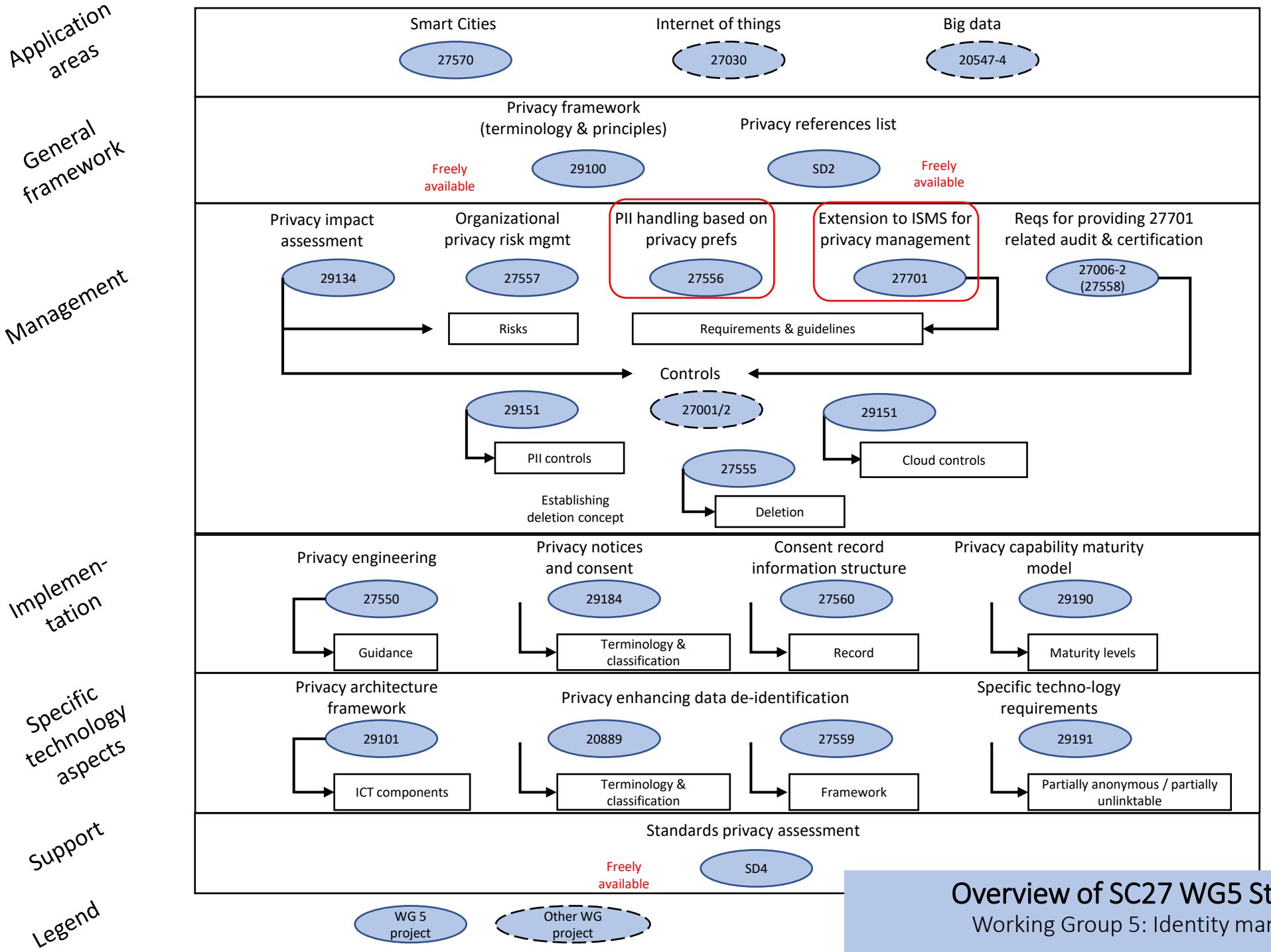
- 27034 — Application security management process, validation, security control data structure, Case studies
- 15816 — Security information objects for access control

