CRA Standards Unlocked

Navigating smartcards and similar devices & secure element compliance

Deep Dive, 2025-10-13

CEN/CENELEC TC224 WG17

Task Force for creation of the Vertical Category 41b Standard

Content

1. Introduction
2. Risk assessment principles
3. Use case details: Governmental ID
4. CRA compliance evaluation principles
5. Q&A

Introduction

reminder from the webinar on 2025-07-25

Mandate evolving from the EC Mandate M/606

European Commission

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

CEN CENELEC

- CEN/TC 224 WG 17
- CLC/TC 47X
- CLC/TC 65X WG 3
- CEN-CLC/JTC 13 WG 9
- CEN-CLC/JTC 13 WG 6

ETSI

- ETSI CYBER
- ETSI USER

Secure Element

- 41b → Application
- 41a → Secure IC / platform

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

N/A

Soline Renner
Paycert

Heiko Kruse
ETSI TC SET Vice-Chairman

Fabien Deboyer
Security Certification Expert
NXP

N/A

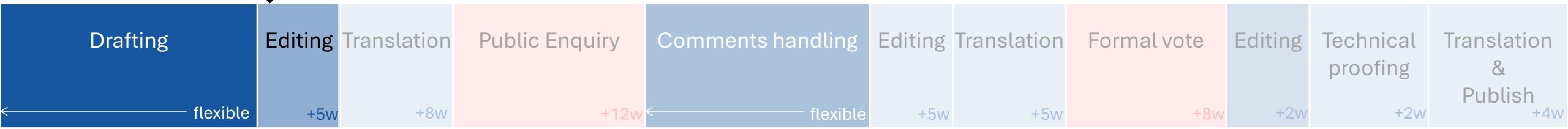
Thomas Aichinger
Sen. Security Certification Officer
Austria Card

