INPACE
EU-India Digital
Cooperation Conference 2026
New Delhi

Session on session “Digital Trust”

Title: “Digital Trust (CRA) – EU status update and Role of Standards & Collaboration”

Speaker: Mr. Dinesh Chand Sharma

Director – Standards & Public Policy (SESEI)



INPACE
Funded by the European Union
Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

©INPACE 2024-2027

SESEI: Local Representative of EU Standardisation Bodies in India

SESEI (**S**econded **E**uropean **S**tandardization **E**xpert in **I**ndia) ***is a local face for the European standardization community in India: Dinesh Chand Sharma***

Launched in Jan'13, currently in its sixth phase (Aug'24 to July'27)

Priority Sectors/topics: Aligned with EU-INDIA TTC & Connectivity Partnership

Digitization: Strategic technologies, digital governance, and digital connectivity

- Smart Cities, ITS, Quantum Technologies, Smart Grid/Meter, AI, 5G/6G, Open RAN, M2M/IoT, DECT, Data Privacy, Satellite Communication, Blockchain, Digital Signature, Smart Manufacturing, e-Accessibility, cybersecurity, digital skills and R&I etc.

Green & Clean Technologies:

- Clean Energy, Energy Efficiency (Green ICT), Environment, Circular Economy including Resource Efficiency, Waste Management, Energy storage technologies, **Electric mobility**, Green Hydrogen, Advanced biofuels including R&I etc.

Market access & Other topics of mutual interests:

- Rail, Ropeways, Machinery Safety etc.

www.sesei.eu , www.sesei.in , Monthly Newsletter Subscribe – Europe & India, 5th Indo European Conference on 15th-16th Feb'27 in New Delhi

© INPACE 2024-2027

SESEI: Achievements 1(2)

- Permanent presence of Project SESEI expert in India since 2013 has provided considerable insight, access, alignment of Indian standardisation programmes and related strategies i.e. roadmaps and priorities.

Local presence:

- ✓ Database of 3000+ contacts: all partners can leverage to engage with stakeholders in India, either directly or with support of the SESEI expert.
- ✓ Contact with Ministries & admins and other CC and/or embassies
- ✓ Picks up queries from EU/Indian Industry/Legislators around Legislation, Standards and extended local support in pursuing Market Access Issues (Quality Control Orders)

Structural cooperation:

- ✓ MoU between BIS -CEN-CENELEC: Framework Copyright Agreement ongoing, Cooperation agreement between BIS – ETSI (Copyright Provisions Included)
- ✓ MoU between ISGF-CENELEC , BIF-ETSI , COAI-ETSI etc.
- ✓ BIS officials visited EU/EFTA as part of the study cum training visit organized by SESEI.

Information flow (both ways):

- ✓ Monthly Newsletter for both EU/EFTA and Indian stakeholders
- ✓ Industry Sector Profile Report on Digitalization and Green & Clean Technologies: India
- ✓ Reports on European Standardisation Initiatives: on the request of IN govt bodies
- ✓ Thematic Webinars & Workshops (Consumer IoT Security and Circular Economy and Eco Design, Eco Labelling, etc)
- ✓ Published articles on key emerging topics covering AI, Consumer IoT, EU-India collaboration etc.

INPACE
Funded by the European Union
Project funded by

SESEI: Achievements 2(2)

- Presence and involvement of SESEI expert in relevant associations, WGs in India is an invaluable asset to raise awareness of Europe's vision and approach to key challenges, Europe's standards, and best practices.
  - Member of many TC's /WG's of BIS, TEC, TSDSI , Niti Aayog, Trade/Tech Associations, and active participations in various forums has led to Considerable Impact on Indian regulatory and Standardisation system.