Electric discovery

- 27050-1 — Overview and concepts
- 27050-2 — Guidance for governance and management of electronic discovery
- 27050-3 — Code of practice for electronic discovery

PKI

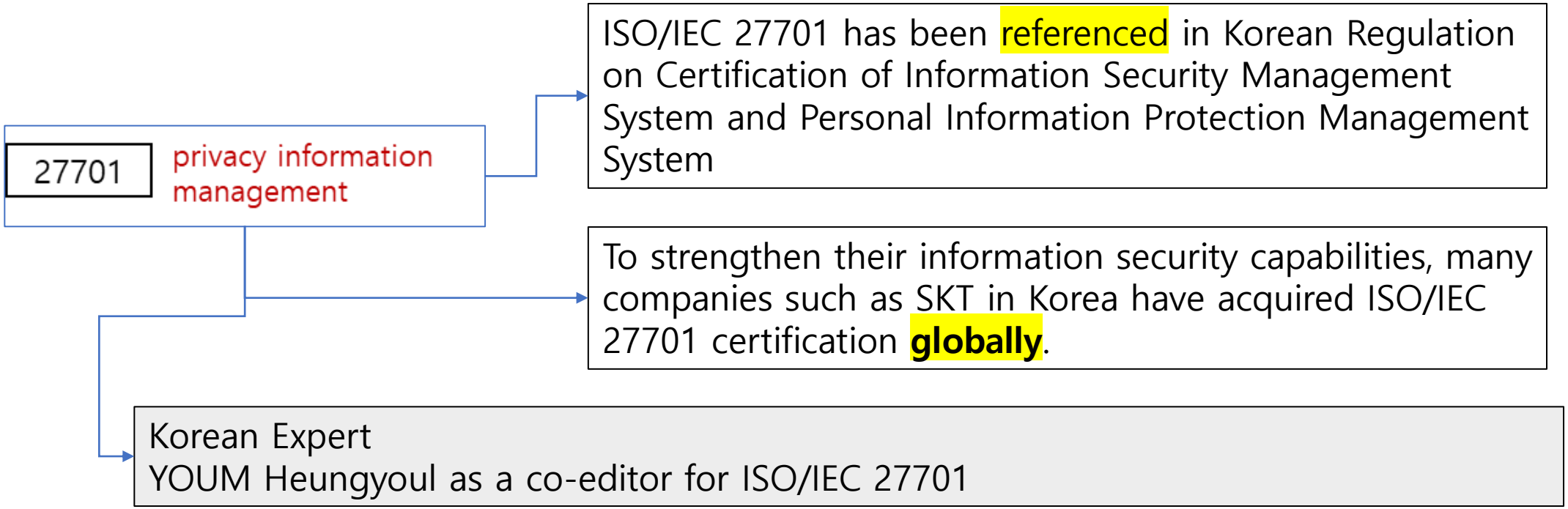
- 27099 — Practices and policy framework



Overview of SC27 WG5 Standards Collection

Working Group 5: Identity management and privacy

Specific example of how international cybersecurity standards (ISO/IEC) have influenced Korean solutions, products, or regulatory frameworks



ISO/IEC 27701 Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines

- This document specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS) in the form of an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management within the context of the organization.
- This document specifies PIMS-related requirements and provides guidance for PII controllers and PII processors holding responsibility and accountability for PII processing.
- This document is applicable to all types and sizes of organizations, including public and private companies, government entities and not-for-profit organizations, which are PII controllers and/or PII processors processing PII within an ISMS.