Yann-Loic Aubin
Payment Standards Expert
IDEMIA Secure Transactions

Ivan Plajh
Rapporteur TC224WG17
Task Force CRA V41b

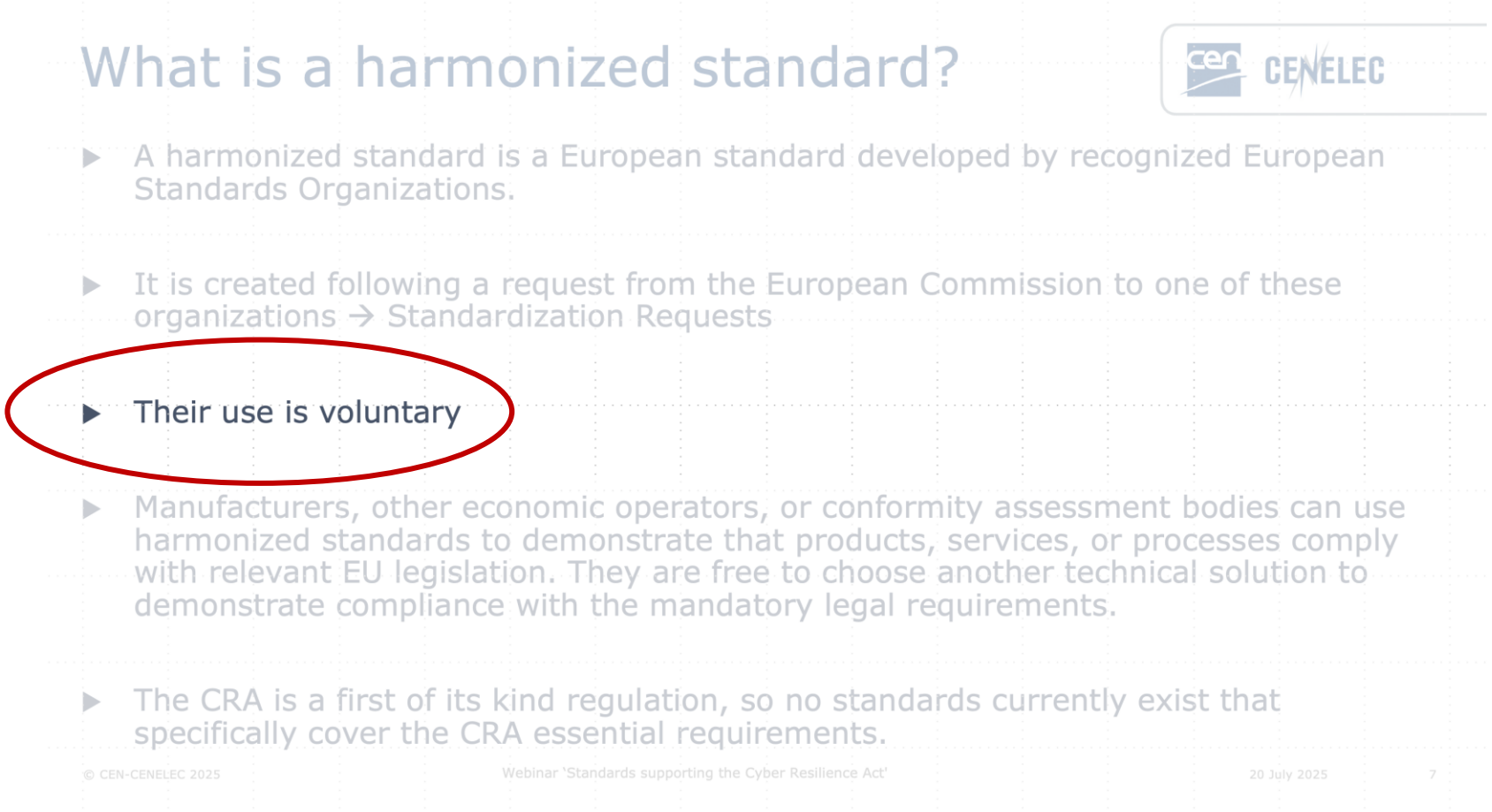
Progress of this standard by now

We are here: ◆



CENELEC process training: https://www.youtube.com/watch?v=_T6zGykI3nI

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



What does this mean?

There are 3 paths for application on the SE to achieve CRA compliance.

IF this standard is optional…

~~… THEN the **CRA compliance is also optional**!!!~~

NOT TRUE.

3 paths to CRA compliance for application on the SE:

1	Assessment according to this standard:
2	Via EUCC evaluation and certification:
3	Manufacturer's own process:

- Lowest effort for manufacturer and for the evaluator
- Shortest time-to-compliance

- Effort to 'close the gap' between ToE and scope of the CRA harmonised standard
- More time needed for EUCC but no additional effort for CRA evaluation (presumption of conformity)

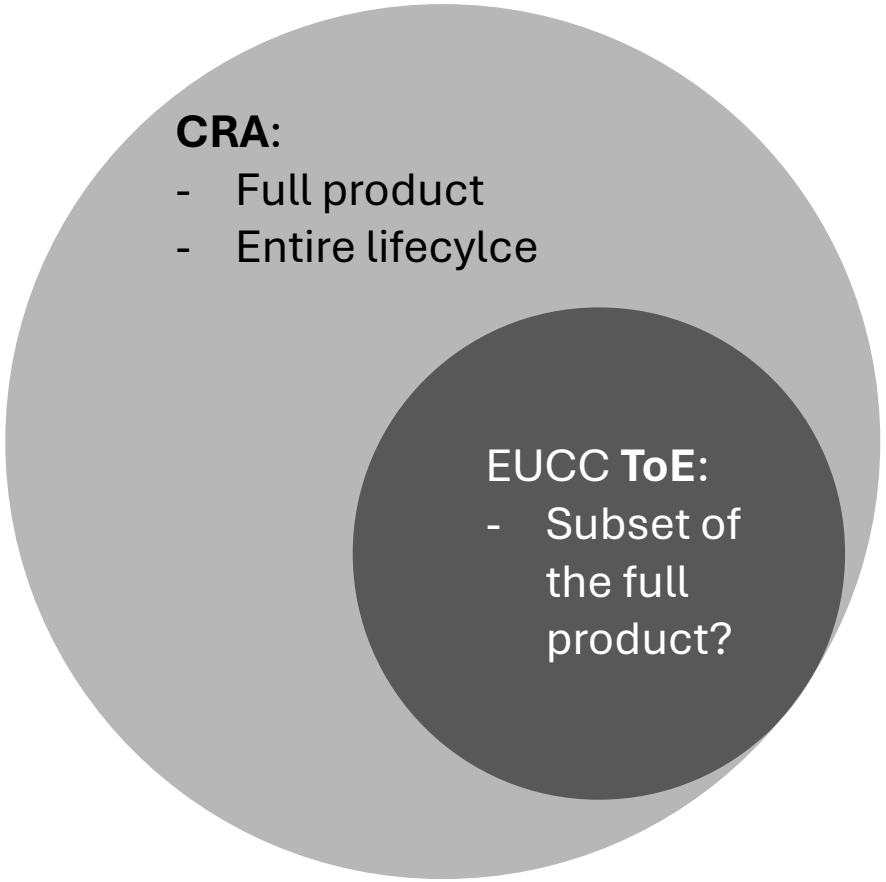
- Highest effort for manufacturer
- Highest effort for an evaluator
- Potentially unpredictible time-to-comply

CRA compliance via EUCC

But … **mind the gap!**

https://certification.enisa.europa.eu/publications/cyber-resilience-act-implementation-eucc-and-its-applicable-technical-elements_en

CRA compliance via EUCC – the (potential) gap



ToE may have a focus on less than what is in the scope of the CRA.

