CRA Standards Unlocked

Navigating smartcards and similar devices & secure element compliance

Webinar, 2025-07-25

Ivan Plajh

Rapporteur for TC224 WG17 Standardization of CRA Vertical Category 41

Content

1. Mandate, team, progress by now, principles
2. Description of the SE, Smart Cards and similar devices, scope
3. Structure of this standard and dependancies
4. Some use cases
5. Risk assessment principles
6. CRA compliance evaluation principles
7. Q&A

Content of this presentation does not follow the content of the standard.

Mandate evolving from the EC Mandate M/606

European Commission

Mandate **M/606** 2025-02-03

CEN CENELEC

CEN/TC 224 WG 17	41b	Application
CLC/TC 47X	41a	Secure IC / platform
CLC/TC 65X WG 3		
CEN-CLC/JTC 13 WG 9		
CEN-CLC/JTC 13 WG 6		

Secure Element

ETSI

- ETSI CYBER
- ETSI USER

Team: TC224 WG17 Task Force for V41b

Dr. **Gisela Meister**
Senior Security Consultant
Eurosmart

N/A

Katharina Wallhäusser
Security evaluation expert
G&D

Alban Feraud
Manager of standardization and regulatory affairs

Marc LeGuin
Head of ITSEF
TÜV NORD Group

Denis Praca
Standardization expert, Thales.
ETSI TC SET Chairman

Heiko Kruse
ETSI TC SET Vice-Chairman

Fabien Deboyer
Security Certification Expert
NXP

N/A

Thomas Aichinger
Sen. Security Certification Officer
Austria Card

Yann-Loic Aubin
Payment Standards Expert
IDEMIA Secure Transactions

Ivan Plajh
Rapporteur TC224WG17
Task Force CRA V41b

Rapporteur / Presenter

Ivan Plajh

Experience relevant for this mission:

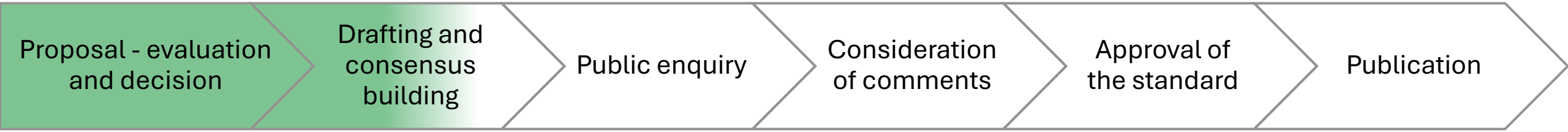
- Semiconductor industry (NXP, Infineon)
  - eSE /Chip OS and application product management and tech support
  - Multiple CC product evaluations (Chip OS, ePP, eMRTD)

- Smart Card production industry (Smartrac, HID)

- Hands-on SE application development (Java Card)

- **Standardization**:
  - UN/ICAO9003, Bruselles Interoperability Group
  - NFC Forum, core tech + NFC Tags
  - Global Platform
  - a couple of industry specific standardizations
  - since Feb 2025: CENELEC TC224/WG17

