INSTAR European Cybersecurity/eID Task Force

A Roadmap of the European Cybersecurity/eID Standardisation Work Items

Project Title	International Cooperation for Digital Standardisation
Project Acronym	INSTAR
Grant Agreement No.	101135877
Start Date of Project	01.01.2024
Duration of Project	30.06.2026
Project Website	https://www.instarstandards.org/

Table of contents

1 About INSTAR project

INSTAR is an EU-funded project that aims to shape the future of international ICT standardisation by promoting EU values and interests in key emerging technologies (AI, Cybersecurity, Digital ID, Quantum, IoT, 5G, 6G and data) by collaborating with leading entitles from Australia, Canada, Japan, Singapore, South Korea, Taiwan, USA.

1.1 INSTAR's role in the international ICT standardisation landscape

INSTAR represents a ground breaking effort by the **European Union** to **cement its global leadership** in the formulation and adoption of **international ICT standardisation** across key emerging technologies, ensuring that European perspectives and standards are well-represented and influential in shaping the future of technology.

INSTAR operates across several pivotal technology domains, including **AI**, **Cybersecurity**, **Digital Identity**, **Quantum Computing, IoT, Data** and **5G/6G**. These workstreams represent the forefront of technological innovation and are crucial areas where European leadership and influence in standardisation are vital.

Unlike similar initiatives, **INSTAR stands apart** through its **comprehensive approach** that integrates extensive data on standardisation, thanks to the work of the INSTAR Task Forces and Joint Committees, with **strong individual relationships with key entities from Australia, Canada, Japan, Singapore, South Korea, Taiwan, USA**. This unique combination enables effective knowledge sharing, policy formulation, and the development of harmonised global standards strategies, taking into account the specific nuances of each participating entity.

1.2 Key actions

- Common vision & roadmap with like-minded partners to promote ICT standards in the target foundational technologies internationally.
- Effective stakeholder engagement across existing and new communities.
- Studies and analyses on ICT standardisation in key HE technologies.
- Monitoring the role of standards in digital partnerships and trade agreements.

2 INSTAR Task Forces

The **INSTAR European Task Forces (ETF)** are specialised groups of **standardisation experts**, integrating **technical** and **industry expertise**, dedicated to facilitating **robust knowledge exchange** and **influencing the development of international standards** in line with EU policies.

The **INSTAR International Task Forces (ITF)** differ from the ETFs in their scope and operation. While ETFs focus on direct communication and knowledge exchange, ITFs are geared towards establishing communication channels with the target entities from Australia, Canada, Japan, Singapore, South Korea, Taiwan, USA and the development and implementation of **high-level standard framework roadmaps** for each technology domain, which are crucial for **aligning international standardisation efforts with European strategies and policies** and fostering a **unified vision** and **actionable steps** across different technology domains.

INSTAR's Task Forces bring a **unique value** to the **standardisation landscape** through their focus on **direct person-to-person exchanges** and the development of **comprehensive frameworks** tailored to specific technology sectors (AI, Cybersecurity, Digital ID, Quantum, IoT, 5G/6G and data). This approach ensures effective alignment with common visions and applications, differentiating them from existing standardisation working groups.

2.1 Roadmap

INSTAR convenes leading European stakeholders involved and impacted by the development of standards in key advanced technologies, (e.g. **AI, 5G/6G, internet protocols, IoT and security aspects, cybersecurity, data, eID, quantum or DLTs**) to agree a common European vision and agenda that can then be pursued and agreed with selected international partners, namely Japan, South Korea, Taiwan, Singapore, Australia, Canada, and the USA.

The approach is to engage stakeholders guided by key and experienced ICT standardisation players from within the consortium to manage a set of **technology domain workstreams** to build **high-level standardisation frameworks** (**a roadmap**). INSTAR results map onto a **Standards Dashboard** which will serve as a robust mechanism that expresses the common vision in international fora/SDOs.