Other standards in WG 5

- Other standards in which Korean experts are actively participating as an editor and a co-editor include:
  - ISO/IEC PWI Exploration of digital wallets storing digital credentials
  - ISO/IEC PWI 27575 Privacy for metaverse frameworks
  - ISO/IEC 27091 Artificial intelligence – Privacy protection
  - ISO/IEC 27568 Security and Privacy of Digital Twins
  - ISO/IEC 27573 NP privacy protection of user avatar system avatar interactions in the metaverses
  - ISO/IEC 29151 Code of practice for personally identifiable information protection
  - ISO/IEC 27562 Privacy guidelines for fintech services

ISO/IEC TC 307_Structure

Blockchain and distributed ledger technologies

TC 307 Plenary

- The main decision-making body, where national member bodies participate.
- Oversees and coordinates the work of WGs, JWGs, and AGs.

Working Groups

- ~~**WG 1: Foundations** – Defines fundamental concepts, terminology, and architecture~~.
- ~~**WG 2: Security, Privacy, and Identity** – Works on security aspects, cryptographic techniques, privacy mechanisms, and identity management in blockchain~~.
- **WG 3: Smart Contracts and Their Applications** – Develops standards for smart contract frameworks, execution, and verification.
- **WG 5: Governance** – Addresses governance models for blockchain and DLT.
- **WG 6: Use Cases** – Gathers and standardizes use cases across different industries.
- **WG 7: Interoperability** – Ensures compatibility between different blockchain systems.
- **WG 8: Tokenization of assets** systems.

Advisory Groups (AGs)

- **AG on Strategy** – Defines the long-term roadmap and vision for blockchain standardization.

Korea Mirror committee for TC 307

- Supervising Organization
  - KATS (Korean Agency for Technology and Standards)
- Secretariat Organization
  - TTA (Telecommunications Technology Association)
- It involves experts from government, academia, and industry.
- It coordinates Korea’s participation in blockchain and distributed ledger technology (DLT) standardization under ISO/IEC TC 307

Standards in which Koreans are actively participating as an editor and a co-editor

WG	No.	Title	Stage	
WG5	ISO TS 23353	Blockchain and distributed ledger technologies — Auditing guidelines	WD	Yoo Sally Soonduck (editor)
JWG 1	ISO 24876	Blockchain and distributed ledger technologies — Privacy protection when involving trust anchors in DLT-based identity management	WD	Lee Jong-Hyouk (editor)
JWG 1	ISO 25126	Information security controls based on ISO/IEC 27002 for distributed ledger services	WD	Oh Kyeong Hee (editor)
JWG 4	ISO 24875	Secure smart contracts	PWI	Choi Dong Bin (co-editor)
WG 8	ISO 20435	A framework for representing physical assets using tokens	CD	Park Young Bom (co-editor))

ITU-T SG 17

Security

WP1/17: Security strategy and coordination
- **Q1/17:** Security standardization strategy and coordination.
- **Q15/17:** Security for/by emerging technologies including quantum-based security.

WP2/17: 5G, IoT and ITS security
- **Q2/17:** Security architecture and network security.
- **Q6/17:** Security for telecommunication services and Internet of Things (IoT).
- **Q13/17:** Intelligent transport system (ITS) security

WP3/17: Cybersecurity and management
- **Q3/17:** Telecommunication information security management and security services.
- **Q4/17:** Cybersecurity and countering spam.

WP4/17: Service and application security
- **Q7/17 :** Secure application services.
- **Q8/17:** Cloud computing and big data infrastructure security.
- **Q14/17:** Distributed ledger technology (DLT) security

WP5/17: Fundamental security technologies
- **Q10/17 :** Identity management and telebiometrics architecture and mechanisms.
- **Q8/17:** Cloud computing and big data infrastructure security.
- **Q11/17:** Generic technologies (such as Directory, PKI, formal languages, object identifiers) to support secure applications

Korea Mirror committee for SG 17

- Supervising Organization
  - MSIT (Ministry of Science and ICT)
- Secretariat Organization
  - TTA (Telecommunications Technology Association)
- It involves experts from government, academia, and industry.
- It serves as a vital link between Korea’s cybersecurity policies and international standardization efforts.
- By actively participating in ITU-T SG 17, Korea contributes to the global cybersecurity landscape while ensuring alignment with domestic regulations and industry needs.