- **Resulted in Adoption of EN's by Indian SDO's** :
  - Adoption of EN-115 standards as Indian Standard: BIS
  - Adoption of EN 301 549 (Accessibility requirements suitable for public procurement of ICT products and services): BIS
  - Adoption of E/Digital – Signatures: plans to adopt entire ETSI library
    - Total = 76 , Published = 5, Under Publication = 4, Preliminary Draft Stage = 3, Next Transposition: 3
  - TSDSI transposition of 3GPP for IMT-Advanced/4G/5G specifications adopted as National Standards by TEC: Indian 5Gi is aligned with 3GPP Specifications.
  - Adoption of OneM2M Release 2 and Release 3 Specifications as national Standards in India
    - BIS Standard on Smart Infrastructure has IoT reference Architecture standards and is based on oneM2M Reference Architecture, Other Indian standard also includes ETSI NGSI-LD as well.
  - Adoption of EN 303 645 - cyber security standard for consumer IoT devices: TEC Code of Practice
  - Standard for "Energy Consumption Rating and Energy Passport" for Telecommunications at TEC are based on ETSI Standards
    - EN 303 215, EN 202 706-1, EN 102 706-2, EN 303 470, ES 201 554 etc.
  - TSDSI adoption of ETSI Standards on NFV and IoT (Security).

- **Indo European Conference on Standards & Emerging Technologies**: a strong platform established by SESEI for effective and continuous dialogue between India and EU/EFTA to identify the key areas of collaboration: 4th Edition of the Conference was held on 7th December 2023 => The next (5th) edition of the Conference is to be held on 15-16 February 2027 in New Delhi=> AI, DPP, Digital Wallet, Digital trust and signature

INPACE
Funded by the European Union
Project funded by

EU/EFTA - India Relations

- At G20 held in India, creation of the India-Middle East-Europe- Economic Corridor was launched: Sep'23
  - EU-India Connectivity Partnership aligned with EU's Global Gateway
- **Trade Technology Council (TTC)** set up in February 2023
  - **Strategic Technologies** : Quantum and High-performance Computing, Trustworthy Artificial Intelligence, Semiconductor sector, Digital skills, 5G , IoT and enhance interoperability of respective digital public infrastructure.
  - **Green & Clean Energy Technologies**: Waste-water management, Recycling of Batteries for Electrical Vehicles, Standards in the Research Domain (Waste to Green Hydrogen, Marine Plastic Litter and Wastewater, E-Mobility – Circularity aspects of batteries & interoperability of Charging Infrastructure)
  - **Trade Investment and Resilient Value Chains**: Resilient Value Chains, resolve bilateral market access issues, exchange information on mechanism for FDI screening, address global and multilateral trade issues
- **New Strategic EU-India Agenda towards 2030**
- Building on the EU's Joint Communication in 2025 'New Strategic EU-India Agenda', Cooperation on research and innovation is a cross-cutting and integral part of Joint EU-India Comprehensive Strategic Agenda Towards 2030, adopted on 27 January 2026 at 16th EU-India Summit
  - Agenda will strengthen the cooperation on sustainability, technology and innovation, security and defence, connectivity, global issues, and people-to-people cooperation.
  - During the summit, India and European Commission have signed and exchanged an **Administrative Arrangement on Advanced Electronic Signatures and Seals.**
- India and European Union concluded negotiations for a comprehensive **Free Trade Agreement (FTA)** on January 27, 2026
  - Expected by early 2027, FTA will reduce or eliminate tariffs on 99.5% of EU tariff lines and 92.1% of India's, covering 97.5% of trade value.
- India-EFTA trade talks > Trade and Economic Partnership Agreement (TEPA) signed in March 2024, operational from 1st Oct'25