3 Methodology

A starting point of the analysis of inputs for the roadmap is the following:

1. Digital partnerships.
2. Annual Union Work Programme for European Standardisation for 2024.
3. Relevant EU legislation with standardisation mandates relevant for this workstream.
4. European Rolling Plan for ICT Standardisation 2024.
5. EU funded research and innovation projects.
6. Relevant SDOs.
7. Priorities identified in the national standardisation roadmaps and feedback from national delegations to the SDOs.

4 About the Cybersecurity/eID

The INSTAR European Cybersecurity/eID is a volunteer group of international experts that provides advisory support to the INSTAR project on the standardisation needs in (workstream). This Task Force focuses on the standardisation activities related to the (workstream) in Europe. It plays a key role in supporting the development of a European Standards Priority List in (workstream), considering the broader trends, regulatory framework and market developments in Europe.

The roadmap developed by this Task Force represents the latest version of ongoing standardisation efforts in (workstream). It will be updated regularly to ensure alignment with insights from international experts and partner countries collaborating with the INSTAR project.

Disclaimer:

This roadmap was prepared by the European Cybersecurity/eID Task Force experts in their personal capacity. The opinions expressed in this roadmap are the experts' own and do not reflect the views of the INSTAR project or its partners. The statements, opinions and data contained in this roadmap and the presentation of materials therein do not imply the expression of any opinion by the INSTAR project or its partners. The views and recommendations in this report are those of the ETF members acting in their personal capacities and do not necessarily represent the opinions of the European Commission or any other body, nor do they commit the Commission to implement them.

5 ETF Cybersecurity/eID Roadmap Inputs

5.1 Digital partnerships

Digital partnerships have proved a vital component in creating unity and connection across the EU and the world. By collaborating with like-minded countries, the EU is able to tackle the digital divide and strengthen its ties beyond Europe. In keeping with the Digital Compass strategy, which aims to make Europe a digitally connected continent by 2030, the EU have committed to building strong partnerships using the four pillars of The Digital Compass- skills, infrastructures, transformation of business and of public services. This ensures the EU and its partners can foster a fair, inclusive and equal digital environment for all.

Identified Actions of Interest:

Partner	Identified Action - Cybersecurity	Identified Action - eID
Canada	27562 (1.27.158) FDIS Privacy guidelines for fintech services. Migration of cryptographic algorithms to quantum resistant cryptography Development of Decentralized Public-Key Infrastructure (DPKI) Alignment on Trusted data and data innovation. Alignment on Filtering foreign information manipulation and disinformation	Challenges of digital identification Safe and secure digital wallet Creation of a "EU Digital Identity Toolbox" and training for its uptake Overview on Digital Wallets and related ISO, IEC, IETF and OpenID Foundation projects 27562 (1.27.158) FDIS Privacy guidelines for fintech services. Alignment on Trusted data and data innovation. Alignment on Filtering foreign information manipulation and disinformation. Alignment on Digital identity data governance and data spaces.
Japan	Cybersecurity of cloud services Cybersecurity of IoT devices Security of the software supply chain Migration of cryptographic algorithms to quantum resistant cryptography. Development of Decentralised Public-Key Infrastructure (DPKI). Possible convergence between Japan's IoT product security conformity assessment policy (currently in draft) and measures adopted under the CRA, specifically in relation to standardisation request M585 and the work underway within CENELEC and the existing work done by Germany and Finland on "IoT cybersecurity labelling scheme". Alignment on the Japan's IoT product security conformity assessment policy (currently in draft) Possible convergence between Japan's IoT product security conformity assessment policy and measures adopted under the CRA, specifically in relation to standardisation request M585 and the work underway within CENELEC Feedback to the CRA provided by the Japan Business Council in Europe. Japan's security labelling scheme "introducing an European labelling scheme, e.g. a BSI IT security label" Harmonisation and promotion of the existing work done by Germany and Finalnd on "IoT cybersecurity labelling scheme" Alignment (Singapore is also working on this) Alignment on massive distributed networks, including a plethora of IoT devices, and powered by 5G/6G technologies.	