Manufacturer should examine harmonized standard(s) and additional documentation.

Gaps are to be closed by new or updated Security Target / Protection Profile.

Otherwise, presumption of CRA conformity cannot be claimed.

For the application on the SE - in any of these 3 cases:

AVA_VAN.5
AVA_VAN.4

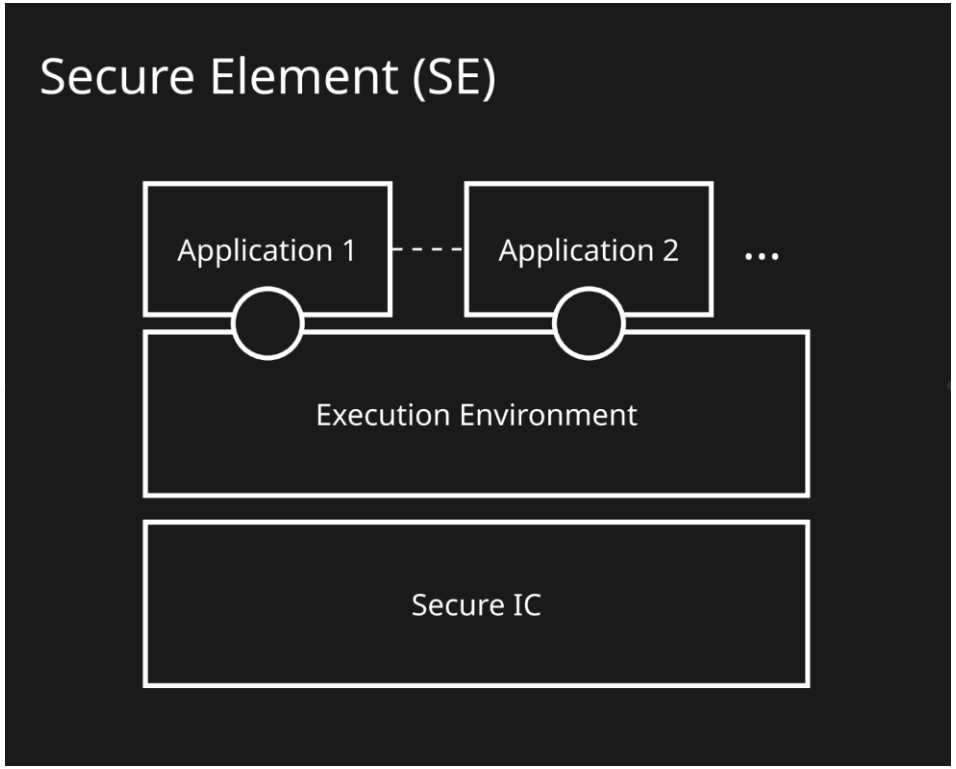
3rd party to assess / evaluate
(CRA **critical** category)

There is one known exception, allowing AVA_VAN.3

What to evaluate?