Standards in which Koreans are actively participating as an editor and a co-editor

- Korean experts are actively working as editors or co-editors in more than 40 standardization projects across almost all Questions.
  - Areas: Privacy and Data Protection, Cryptographic Techniques & Quantum Security, Blockchain & Distributed Ledger Technology, Security Threats & Vulnerabilities, IoT and 5G/6G Security, AI & Machine Learning Security, Metaverse security
  - Key editors from Korea: Jae Hoon NAH, Oh Kyeong Hee, Heebong Choi, Jonghyun Baek, Hyungsoo KIM, Jongyoul Park, Changhun Jung, Migyeong Kim, Young Joo Lee, Jonghyun Woo, and about 40 others

What are the main challenges in aligning cybersecurity regulatory efforts between Korea and the EU?

- Differences in Legal and Regulatory Frameworks
  - Korea's cybersecurity regulations are driven by national priorities.
  - The EU’s CRA reflects a broader, union-wide regulatory approach emphasizing cross-border cooperation
  - **Challenge**: Harmonizing national regulatory philosophies.
- Standardization and Technical Alignment
  - While Korea and EU reference international standards (like ISO/IEC 27001), the implementation may vary.
  - **Challenge**: Collaborating on international standards in order to coordinate the adoption of standards and compliance mechanisms
  - Examples of new areas of cooperation in cybersecurity international standards
    - Security, privacy and test method for AI-system
    - Security, privacy and test method in the metaverse

Thank you very much!

Q/A

IDnow. INSTAR

Europe’s impact on global cybersecurity and eID standards

INSTAR workshop
March 25, 2025

Sebastian Elfors

Senior architect and CSO

Agenda.

1 EU-US TTC Digital Identity Mapping.

2 EU interoperability with 3rd countries.

3 eIDAS interoperability with Ukraine.

EU-US TTC Digital Identity Mapping.

Cooperation between the US NIST and EU DG-CNCT.

Comparison of digital identity standards.

EU-US Trade and Technology Council (TTC).

Cooperation between US NIST and EU Commission DG-CNCT.

Comparison of US NIST SP 800-63 with eIDAS eID schemes.

Analysis at three levels:

- Concepts used in each framework
- Mapping of different levels of assurance of digital identities systems
- Listing of international standards referenced

Result: Digital Identity Mapping Excercise Table.

Extracts of the EU-US TTC tables.

Concept No match Partial match Identical match	NIST Definitions (SP 800-63-3)	EU No 910/2014 Definitions
Authentication	**Authentication:** verifying the identity of a user, process, or device, often as a prerequisite to allowing access to a system's resources.	**Authentication:** electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed.
Authoritative source	**Authoritative source:** an entity that has access to, or verified copies of, accurate information from an issuing source such that a CSP can confirm the validity of the identity evidence supplied by an applicant during identity proofing. An issuing source may also be an authoritative source. Often, authoritative sources are determined by a policy decision of the agency or CSP before they can be used in the identity proofing validation phase.	**Authoritative source:** any source irrespective of its form that can be relied upon to provide accurate data, information and/or evidence that can be used to prove identity.
Authentication factor	**Authentication factor:** the three types of authentication factors are something you know, something you have, and something you are. Every authenticator has one or more authentication factors.	**Authentication factor:** a factor confirmed as being bound to a person, which can be possession-based (something the person owns), knowledge-based (something the person knows) or inherent (something based on a physical attribute).
Identity	**Identity:** an attribute or set of attributes that uniquely describe a subject within a given context.	**Person identification data:** a set of data enabling the identity of a natural or legal person, or a natural person representing a legal person, to be established.
Person identification data	**Personally identifiable information:** information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.	
Signature	**Digital signature:** an asymmetric key operation where the private key is used to digitally sign data and the public key is used to verify the signature. Digital signatures provide authenticity protection, integrity protection, and non-repudiation, but not confidentiality protection.	**Electronic signature:** data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign.
Relying party	**Relying party:** an entity that relies upon the subscriber's authenticator(s) and credentials or a verifier's assertion of a claimant's identity, typically to process a transaction or grant access to information or a system.	**Relying party:** natural or legal person that relies upon an electronic identification or a trust service.
Risk management	**Risk management:** the programme and supporting processes to manage information security risk to organisational operations (including mission, functions, image, reputation), organisational assets, individuals, other organisations, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk;	**Information security management system:** a set of processes and procedures designed to manage to acceptable levels risks related to information security.