INPACE
Funded by the European Union
Project funded by

Digital Trust

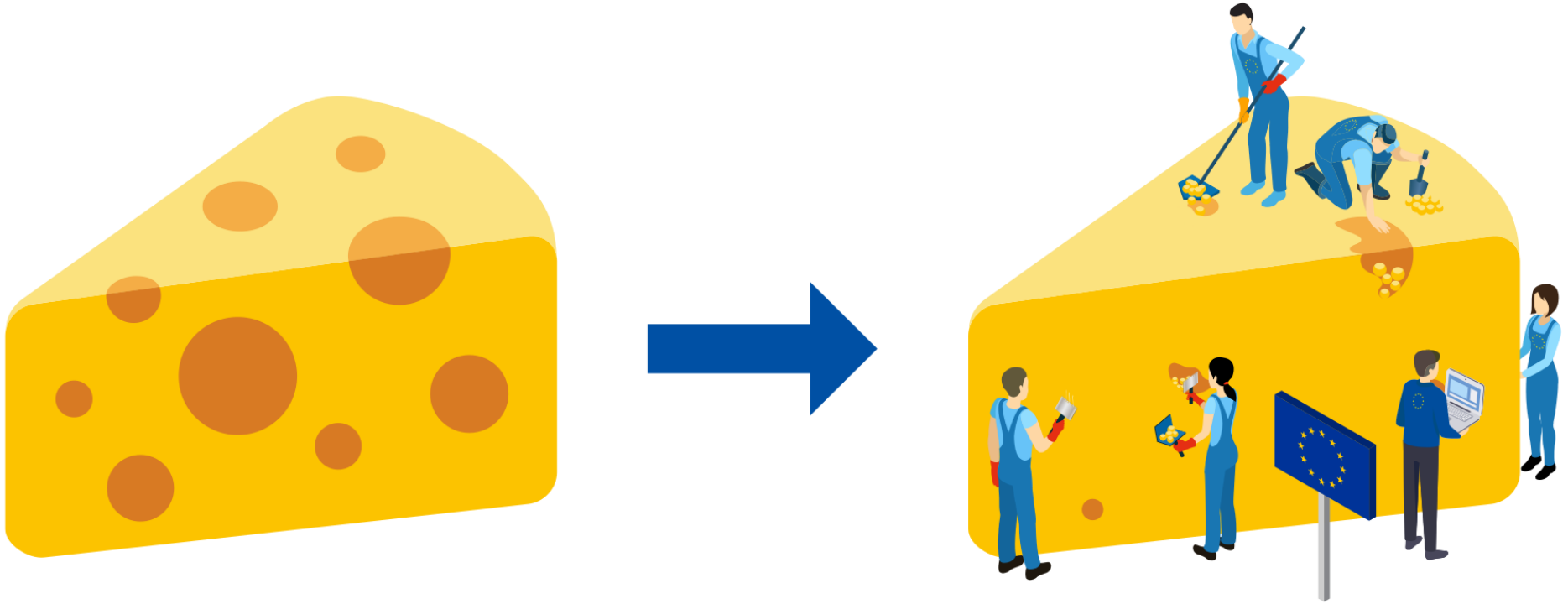
Key Elements:

- **Security:** Protecting systems and data from cyber threats (CRA, NIS2)
- **Reliability:** Digital services are available and function correctly when needed (CRA)
- **Privacy:** Ensuring personal information is collected, stored, and used appropriately (GDPR/DPDP - eIDAS 2.0/Aadhar+Digital Wallet)
- **Transparency:** Organizations are open about how they use data and make decisions (GDPR/DPDP)
- **Ethics:** Using technologies such as AI responsibly and fairly (AI ACT)
- **Compliance:** Adhering to laws, regulations, and industry standards

INPACE
Funded by the European Union
Project funded by

EU Cyber Resilience Act (CRA) in Nutshell

Regulation (EU) 2024/2847 establishes horizontal cybersecurity requirements for products with digital elements placed on the EU market.



Products will bear "CE marking" to indicate that they comply with the CRA requirements and national market surveillance authorities will ensure enforcement of the rules.

© INPACE 2024-2027

Main elements of the law

- **Cybersecurity rules** for placing in the EU market of hardware and software
- **Obligations applies** for manufacturers, importers and distributors
- Cybersecurity **essential requirements applicable** across the life cycle
- Harmonised **standards** to support implementation
- **Conformity assessment** – differentiated by product category
- **Reporting** obligations – actively exploited vulnerabilities & severe incidents
- **Market surveillance and enforcement**

INPACE
Funded by the European Union
Project funded by
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