Deep dive into architectures & applications

Application on the Secure Element

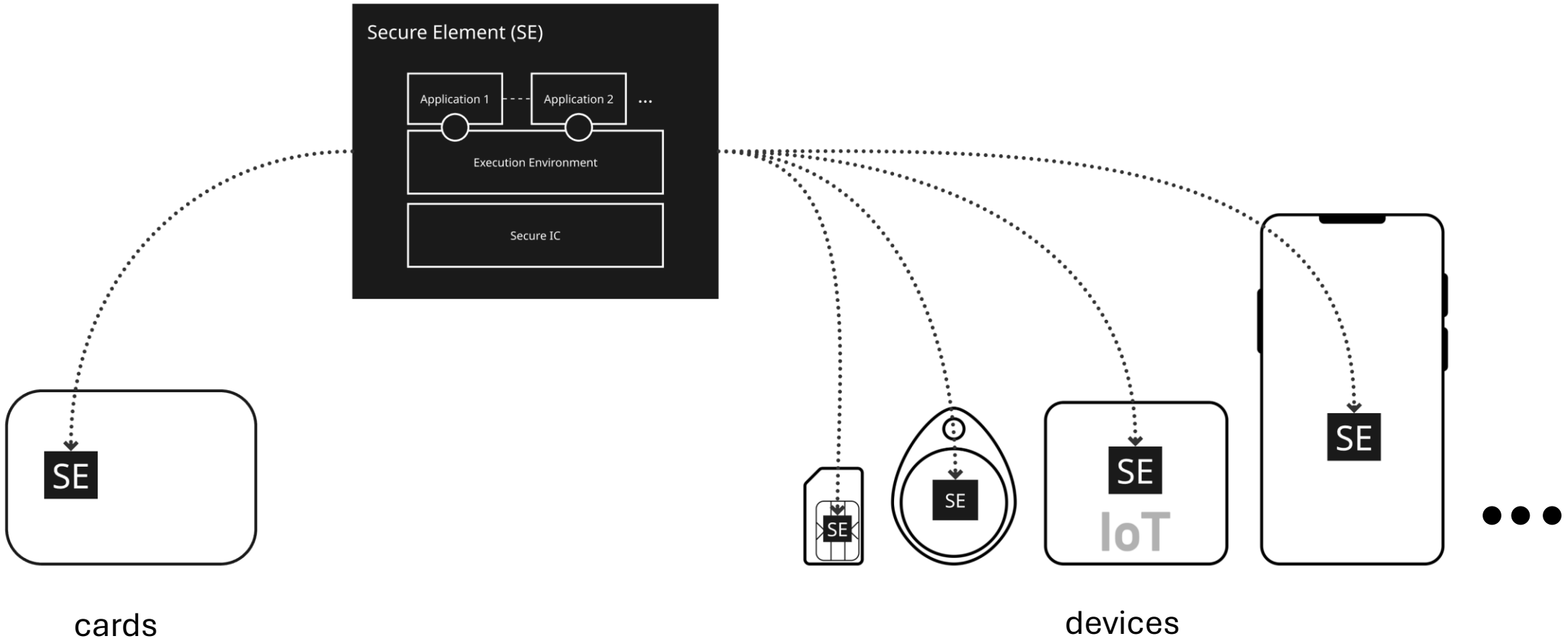


A **Secure Element** designates:

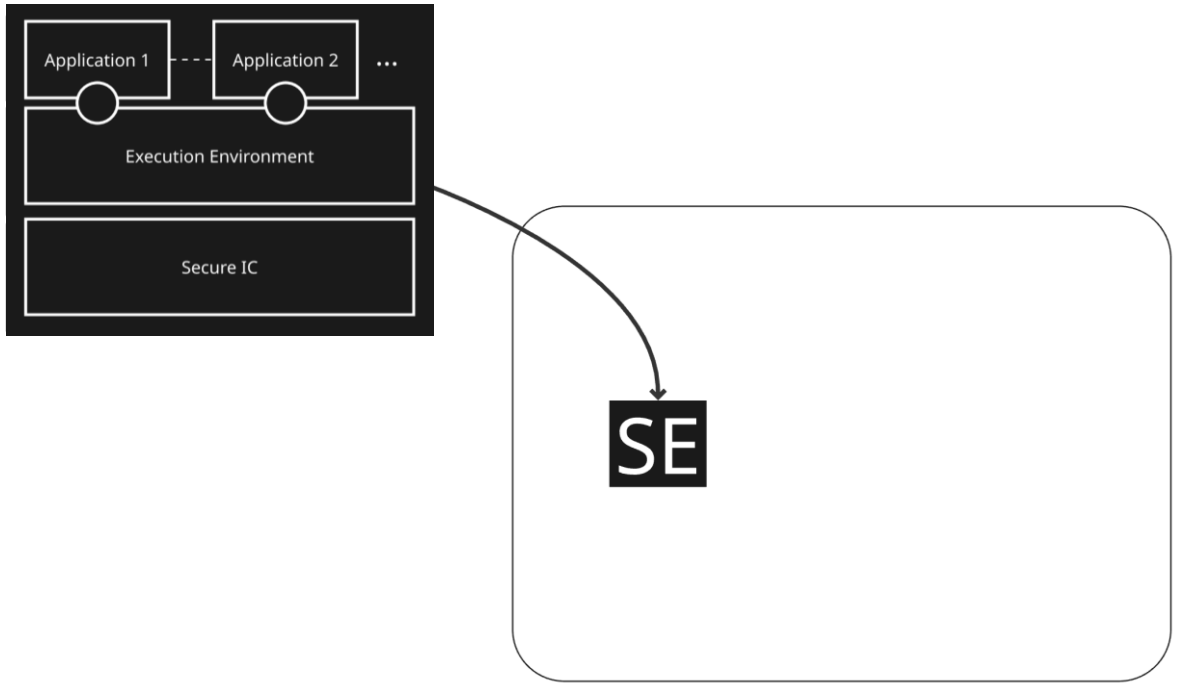
(1) an underlying Secure IC,
(2) execution environment, and
(3) at least one application which is embedded and runs on that underlying IC

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.).