	Alignment on Devices at the edge to avoid that tampering them poisons the entire system (e.g. 6G, satellite).	
South Korea	Both sides are expected to explore ways to increase sharing of information on cybersecurity threats and on other areas where exchanges are considered valuable for both sides. Both sides intend to cooperate in capacity building for third countries with the involvement of the private 12 sector. Such cooperation may include signing of a Memorandum of Understanding between MSIT and ENISA. In the field of cybersecurity, the Republic of Korea and the European Union envisage to enhance information sharing on cybersecurity threats and intend to expand information sharing on cybersecurity policy and explore ways to cooperate.	Both sides intend to collaborate on digital identity solutions. Both sides endeavour to work on the basis of use cases and pilot projects towards interoperability of their trust services such as electronic signatures.
Singapore	Migration of cryptographic algorithms Lack of security in communications products Alignment with the Cyber Resilience Act	Alignment with the European Digital Identity Wallet (EUDIW) Frameworks for decentralized digital identity (as in ISO/IEC JTC 1/SC 27/WG 5) Adoption of blockchains and distributed ledger technologies for digital identity management and exchange of attributes (as in ISO/TC 307/JWG 4) Mutual recognition and integration of trust services and trust services list (as developed by ETSI ESI)
US		Digital identity standards report

5.2 Annual Union Work Programme for European Standardisation for 2024

The Annual Union Work Programme on European Standardisation (AUWP) 2024 sets out its priorities on all standards-related activities. The AUWP was informed and advised by the High-Level Forum on European standardisation, a multi-stakeholder group chaired by the Commissioner.

The 2024 AUWP includes 72 actions supporting the EU's policy ambitions towards a green, digital and resilient Single Market. Amongst these, the Commission highlights eight particular actions as policy priorities, including standards for activities on quantum, critical raw materials, the data economy, digital identity, heat pumps, cybersecurity, hydrogen and electric vehicle charging infrastructure.

INSTAR will explore opportunities to introduce reflections from this roadmap into the chapters of the ICT Rolling Plan. This effort would focus on areas relevant to the technologies INSTAR covers, such as cybersecurity. INSTAR may also propose reinforcing these insights during future MSP meetings to align with global perspectives and further contribute to the EU's standardisation strategy.

Identified Actions:

Action	Description
Action 6 Cybersecurity requirements for products with digital elements	Develop European standards and European standardisation deliverables corresponding to essential cybersecurity specifications as set out by the Cyber Resilience Act and notably concerning: (i) security specifications relating to the properties of products with digital elements and vulnerability handling specifications (ii) methodologies concerning assurance levels relating to products with digital elements as referred to above; (iii) evaluation methodologies for evaluating cybersecurity risks associated with products with digital elements. The main objective is to create conditions for developing secure products with digital elements by ensuring that hardware and software products are placed on the market with fewer vulnerabilities and ensure that manufacturers take security seriously throughout a product's life cycle.
Action 8. European Digital Identity framework	Align European and international standards, incorporating a cohesive European Digital Identity Framework. This includes devising technical reports, standards, and guidelines for the EU Digital Identity Wallet and electronic attestations. The goal is to empower citizens with a universally-recognised, secure, and user-friendly digital identity, paving the way for enhanced online transactions and business opportunities while upholding European data protection values.

5.3 Relevant EU legislation with standardisation mandates

Identified mandates:

Regulation	Description
European Digital Identity (EUDI) Regulation	To be published
Radio Equipment Directive	Published as: Regulation (EU) 2024/1183 M/585 Amd 1 – C(2023)5624 COMMISSION IMPLEMENTING DECISION of 23.8.2023 amending Implementing Decision C(2022) 5637 on a standardisation request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation as regards radio equipment in support of Directive 2014/53/EU of the European Parliament and of the Council and Commission Delegated Regulation (EU) 2022/30 M/585 – C(2022)5637 COMMISSION IMPLEMENTING DECISION of 5.8.2022 on a standardisation request to the European Committee for Standardisation and the European

	Committee for Electrotechnical Standardisation as regards radio equipment in support of Directive 2014/53/EU of the European Parliament and of the Council and Commission Delegated Regulation (EU) 2022/30