Progress of this standard by now



Principle – 41b

REVIEW

established standardization / evaluation practices

for Secure Elements, smart cards, similar devices

RE-USE

What is evidently compliant with CRA essential requirements

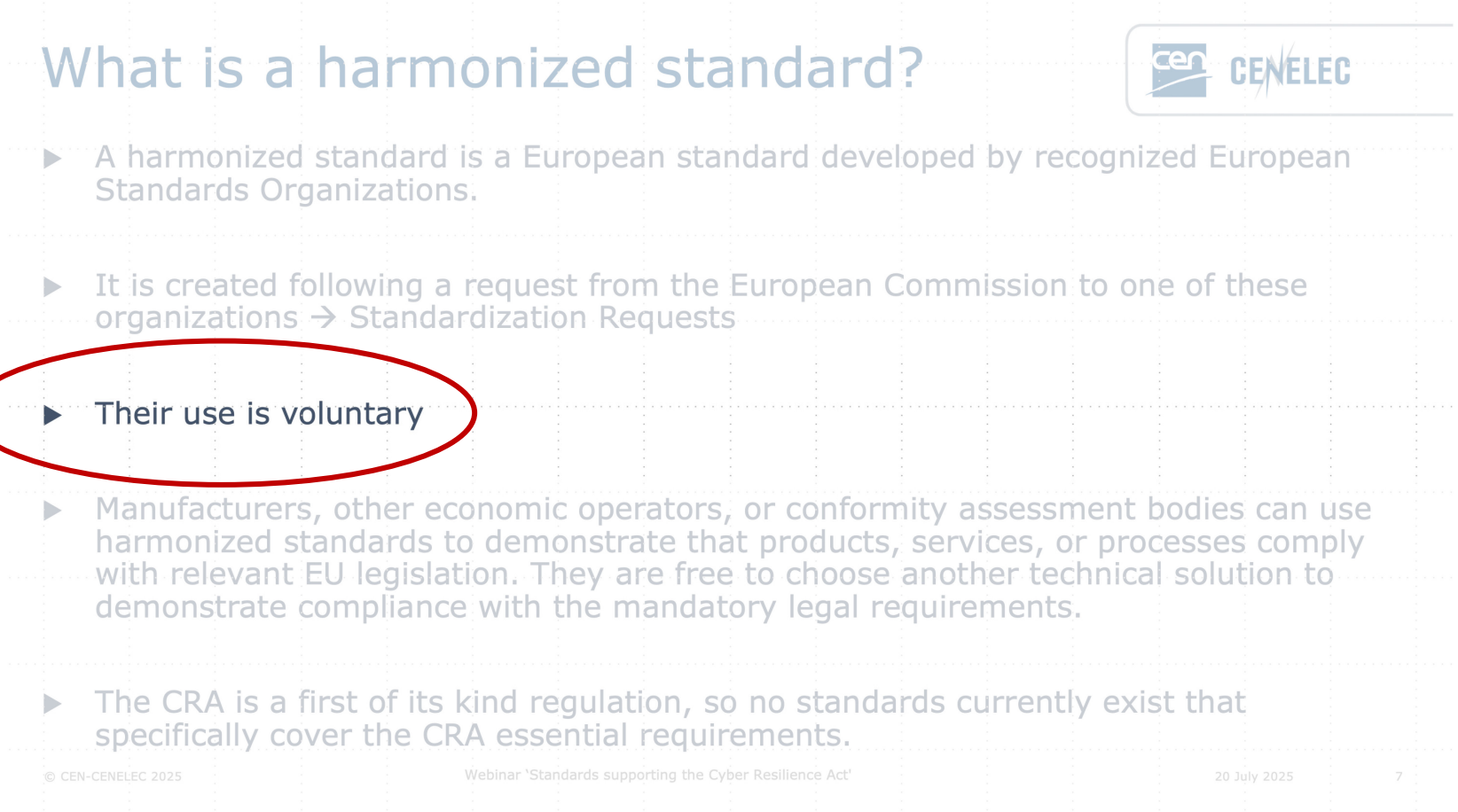
Listed in:
CRA Annex I, part I and part II

!

Wherever the established practices are not offering baseline for compliance, standard will demand additional effort from manufacturers.

Essential CRA requirements → Annex I p.I & II

Important: **this one will be a CRA harmonized standard**



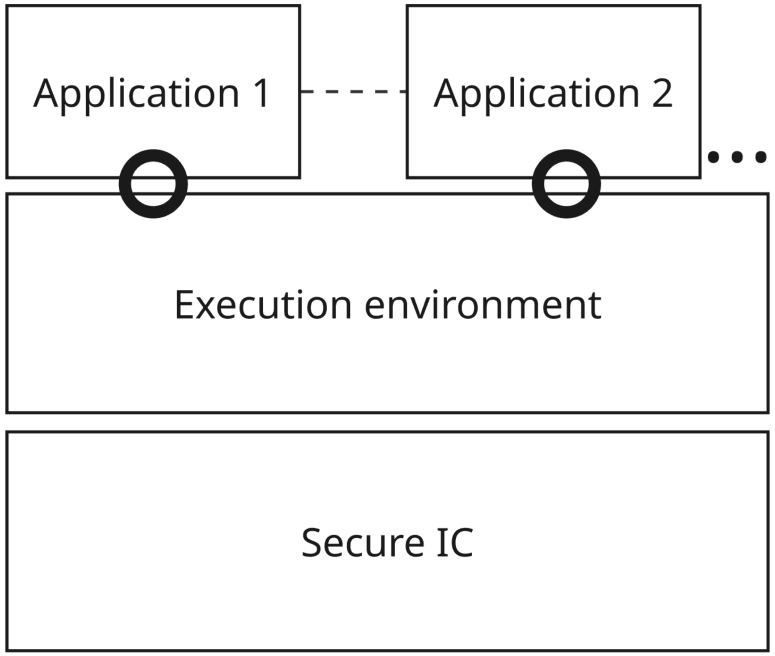
Harmonization needs consensus
But this might come with industry specific trade-offs

Structure of the standard

Normative part	Security requirements, as response to Annex I part I and part II
Descriptive / Informative	General provisions
	Risk assessment guideline
	Life Cycle Management – essential for CRA compliance
	Use cases: payment, government, embedded, UICC, …
	Harmonization: Annex describing ‘bridges’ to other standards