Obligations of manufacturers



© INPACE 2024-2027

CRA implementation milestones

2025

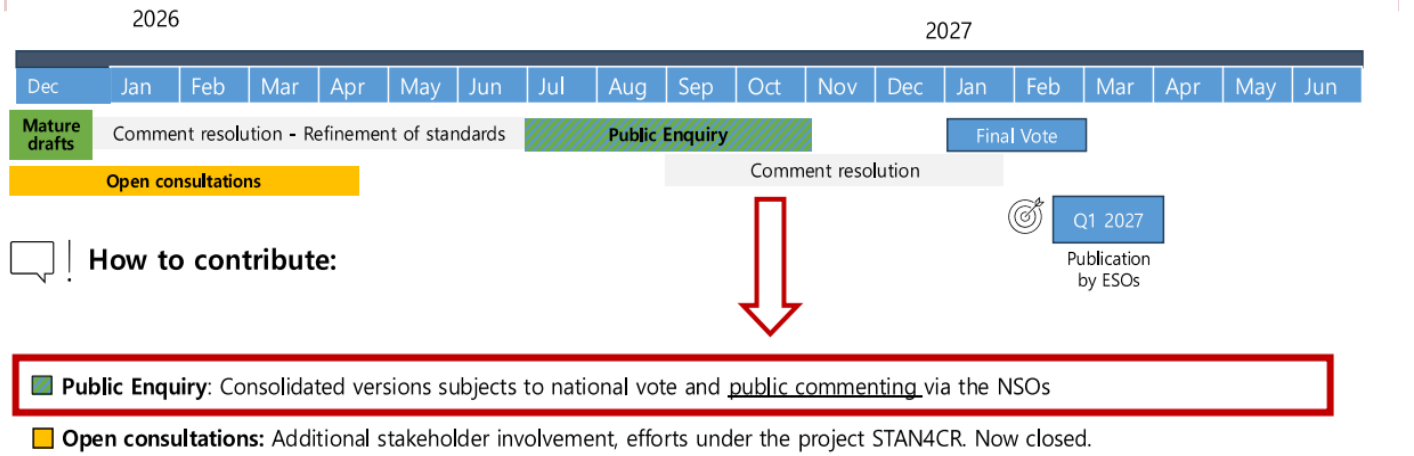
- Standardisation request (M/606)
- Launch of CRA expert group
- MS coordination bodies
- FAQ & CRA website
- Two IA/DA on time

2026

- First set of CRA guidelines
- Adoption of 36 standards
- Sufficient notified bodies
- ENISA Single Reporting Platform - Sept 2026
- DA on EUCC-CRA

2027

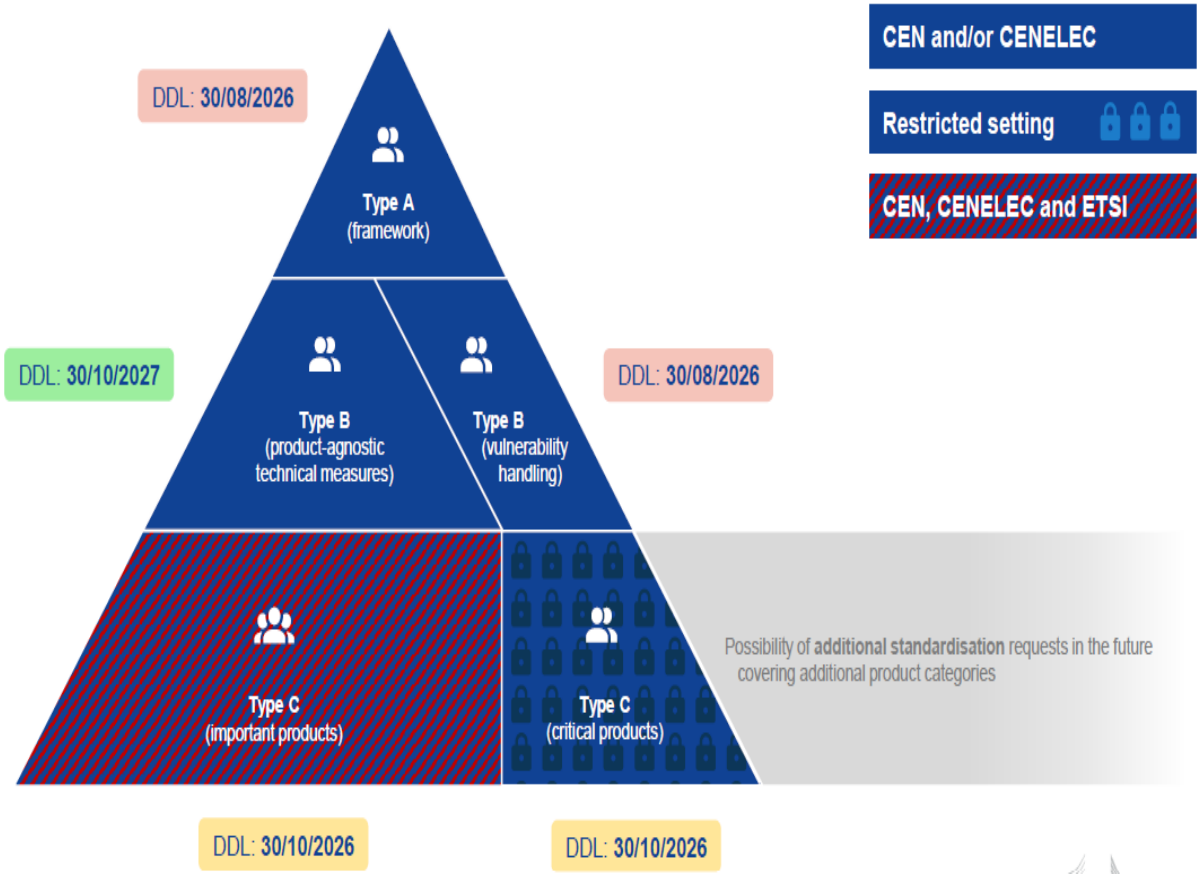
- More standards, guidance…
- Market surveillance
- Dec 2027: Full Application