5.4 European Rolling Plan for ICT Standardisation 2024

Identified Action - Cybersecurity	Identified Action - eID
Action 1: ESOs to develop standards in support of the cybersecurity essential requirements set out in the Cyber Resilience Act. Furthermore, SDOs to develop standards and sectorial specifications for critical infrastructure protection in support of and responding to the requirements in anticipation of the reviewed NIS2 Directive. Foster the application of EN 62443 series (based on IEC 62443 series) by development and implementation of the IEC 62351 series for the firm establishment of EU regulatory requirement operational technology (OT) security including critical infrastructures. **Action 2**: SDOs to assess the content of existing standards and specifications applied under the European Cybersecurity Certification Framework in order to revise existing documents or create new standards. It should be ensured that these standards are gradually and timely made available for providing support to any certification activity, particularly as the preparation and implementation of certification schemes has come under the remit of ENISA on Common Criteria (EUCC), Cloud services (EUCS) and 5G (EU5G). In particular, SDOs are encouraged to develop and harmonise standards related to the specification and assessment of security properties in ICT products and services (including cloud services), as well as those related to security in processes related to the design, development, delivery and maintenance of an ICT product or service, as well as methodologies concerning assurance levels for industry sectors. **Action 3**: SDOs to investigate and prepare harmonised evaluation methodologies of cybersecurity risks, controls and interfaces as required by EU policy instruments such as the Certification Framework of the EU Cybersecurity Act, the Cyber Resilience Act and others for their horizontal application into trusted products such as semiconductors, the European Digital Identity Wallet, and other digital technologies. **Action 4**: SDOs to assess European cybersecurity policies with respect to the upcoming Cyber Resilience Act, but also in relation to other policy instruments, such as the Machinery Directive, the Radio Equipment Directive or to the machine learning component for the AI Act. **Action 5**: SDOs to investigate requirements for secure and interoperable communication protocols for cloud native AI architectures, mobile and fixed networks of distributed devices and services that may in addition rely upon limited resources and interfaces. Requirements and their fulfilment should address relevant mechanisms of authenticating by use of digital signatures, cryptographic key management, encryption, registering, and processing user identities seamlessly across devices, services and applications. **Action 6**: SDOs to assess the availability of standards and technical specifications in general or for business sectors relevant for the requirements relating to cybersecurity risk-management, including those pertaining to supply chain, incident notifications for entities in line with the NIS 2 Directive, or in support of the upcoming Cyber Resilience Act and other potential EU legislation, including as regards certification schemes as defined in the Cybersecurity Act. **Action 7**: SDOs to assess gaps and develop standards on cybersecurity of products in support of possible certification schemes completed under the European Cybersecurity Act and in support of the upcoming Cyber Resilience Act. **Action 8**: SDOs to explore options for the composition and matching of assurance statements as issued under the Certification Framework of the Cybersecurity Act also in conjunction with the provisions of related EU regulatory instruments like the Cyber Resilience Act, the NIS2 Directive or the new eIDAS regulation. **Action 9:** SDOs should foster/establish cooperation with the European Cybersecurity Coordination Centre and national Cybersecurity Centres in order to facilitate the results of current research and outputs from the funding programmes Horizon Europe and Digital Europe. **Action 10**: SDOs to assess gaps and develop standards in support of trust services under the NIS2 Directive and other possible instruments of EU law **Action 11**: ESOs to work with global SDOs and the open source community to identify available or ongoing technologies of relevance for supporting EU regulation, in particular the upcoming EU Cyber Resilience Act.	**Action 1.** Take ongoing EU policy activities into account in standardisation, e.g. in ISO/IEC JTC 1/SC 27/WG 5 (identity management and privacy technologies) and other working groups of ISO/IEC JTC 1/SC 27 and ISO/TC 307/JWG4. Also, the standards being developed by ISO/IEC JTC1 SC17 including on mobile driving licenses and identity management via mobile devices are particularly relevant to electronic identification. Furthermore, in order to promote the strengths of the European approach to electronic identification and trust services at global level and to foster mutual recognition of electronic identification and trust services with non-EU countries, European and international standards should be aligned wherever possible. The promotion and maintenance of related European approaches, which especially take into account data protection considerations, in international standards should be supported. **Action 2:** As required by the framework established under the proposed regulatory framework for European Digital Identities prepare standards for • interfaces between the European Digital Identity Wallet and trust services as well as services for signing by means of electronic signatures and seals • interfaces between the European Digital Identity Wallet and relying parties and issuers of electronic attestations of attributes • Issuance and revocation of wallets and electronic attestation of attributes • security evaluation and certification of the European Digital Identity Wallet • new trust services including electronic attestation of attributes, electronic archiving and electronic ledgers and including update of protocol and security standards and the trusted list format. • Supporting additional requirements for identity proofing and validation of attributes. • Adapting existing standards to take into account new provisions of eIDAS 2.0 including alignment with NIS2 and ensuring that the requirements of privacy by design are met. • Next generation of registered electronic mail and electronic delivery to take account of new services available under eIDAS 2.0 including EU digital identity wallets and electronic ledgers. • Use of electronic identities and electronic signatures with electronic ledgers (e.g. EBSI) in support of smart contracts. • Integration of eIDAS2 into new initiatives, like the Digital Product Passport **Action 3:** SDOs to cooperate and work in the areas of identifiers, vocabularies, semantics, taxonomies, ontologies for electronic attestations **Action 4:** The impact of quantum computing technologies on the cryptographic algorithms, in particular public key cryptography, used for electronic identification and trust services including e-signatures needs to be analysed, and the potential impact on the relevant standards identified. This should lead to guidance on the migration to Quantum Safe Cryptography. **Action 5:** Reconciliation of diverging and incompatible standards (e.g. W3C VCDM, ISO mDL, SD-JWT VC) that pose obstacles to interoperability both within Europe and globally. **Action 6**: Enhance e-ID for mobile platforms by focusing on secure integration of digital ID solutions with mobile devices. **Action 7**: Promote standards for Identity Lifecycle Management to address issuance, renewal, and revocation processes in digital ID systems. **Action 8**: Standardize recovery mechanisms for digital IDs by defining protocols for account recovery and management of compromised digital identities.:

Action12: SDOs to develop standards for threat intelligence sharing by encouraging interoperability and common data models for threat intelligence. **Action 13:** Set standards for ransomware defence strategies by providing guidelines for prevention, response, and recovery from ransomware incidents.	

5.5 EU funded projects standardisation activities

Source		
European Commission		

5.6 Identified ongoing working items in relevant SDOs and alliances

SDO/Alliance	Cybersecurity	eID
CEN-CENELEC	Establishment of a portfolio of quantum resistant algorithms; Guidelines for migration readiness and the migration of cryptographic algorithms to quantum resistant cryptography. Adaption to existing and upcoming threats Radio Equipment Directive (RED) standardisation request: cybersecurity requirements Cyber Resilience Act (CRA) standardisation request: horizontal cybersecurity standards (JTC 13) and selected sector-specific cybersecurity standards (various CEN and CENELEC TCs)	ID wallet Privacy by technical design.
ETSI	Relevant ETSI TC CYBER Technical Report Standards mapping and gap analysis against regulatory expectations New work item proposals submitted to ETSI TC CYBER meeting 39c. The work programme of ETSI CYBER QSC addressing the use of, and migration to, Quantum Safe Cryptography (link to be added). The work programme of ETSI ISG QKD on the role of Quantum Key Distribution in the domain of a quantum ready network. The work programme of ETSI ISG PDL on the role of digital ledgers in a range of applications (see also e-ID).	The work programme of ETSI TC ESI The work programme of ETSI ISG PDL The work programme of ETSI TC HF on age-verification including the role of the Digital Wallet, Selective Disclosure, and trust service providers for age attestation.
ISO-IEC	Revision of authentication and identity assurances concept. Revised standards taking in account global approaches for securing and achieving assurance levels.	Cross-border interoperability of digital identities (tech & LoAs), including ISO NWIP 23042. Mapping of assurances and interfaces for transferring/covering credentials. Inclusiveness in digital identity tools to really take in account user experience and inclusion in eID to ensure they are used properly and globally. SC27 WG5 AHG Digital Wallets
IEEE	Deepfake detection security and trust ; define systems, levels of security and assessment schemes to enable anyone to have confidence on information ; Spread of fake or modified content.	
W3C		Decentralized Identifiers (DIDs) 1.1 DID Resolution 1.0 Verifiable Credentials Data Model 2.0