Clarify how to implement essential CRA requirements

Secure Element

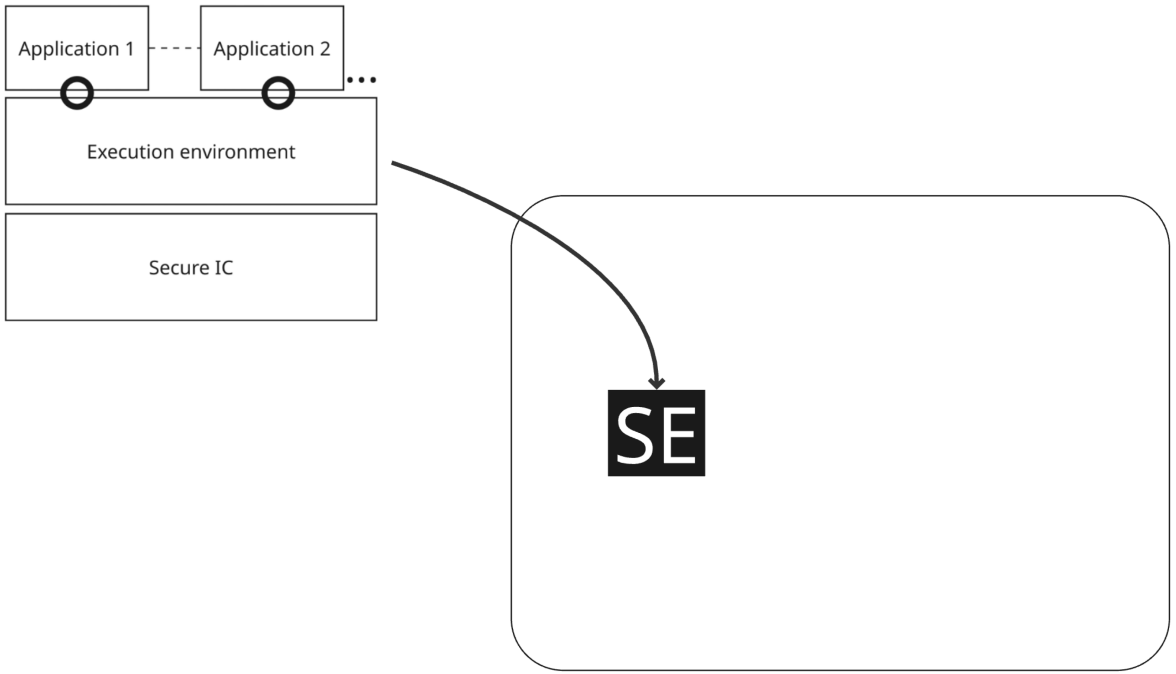


A **Secure Element** designates:

(1) an underlying Secure IC,
(2) execution environment, and
(3) at least one application which is embedded and runs on that underlying IC

The execution environment may be provided separately from the Secure IC as a set of basic input/output services (e.g access to memory – read/write, access to basic crypto services, access to IO, etc.) or a secure embedded operating system providing computation services (e.g. memory management, cryptographic functions library, runtime environment, etc.).