Application on the SE within the smart cards & similar devices



Smart card

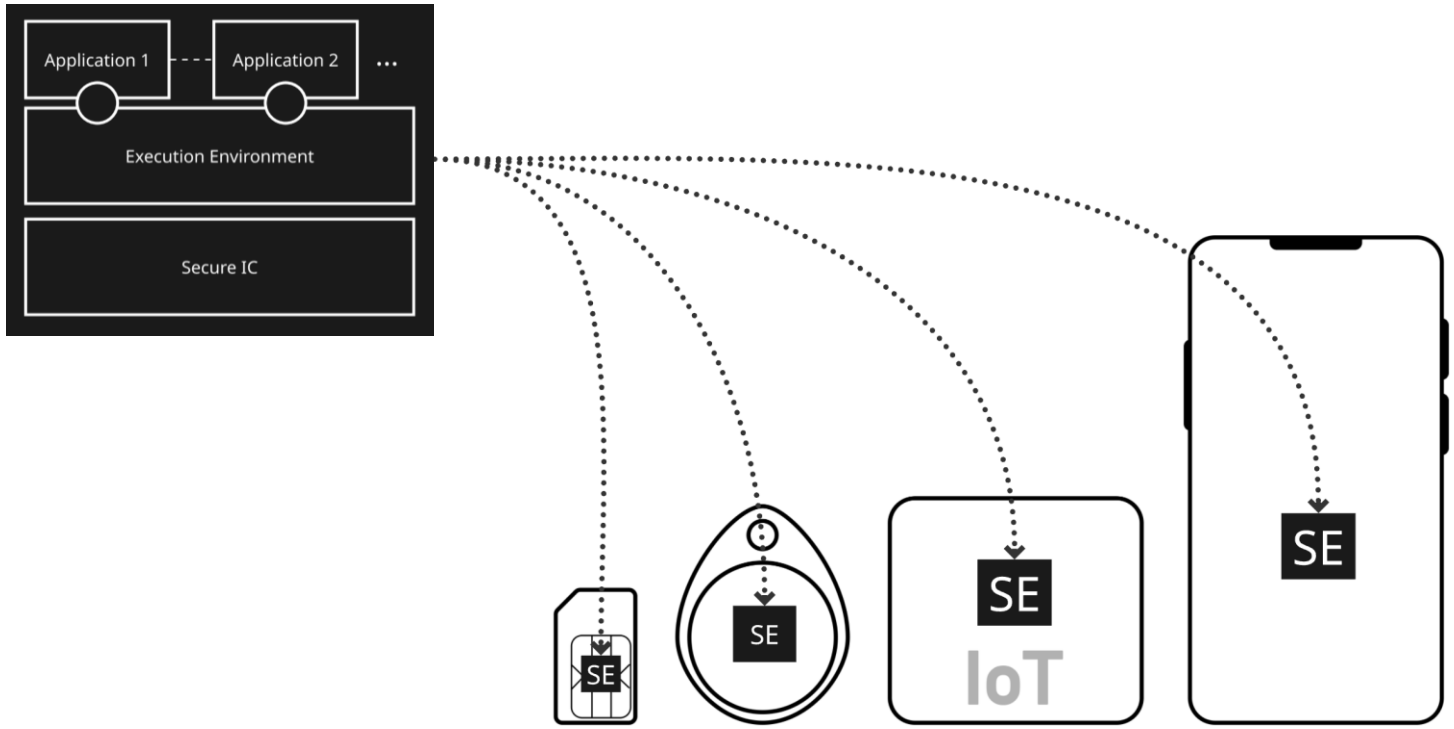


Within the scope of this standard, a smart card consists of a **Secure Element** that is embedded in a body which has an ID1/TD1 form factor as defined in ISO/IEC 7810:2019.

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.

●●●

Intended purpose and forseeable use of the SE

- **Intended purpose**:
  - **Capability 1**: retrieval and communication of the sensitive information from and through the secure element's interfaces
  - **Capability 2**: processing of these information, which includes performance of computational and cryptographic operations
  - **Capability 3**: secure storage of retrieved and/or processed information

- **Forseeable use** (clasification):
  - **Use case 1**:
    - Function 1.1
    - Function 1.2
    - …
  - **Use case 2**:
    - Function 2.1
    - Function 2.2
    - …
  - …

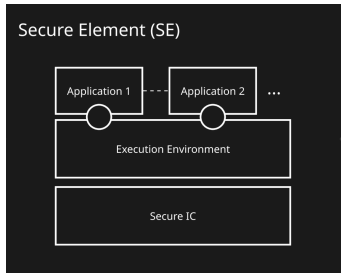
Concrete example in 2 slides from now.