6 Task Force Recommendations on Standardisation Priorities in the Cybersecurity/eIDdomain

Cybersecurity

- Adopt Quantum-Resistant Cryptography.
- Strengthen Cloud Security.
- Implement Strong Security for IoT Devices.
- Strengthen the Security of Software Supply Chains.
- Introduce a Cybersecurity Labelling Scheme.
- Promote Security-by-Design Principles.
- Promote Cross-Border Cybersecurity Standards Alignment.
- Develop Standards for Vulnerability Handling.
- Ensure IoT Product Security Conformity.
- Develop a Decentralised Public Key Infrastructure (DPKI).
- Develop a standardised cybersecurity framework that aligns with existing regulations like the NIS2 Directive, the EU Cybersecurity Act and DORA.
- Develop Standards for Implementation of Zero-trust Architecture Including defining secure identity and access management practices, multi-factor authentication (MFA), and continuous monitoring standards.
- Address cybersecurity vulnerabilities and attacks on AI/ML systems.
- Promote compliance with EU regulations.

eID

- Promote the European Digital Identity Wallet (EUDIW).
- Ensure Cross-Border Interoperability of Digital ID.
- Develop Decentralised Identity Frameworks.
- Foster Self-Sovereign Identity Systems.
- Align and Recognise Trust Services Across Borders.
- Ensure the Security of Digital Wallets.
- Improve Inclusion in Digital Identity Systems.
- Integrate Privacy by Design in eID Wallets.
- Develop Trust Frameworks for Decentralised Identity.
- Develop Digital ID Interoperability Framework that ensures the interoperability of national e-ID schemes and digital ID wallets across borders.
- Develop Standards for Cross-Sector Identity Integration to enable the use of digital identity across sectors, such as healthcare, finance, education, etc.
- Integrate eIDAS into new initiatives like Digital Product Passport (ESPR Regulation).
- Explore future cryptographic capabilities, e.g. privacy-enhancing ZKP.

7 INSTAR European Cybersecurity/eID Task Force Members

The INSTAR Cybersecurity/eID Task Force leaders are grateful to the many experts for their input and private conversations. In particular, they would like to thank:

Expert	Affiliation	Country
Silvana Muscella- Chair	Trust-IT	Italy
Luigi Colucci- Chair	Trust-IT	Italy
Sara Bozzi - Chair	Trust-IT	Italy
Christoph Schmittner	Austrian Institute of Technology	Austria
Erwin Schoitsch	Austrian Institute of Technology	Austria
Erik Andersen	Andersen's L-Service	Denmark
Rob Brennan	University College Dublin	Ireland
Julien Bringer	Kallistech	France
Scott Cadzow	Cadzow Communications Consulting Ltd	United Kingdom
Paolo Campegiani	Namirial	Italy
Tasos Dagiuklas	London South Bank University	United Kingdom
Muslim Elkotob	Vodafone	Germany
Fotios Giannakopoulos	Bavarian Consultants	United Kingdom
Rusnė Juozapaitiene	ANEC	Lithuania
Pankaj Pandey	Norwegian University of Science and Technology	Norway
Octavian Popescu	EUCOMREG	Belgium
Paweł Rybicki	Homeland Security Institute- EFIC	Poland
Markus Sabadello	Danube Tech GmbH	Austria
Raul Sanchez-Reillo	Universidad Carlos III de Madrid	Spain
Antoine Sciberras	University of Malta	Malta
Walter Fumy	Bundesdruckerei-Gruppe	Germany