Smart card

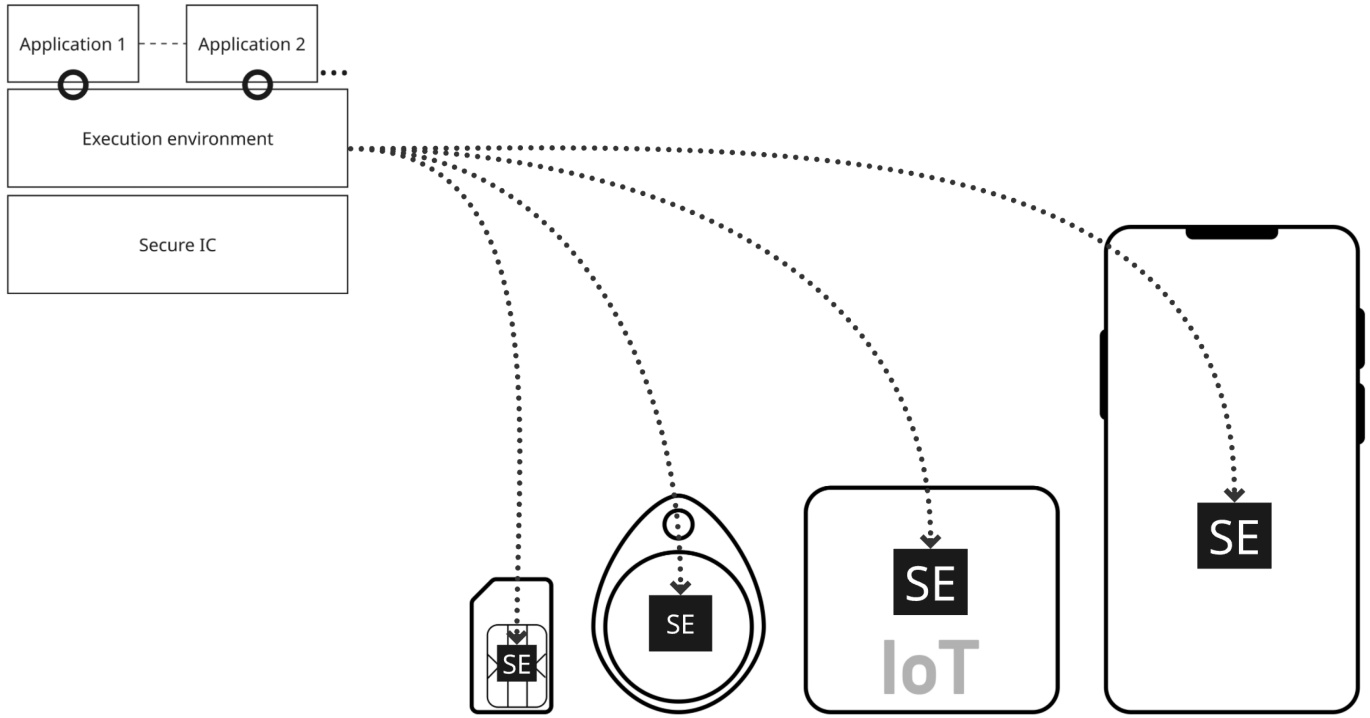


Within the scope of this standard, a smart card consists of a **Secure Element** that is embedded in a body which has an ID1/TD1 form factor as defined in ISO/IEC 7810:2019.

The body may be made of one or multiple layers of plastic, wood or any type of material.

In most of the cases a smart card supports contactless (ISO14443) and/or contact-based (ISO7816) interfaces for communication.

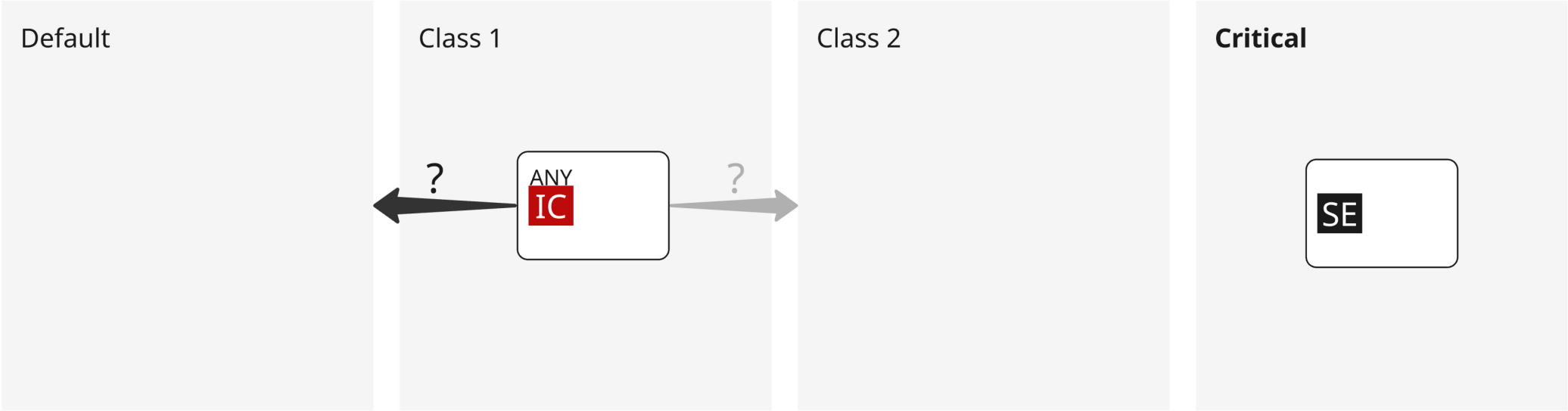
Similar Devices



Similar devices comprise Secure Element embedded in bodies which

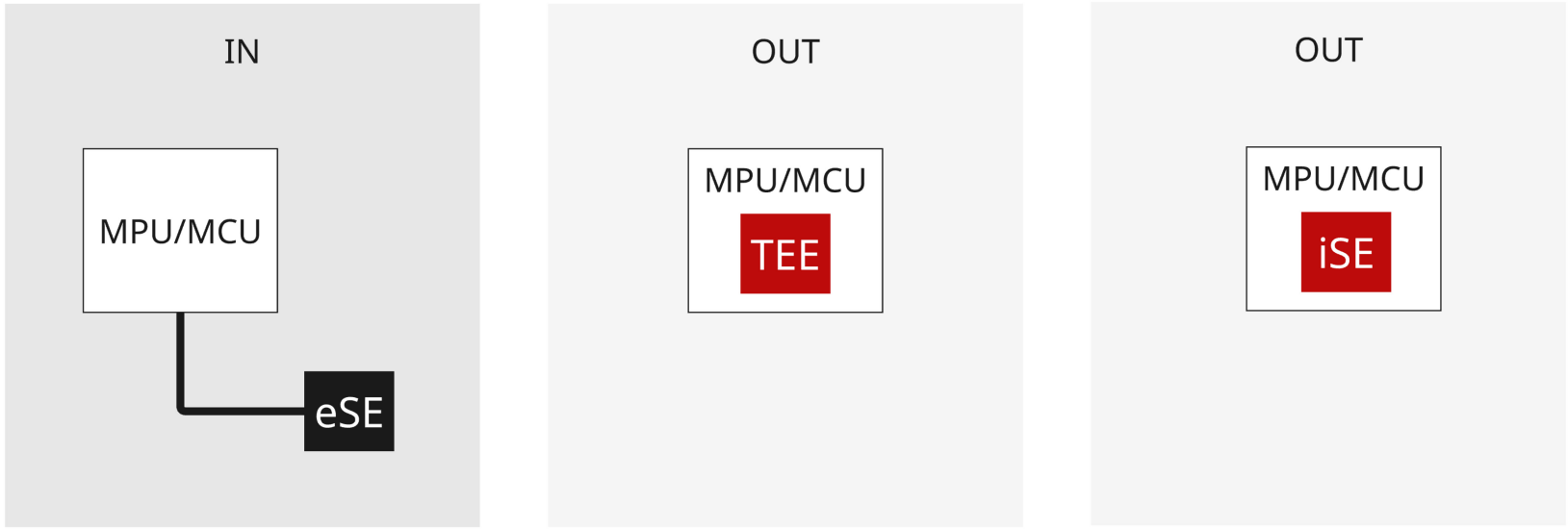
(1) have a form factor different from the smart card, and
(2) are optionally equipped with additional electronic and digital devices.