INPACE
Funded by the European Union
Project funded by

CRA standardisation request (M/606) in a nutshell

- **41 requested deliverables**
- Includes both horizontal and vertical (or product-specific) standards
- **Horizontal standards** provide a common a framework, promoting coherence and offer horizontal processes for compliance with the CRA, including on vulnerability handling.
- **Vertical (also called product-specific) standards** intend to provide presumption of conformity for product types considering the risks involved in their intended purpose or reasonably foreseeable use.
- CRA standardisation request **prioritises** the development of standards covering the important and **critical product categories** set out in CRA Annex III and IV
- Project teams, experts and rapporteurs are supported by EU and EFTA funded projects STAN4CR and CYBESTAND.eu



© INPACE 2024-2027

CRA “Horizontal” Standards

Work Item		Mature Drafts	Final Drafts	Public Enquiry	Comment Resolution	Formal Vote
prEN 40000-1-1	Cybersecurity requirements for products with digital elements - Part 1-1: Vocabulary	✅	✅	✅	✅	✅
prEN 40000-1-2	Cybersecurity requirements for products with digital elements - Part 1-2: Principles, product risk management, and lifecycle activities	✅	✅	✅	✅	✅
prEN 40000-1-3	Cybersecurity requirements for products with digital elements - Part 1-3: Vulnerability Handling	✅	✅	✅	✅	🟡
prEN 40000-1-4	Digital elements – Generic Security Requirements	✅	✅	🟡		
Broad verticals: common OT requirements from which the CRA product-specific vertical standards are derived.						
EN IEC 62443-4-1:2018/prAA:2026	Secure product development lifecycle requirements	✅	✅	✅	✅	🟡
EN IEC 62443-4-2:2018/prAA:2026	Secure product development lifecycle requirements	✅	✅	✅	✅	🟡

INPACE
Funded by the European Union
Project funded by
Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

CRA “Vertical” standards 1(5)

Work Item		Mature Drafts	Final Drafts	Public Enquiry	Comment Resolution	Formal Vote
prEN 50770-1	Firewalls /intrusion detection and prevention systems	✓	✓	●		
prEN 50770-2	Network management systems	✓	●	-		
prEN 50770-3	Physical and virtual network interfaces	✓	●			
prEN 50770-4	Virtual private network (VPN)	✓	●			
prEN 50770-5	Routers, modems and switches	✓	●			
prEN 50770-6	SIEM	✓	●			
prEN 40003-3:2026	Platforms of smartcards and similar devices including secure elements	✓	✓	✓	✓	●
prEN 40001-3:2026	Microprocessors and microcontrollers with security-related functionalities	✓	✓	✓	✓	●
prEN 40002-3:2026	Tamper-resistant microprocessors and microcontrollers	✓	✓	✓	✓	●
prEN 40004-3-2026	Application Specific Integrated Circuits (ASICs) and Field-Programmable Gate Arrays (FPGAs)	✓	✓	✓	●	
prEN 18330	Smartcards or similar devices, including secure elements - Application layer	✓	✓	✓	●	
prEN 40000-10	Digital elements in identity management systems and privileged access management software and hardware	✓	✓	✓	●	
prEN 40000-11	Hardware Devices with Security Boxes	✓	✓	✓	●	
prEN XXX	Digital elements – Smart Meter Gateway	✓	✓	●		

- Important products class I
- Important products class II
- Critical products

INPACE
Funded by the European Union
Project funded by

CRA “Vertical” standards 2(5)