Source: EU-US TTC Digital Identity Mapping Exercise Report

Conclusions.

The EU eID schemes are legally defined by the eIDAS regulation.

The US digital identity framework is based on policies, i.e. NIST SP 800-63.

There are several similarities between the level of assurance in the EU and the US.

The EU-US TTC report does not cover eIDAS2, which would be of interest since:

- The EUDI Wallet has a (bigger) potential for cross-border interoperability
- ISO 18013-5 mobile driving license (mDL) is a global standard
- ICAO Digital Travel Credentials (DTC) can be used for international travelling

EU interoperability with 3rd countries.

How to integrate eIDAS trusted lists with 3rd countries.

Recognition of Qualified Electronic Signatures.

eIDAS article 14.

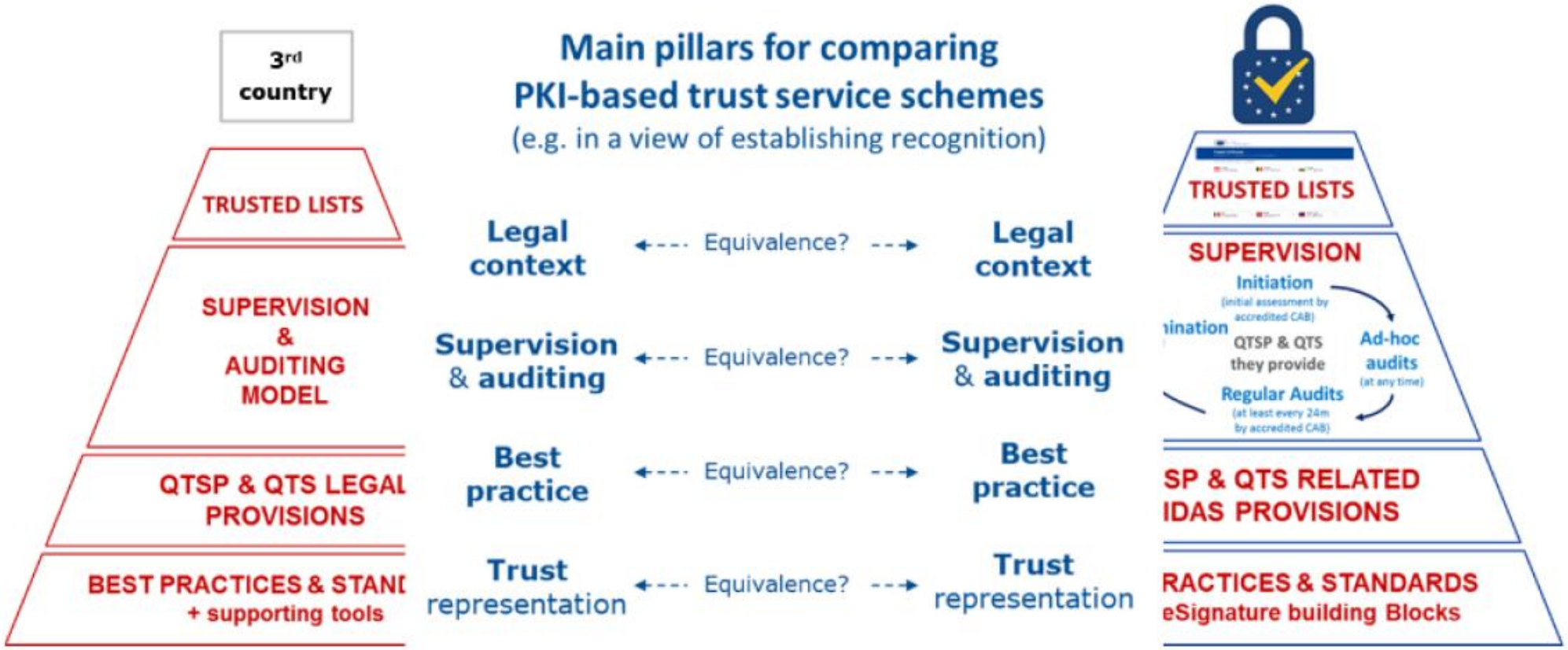
Recognition of 3rd country TSP as legally equivalent to EU QTSP.