What is not in the scope of this standard?



There are use-case-specific cards without (the need for) Secure Elements.

What is also not in the scope of this standard?



There are other possibilities to manage security functions in the IC's and systems.

Life cycle management

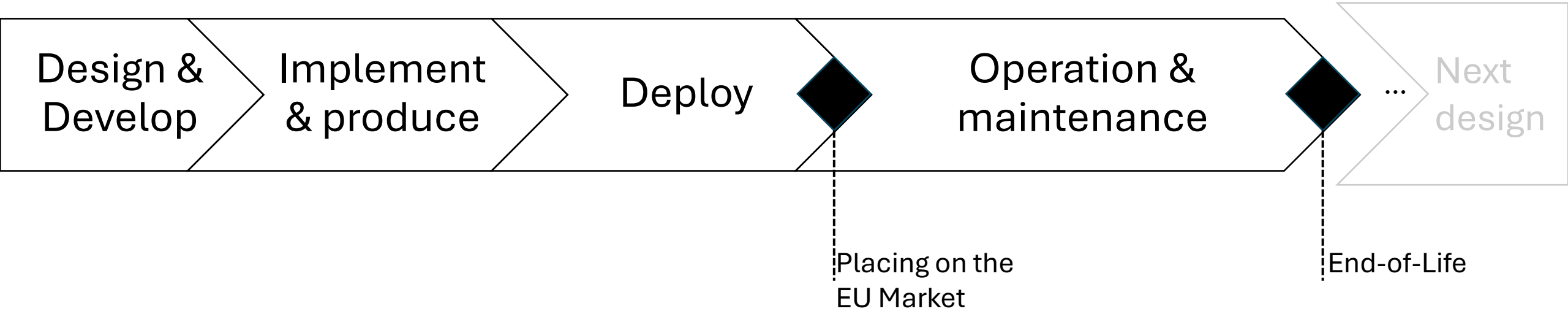


*illustration based on M. Wolf (BOSCH Security), presentation given on the IoT Cyber Compliance Day | Brussels | 2025-03-25

Life cycle management – why descriptive?

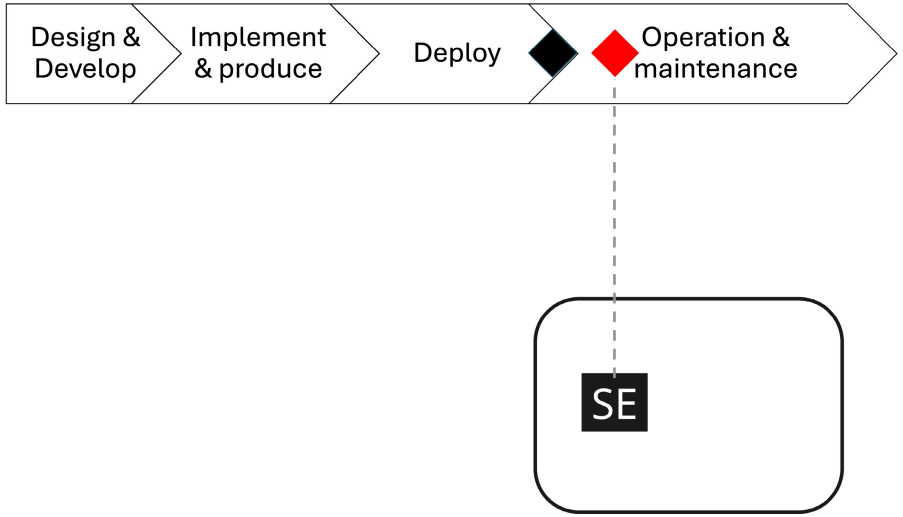
- There are industry specific Life Cycle Management Systems (LCMS) which
  - Are covering functional parts that are evidently out of the CRA scope
  - Are rather specific to a use case and therefore may require an exception that is still within regulative compliance boundaries