- CEN/TC 224 WG 17
- ETSI TC Cyber EUSR
- CLC/TC 47X WG 1-4
- CLC/TC 65X WG 3
- CEN-CLC/JTC 13 WG 6

Work Item	Mature Drafts	Final Drafts	Public Enquiry
EN 304 617 – Browsers	✓	✓	✓
EN 304 618 – Password Managers	✓	✓	✓
EN 304 619 – Antivirus	✓	✓	✓
EN 304 620 – VPNs	✓	✓	✓
EN 304 621 – NMS	✓	✓	✓
EN 304 622 –SIEM	✓	✓	✓
EN 304 623 – Boot Managers	✓	✓	✓
EN 304 624 – PKIs	✓	✓	✓
EN 304 625 – Network interfaces	✓	✓	✓
EN 304 626 – Operating Systems (OS)	✓	✓	✓
EN 304 627 – Routers, modems, switches	✓	✓	✓
EN 304 631 – Smart home general purpose virtual assistants	✓	✓	✓
EN 304 632 – Smart home products with security functionalities	✓	✓	✓
EN 304 633 – Internet connected toys	✓	✓	✓
EN 304 634 – Personal wearable products	✓	✓	✓
EN 304 635 – Hypervisors and container runtime systems	✓	✓	✓
EN 304 636 – Firewalls, intrusion detection and/or prevention systems	✓	✓	✓
EN 304 642 – Network functions of telecommunications systems	●		

✓ Completed | ● In Progress | ▢ Not Started

INPACE
Funded by the European Union
Project funded by

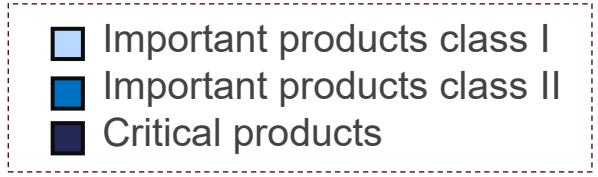
- Important products class II
- Critical products

CRA “Vertical” standards 3(5)

- CEN/TC 224 WG 17
- ETSI TC Cyber EUSR
- CLC/TC 47X WG 1-4
- CLC/TC 65X WG 3
- CEN-CLC/JTC 13 WG 6

CLC/TC 47X ‘Semiconductors and Trusted Chips Implementation’

- microprocessors and microcontrollers with security-related functionalities application specific integrated circuits (ASIC) and field-programmable gate arrays (FPGA) security-related functionalities
- tamper-resistant microprocessors and microcontrollers
- smartcards or similar devices, including secure elements (shared with CEN/TC 224)



INPACE
Funded by the European Union
Project funded by

CRA “Vertical” standards 4(5)

- CEN/TC 224 WG 17
- ETSI TC Cyber EUSR
- CLC/TC 47X WG 1-4
- **CLC/TC 65X WG 3**
- CEN-CLC/JTC 13 WG 6

CLC/TC 65X ‘Industrial-process measurement, control and automation’

EN IEC 62443-4-1/-4-2 provide the common OT requirements from which the CRA product-specific vertical standards intended for OJEU citation are derived. Both standards are not foreseen for citation in the OJEU.

- products with digital elements with the function of virtual private network (VPN)
- network management systems
- Security information and event management (SIEM) systems
- physical and virtual network interfaces
- routers, modems intended for the connection to the internet, and switches
- firewalls, intrusion, detection and/or prevention systems, including specifically those intended for industrial use

Important products class I
Important products class II
Critical products

INPACE
Funded by the European Union
Project funded by

CRA “Vertical” standards 5(5)

- CEN/TC 224 WG 17
- ETSI TC Cyber EUSR
- CLC/TC 47X WG 1-4
- CLC/TC 65X WG 3
- CEN-CLC/JTC 13 WG 6

CEN-CLC/JTC 13 WG 6: ‘Product Security’

- smart meter gateways within smart metering systems

- Important products class I
- Important products class II
- Critical products

INPACE
Funded by the European Union
Project funded by
Schweizerische Eidgenossenschaft / Confédération suisse / Confederazione Svizzera / Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