Mutual Recognition Agreement (MRA) between the EU and the 3rd country in accordance with TFEU Article 218.

Compliance assessment of 3rd country:

- Legal framework
- Supervisory framework
- Technical standards and best practices
- Trusted list representation of TSP/TS approval

Main pillars for comparing trust services.



Source: DIGITAL eSignature - [The EU Commission's actions on international compatibility of trust services]

EU cooperation with Ukraine.

eIDAS2 interoperability projects.

Cooperation with Qualified Electronic Signatures and the EUDI Wallet.

UA-QES and UA eIDAS-Node.

Formal request received from the **Ukrainian Government** to:

- Recognize UA-QES as eIDAS AdES
- Allow authentication of UA citizens in EU MS services

Technical implementation by EC and UA:

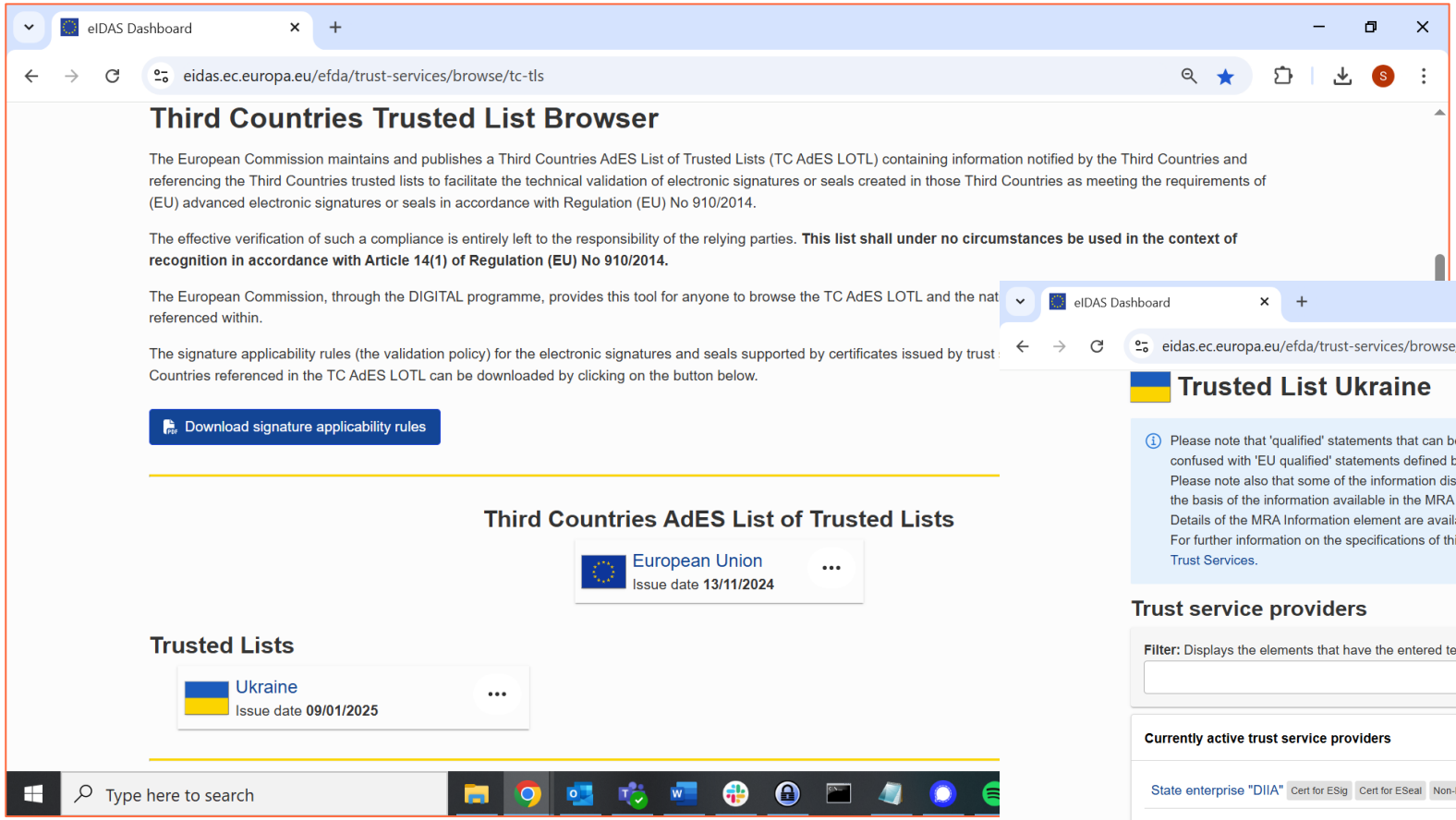
- Publication of AdES LOTL pointing to UA TL
- Update of DSS library to support MRA* elements
- Deployment of UA eIDAS-Node connected to UA IdP
- Prototype of authentication of Ukrainians in EU MS application