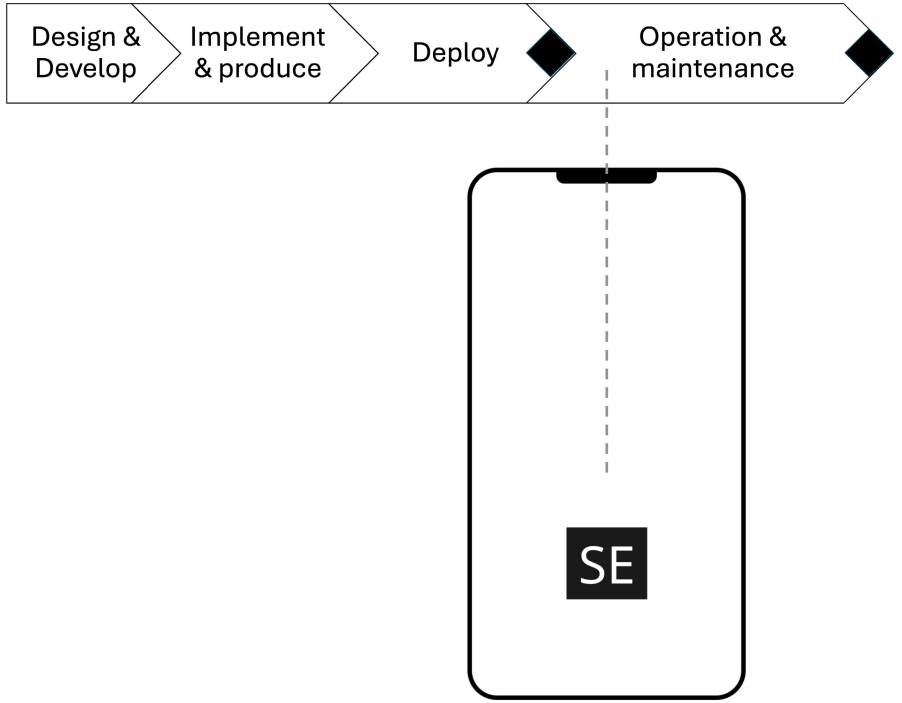
- CRA standard(s) is(are) focused on response to (essential) regulative requirements and manufacturers may have some freedom to accommodate them within their life-cycle systems
  - LCMS must be well documented and auditable
  - CRA requirements from this standard must be consistently implemented and maintaned throughout the entire lifecycle of the PwDE

Some LCM standards

- ISO15228
- PP9911
- GlobalPlatform

Life cycle management – an example of practical differences

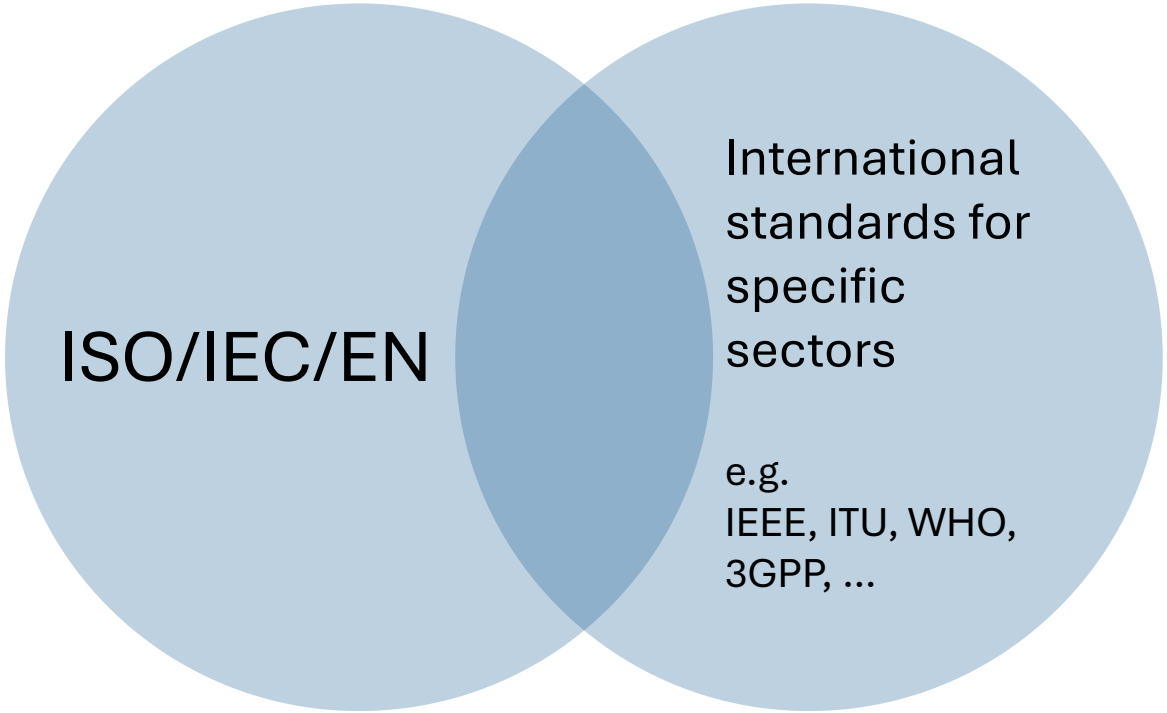




A smart card FW/SW update is not always practical in the operational mode. Established practice is **card replacement**...