Some (but not all) use cases

- Secure Identification
  - Governmental ID: cards & booklets
  - Governmental ID: mobile
  - UICC access to mobile network
  - …
- Access Control
  - Logical
  - Physical
  - Network
- Payment
  - Open loop, closed loop
  - Card, Mobile
- Digital Singatures in private sector
- IoT
- Automated Fare Collection
- …

The list of use cases cannot be finite.

Example:



Intended purpose

Logical access control use case

Capability:
Secure communication

Capability:
Crypto computation

Capability:
Secure storage

Function
User authentication

Function
Credential management

Function
Attestation

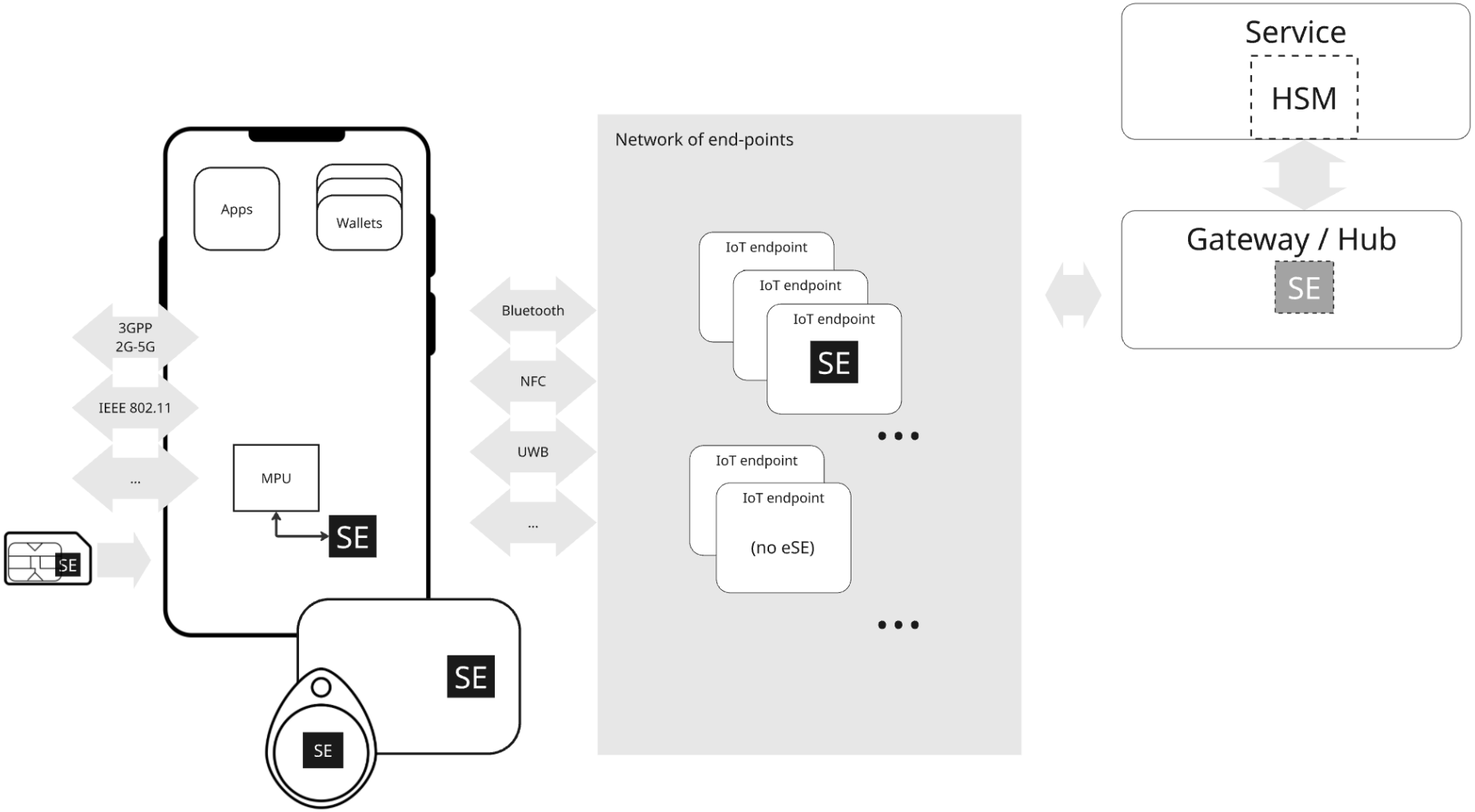
Function
TRNG

Function
...

Function
...