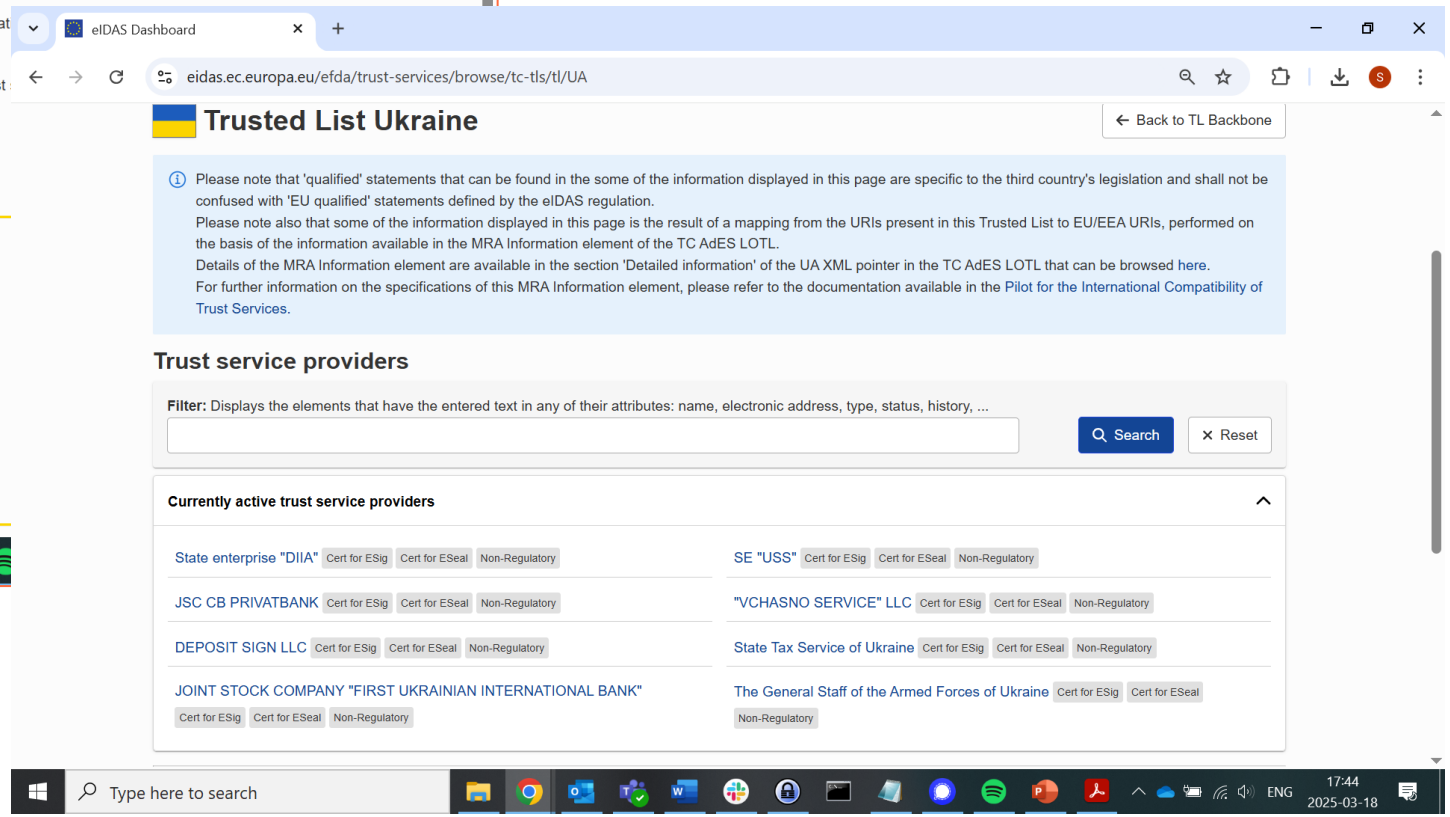
Supported by **eIDAS Art. 27(1)**
To be adopted by MSs on a **voluntary basis**