...while the same security issue, on a Secure Element embeded into a similar device may be handled **automatically**.

Normative references



National standards
Cannot be used / only by reviewed permitted exception

Technical Reports
Only informative, cannot include requirements

Technical Specifications
do not carry the obligation of withdrawal of national conflicting standards

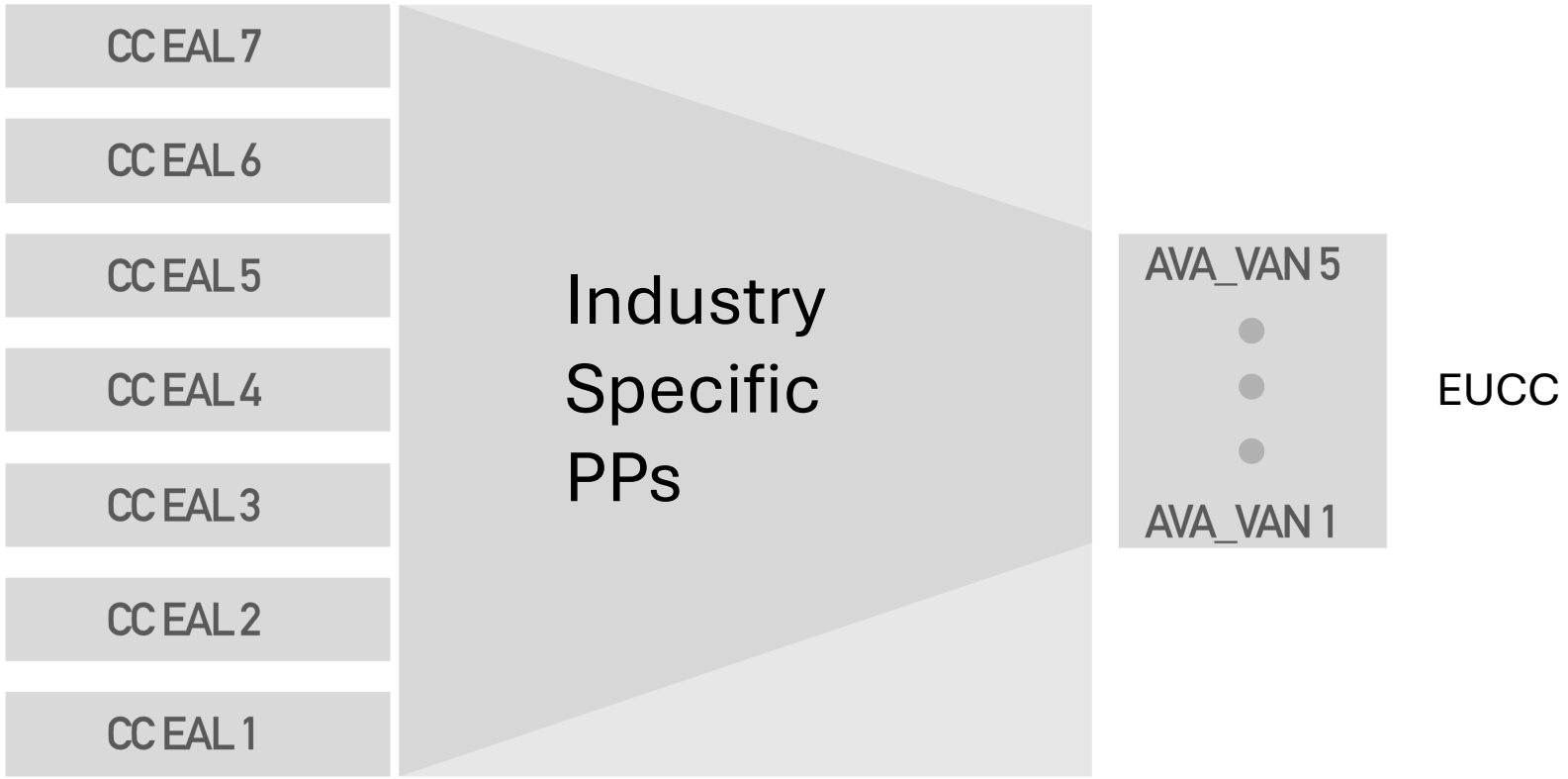
Sources / harmonisation vs. references

Normative (→ state of the art)
prEN XXX(JT013089), Cybersecurity requirements for products with digital elements, Principles for cyber resilience
prEN XXX(JT013090), Cybersecurity requirements for products with digital elements, Vulnerability handling
prEN 50764 (TC47x), Cybersecurity requirements for products with digital elements, Secure IC CRA standard
ISO/IEC 15408:2022 (all parts), Information security, cybersecurity and privacy protection, Evaluation criteria for IT security
…