The system

Where to find SE in real life


Service
HSM
Gateway / Hub
SE
Network of end-points
IoT endpoint
IoT endpoint
IoT endpoint
SE
IoT endpoint
IoT endpoint
(no eSE)
Bluetooth
NFC
UWB
...
Apps
Wallets
3GPP
2G-5G
IEEE 802.11
...
MPU
SE
SE
SE
SE

Architectures

… the **Product**

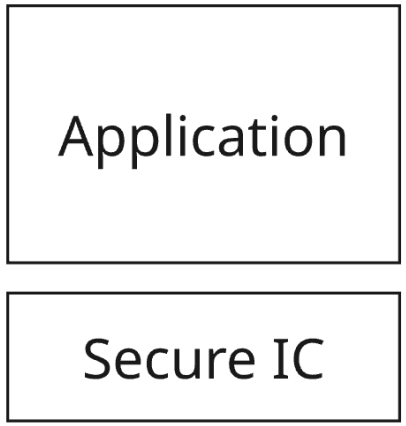
Application

…at least a Java Card applet but it can be the full native implementation

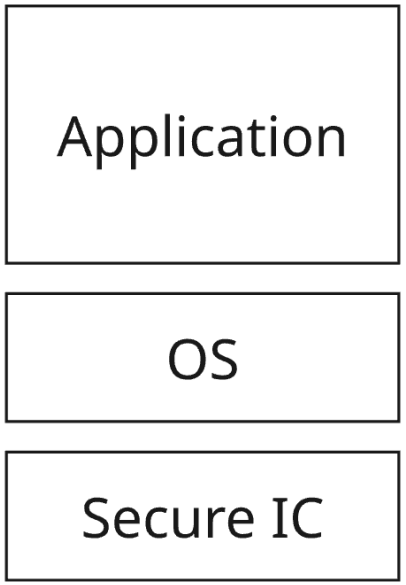
Platform

Secure IC + at least a bootloader but it can be the full operating system

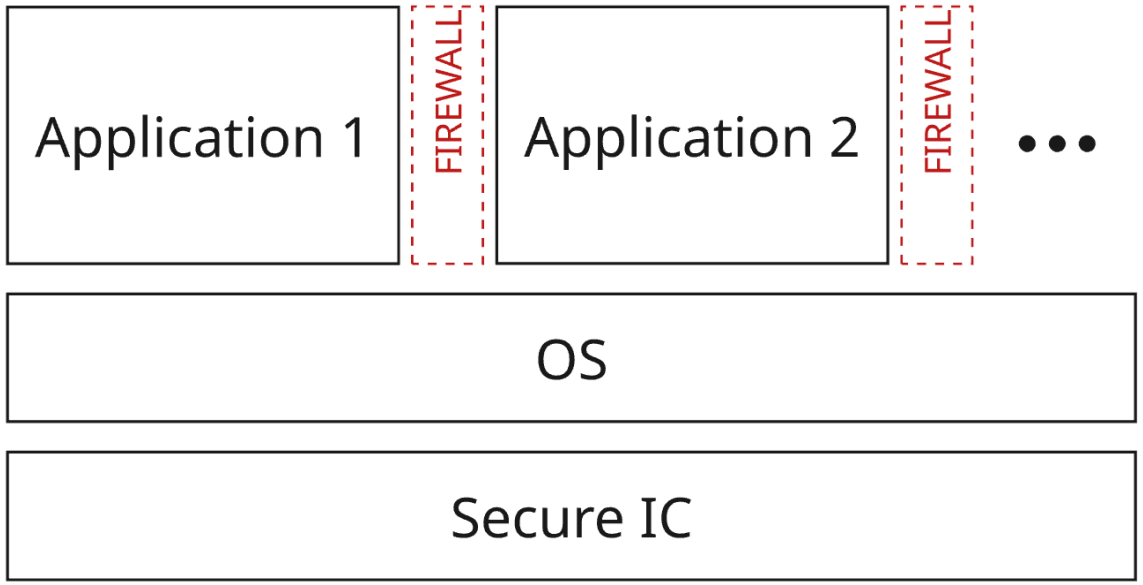
Possibility 1: Application directly implemented on the secure IC