Source: DIGITAL eSignature - The EU Commission's actions on international compatibility of trust services

COOPERATION WITH UKRAINE

Ukraine on the third countries trusted list.





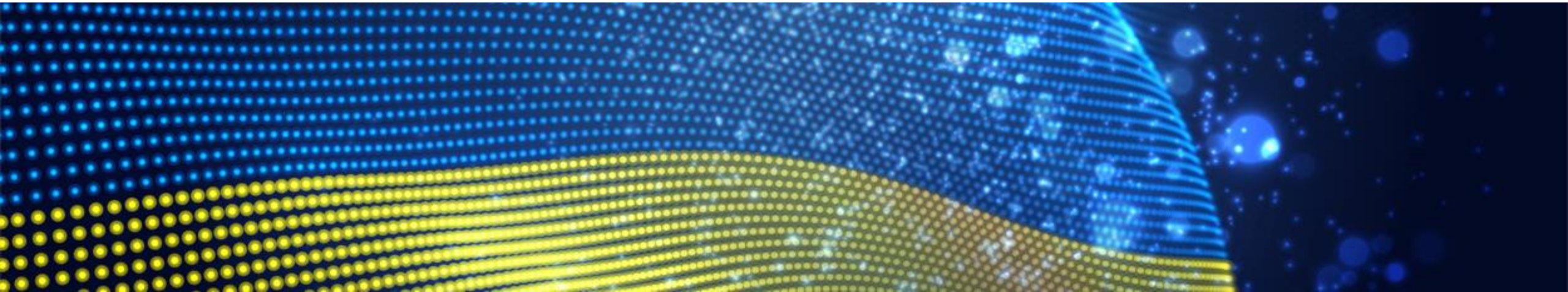
Ukraine is part of EUDI Large Scale Pilot.

Ukraine's Ministry of Digital Transformation is a member of the DT4UA project.

Ukraine has joined the EUDI Large Scale Pilot consortium POTENTIAL.

Shared their experience of the Ukrainian national ‘Diia’ wallet.

The Ukrainian national ‘Diia’ wallet has similar features as the EUDI Wallet.



Thank you!

IDnow.