Bibliography
ISO/IEC 7810:2019 Identification cards - Physical characteristics
ISO14443 (all parts), Cards and security devices for personal identification - Contactless proximity objects,
ISO7816 (all parts), Identification cards - Integrated circuit cards
GPSE PP:2021, Global Platform Secure Element Protection Profile, Version 1.0, February 2021, Reference: GPC_SPE_174
GPTEE:2022, Trusted Execution Environment System Architecture, Global Platform
…

…the lists are still **evolving**

ISO/IEC 15408:2022 relevance



Use cases for a SE

Intended purpose:

- Retrieval and communication of the sensitive information from and through the secure elements' interfaces
- Processing of these information, which includes performance of computational and cryptographic operations
- secure storage of retrieved and/or processed information

- Governmental ID
  - eMRTD, eID
  - digital signatures, wallets
  - Cards & mobile
- Secure Identification
  - Physical and on-line interactions
  - UICC access to mobile network
  - …
- Payment
  - Open loop, closed loop
  - Card, Mobile
- Access control
  - Logical
  - Physical
  - Network
- IoT
- …

The list of use cases cannot be finite.

Risk assessment – within the SE / Smart Card industry – not final

Level of threat → Level of severity → Risk profile → Evaluation

T2

High attack potential

ISO/IEC 15408:2022

T1

Moderate attack potential

ISO/IEC 15408:2022

S3

Impacts and threat to lives, privacy, significant value

S2

Impacts and threat to privacy, significant value

S1

Impacts and threat to value

	S3	S2	S1
T2	**RP3**	**RP2**	**RP1**
T1	**RP3**	**RP1**	**RP1**

Essential security requirements (CRA Annex I, part I & II)

1. Security by design
2. No known vulnerabilities
3. Secure by default when placed on EU market
4. Security updates
5. Access control (to PwDE)
6. Confidentiality protectio
7. Integrity protection
8. Data minimization
9. Basic functionality available despite of incident
10. Minimize negative impact around PwDE
11. Limit attach surface
12. Mitigation of incidents
13. Recording & monitoring
14. Deletion of data & settings by end-user

14

Requirements on product

1. Identify and document components and vulnerabilities
2. Address vulnerabilities
3. Perform regular security testing
4. Publish fixed vulnerabilities
5. Implement and practice vulnerability disclosure policy
6. Support 3rd party reporting
7. Ensure secure distribution of updates
8. Dissemination of updates

8

Requirements on vulnerability handling

Product 1: Security by design

Definition	Reference*	Applicability	Assessmnt**
The application manufacturer shall perform the security analysis of the application, determine the target risk environment and define the security problem in terms of threats and assumptions specific to the application. The application manufacturer identifies and implements the applicable technical requirements for their appication	ASE_INT.1 ASE_SPD.1 ASE_OBJ.2 ASE_REQ.1	Mandatory	ASE_INT.1.1E ASE_SPD.1.1E ASE_OBJ.2.xE ASE_REQ.1.xE ADV_FSP.2.xE ADV_IMP1.xE

Outlook – this is the content for the deep dive (~September 2025)

* ISO/IEC 15408-3:2022 developer (D) and content (C) requirements
** ISO/IEC 18045:2022

Evaluation vs. Certification

This standard involves

ASSESSMENT METHODOLOGIES

This is not the same as

CERTIFICATION SCHEMES

Example:

ADV_ARC.1

- means that a manufacturer shall describe a security architecture for the evaluated PwDE to achieve CRA compliance
- it does not mean that a complete Common Criteria evaluation and certification to a certain level shall be accomplished.

Standard uses ISO/IEC 15408:2022 standardized ‘language’.
Adaptations towards EUCC are considered.

Alternative *languages* shall also adequatly respond to a CRA requirement

CRA essential requirements		Normative response by this standard		Alternative industry specific response	
reference	**description**	**reference**	**description**	**reference**	**description**
Part I, (1)	Security by design	Chapters 8 and 9.1	Risk profiling for Secure Elements and Security by Design	Standard/ chapter / requirement	Description why is it equivalent response to the CRA e.r.

…an essential CRA requirement…

…answered by this standard…

…or by an alternative, use-case specific standard.

Such details will be exposed in the use-case specific annexes, which are informative.

Outlook:
Deep Dive into this standard

~September 2025

What to expect?

- Harmonization / other standards relevance
- Risk profiling refinement
- Evaluation criteria details
- Use cases – aspects of aplicability

JOIN OUR WORK!

Accellerating towards completion:

- Field experts welcome to join via national standardization bodies

Q&A

Thank you!

Ivan Plajh