Other key TCs driving European Digital Trust standards

- **ETSI TC CYBER**: provides market-driven cybersecurity standardisation solutions, advice, and guidance to users, manufacturers, infrastructure/service operators and regulators.
  - Establishes security baselines, privacy-by-design standards, consumer IoT security, and cryptographic mechanism requirements.
- **CEN/CLC JTC 21 on AI**: standardization in the field of Artificial Intelligence
  - Develops standards supporting the EU AI Act, emphasizing trustworthy AI, risk management, and algorithmic auditability.
  - prEN 18282 Artificial intelligence - Cybersecurity specifications for AI Systems (approval stage)
- **ETSI TC SAI**: develops technical standards and frameworks to protect AI systems from cyber threats, mitigate malicious AI misuse, and ensure responsible, safe AI deployment
  - ETSI EN 304 223: Baseline security requirements for AI models and systems.
- **CEN TC 224: Personal identification and related personal devices with secure element, systems, operations and privacy in a multi sectorial environment:**
  - Security requirements for device for authentication,
  - Security requirements for trustworthy systems managing certificates and time-stamps etc.
- **CEN/CLC/JTC 24 on Digital Product Passport - Framework and System**:
  - WG3 on security and WG4 on Interoperability framework
  - EN 18239:2026: Digital product passport - Access rights management, information system security, and business confidentiality
- **ETSI TC Data for on Open, Trusted, Distributed Data Infrastructures**
  - European Data Act and to the data-related aspects of the European AI Act
  - WG Data Infrastructure, Semantic and Information Models, Vertical Products, Applications, and Services : NGSI-LD (Next Generation Service Interfaces - Linked Data) an open standard for Context Information Management (CIM), enabling systems to share, query, and update real-world information in a semantically interoperable way
- **ETSI TC on Electronic Signatures & Infrastructures**: produces standards and technical specifications supporting requirements for Electronic Identity, Authentication and Signatures.
  - eIDAS trust services, digital signatures, electronic seals.

© INPACE 2024-2027

How SESEI and EU–India PI can help

- **EU–India Trade and Technology Council (TTC):** use policy dialogue to identify common priorities and coordinate work on digital governance, security and ICT standardisation.
- **Indian and European SDOs**: exchange technical contributions, align terminology and identify opportunities for common or interoperable specifications through **SESEI**.
- **SESEI**: access to standards bodies, regulators, industry and researchers; available for clarifying Standards, Regulations and participation routes.
- **InDiCo-Global**: connect policy and technical communities around ICT standards, including cybersecurity and IoT security.
- **Research and innovation programmes**: develop joint demonstrators, testbeds and evidence that can feed into standards work.

These instruments enable dialogue and cooperation; they do not themselves make standards, certify products or replace regulatory obligations.

INPACE
Funded by the European Union
Project funded by

Conclusion

- Digital trust is a lifecycle property: design securely, maintain products responsibly, and communicate clearly.
- CRA is moving from legislation to implementation; reporting duties are already applicable, and the main obligations will follow in December 2027.
- Standards make requirements actionable, testable and interoperable — but they need practical validation and sustained implementation.
- SESEI can connect Indian and European stakeholders;
- TTC, InDiCo-Global and research collaboration can add policy alignment, technical depth and pilots.

Goal: Lets jointly shape globally relevant standards so security, interoperability and trust are built into digital technologies from the start.

© INPACE 2024-2027

Important links

- The Cyber Resilience Act - Legislation
- The Cyber Resilience Act - Background information
- The Cyber Resilience Act - Summary of the legislative text
- C(2026) 5252 - Communication on the Cyber Resilience Act (CRA) guidance
- C(2026) 5252 - Annex - Commission guidance on the application of the Cyber Resilience Act (CRA)
- List of designated Notifying Authorities (NAs) and Market Surveillance Authorities
- NANDO website lists the notified bodies under European Union legislation, including (once available) for the CRA.
- CRA European standards | STAN4CR: website where the ESOs make information available on the CRA standards development activities.
- ETSI launches approval process for 17 European Standards supporting the Cyber Resilience Act

© INPACE 2024-2027

INPACE
EU-India Digital
Cooperation Conference 2026
New Delhi

Thank you

INPACE

Funded by
the European Union

Project funded by

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,
Education and Research EAER
**State Secretariat for Education,
Research and Innovation SERI**

The INPACE project has received funding from the European Union's Horizon Europe Research and Innovation Programme under grant agreement 101135568. Funded by the European Union (INPACE, 101135568). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them. This work has received funding from the Swiss State Secretariat for Education, Research and Innovation (SERI).