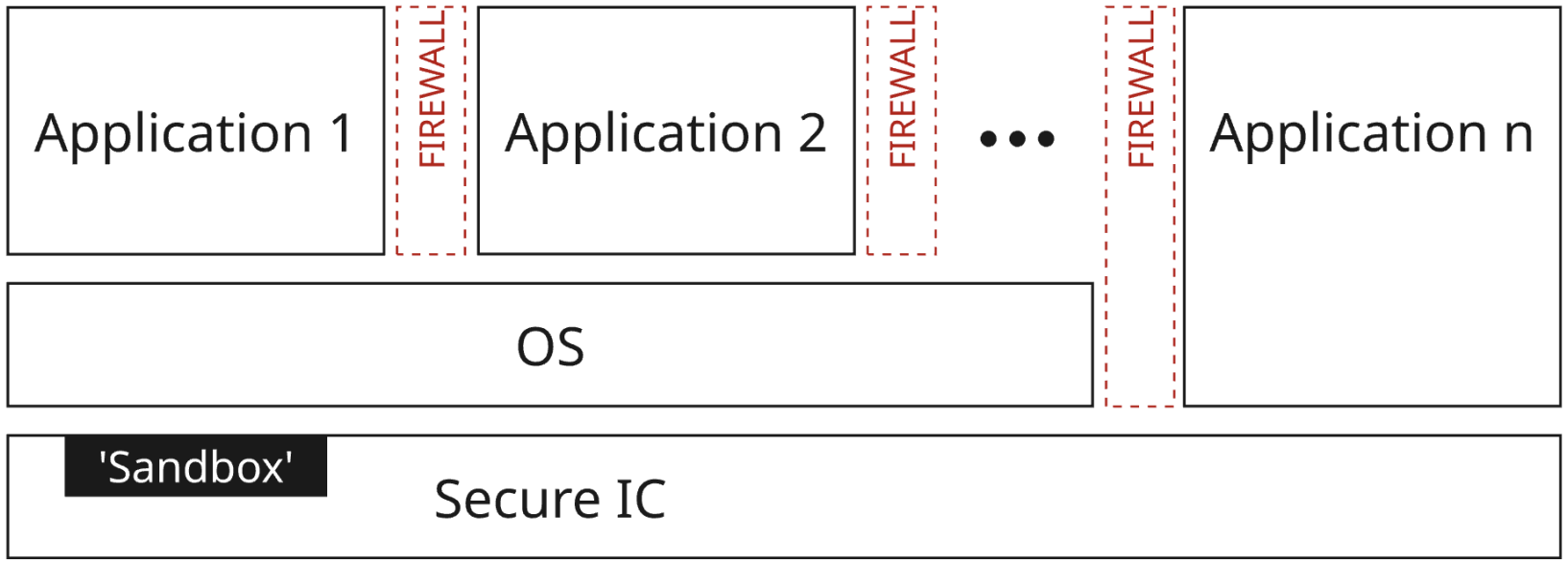
Possibility 2: Application + OS + secure IC



Possibility 3: Multi-application



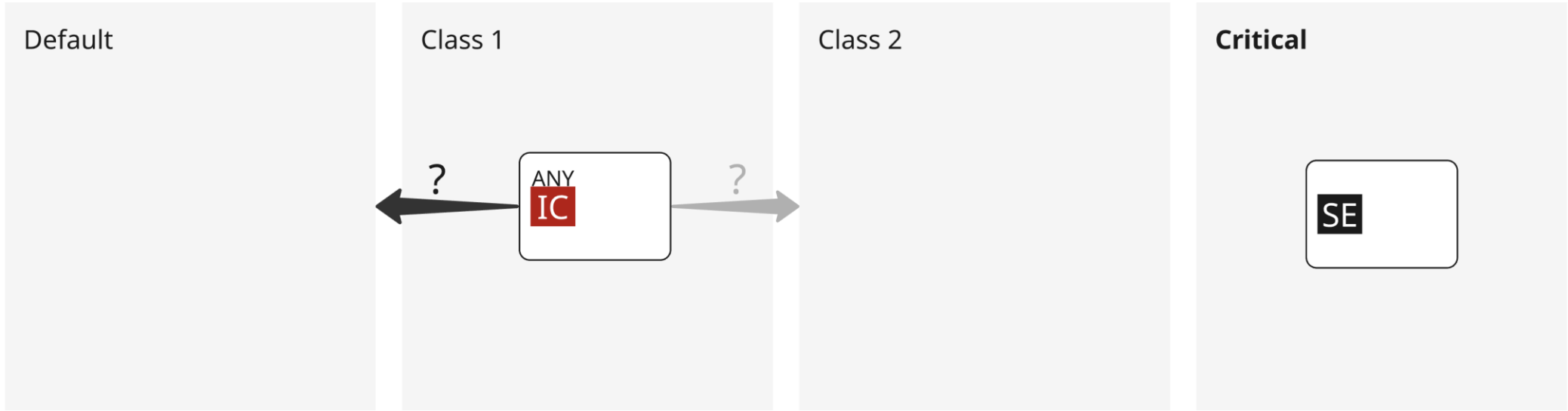
Possibility 4: ‘hybrids’



Out of scope

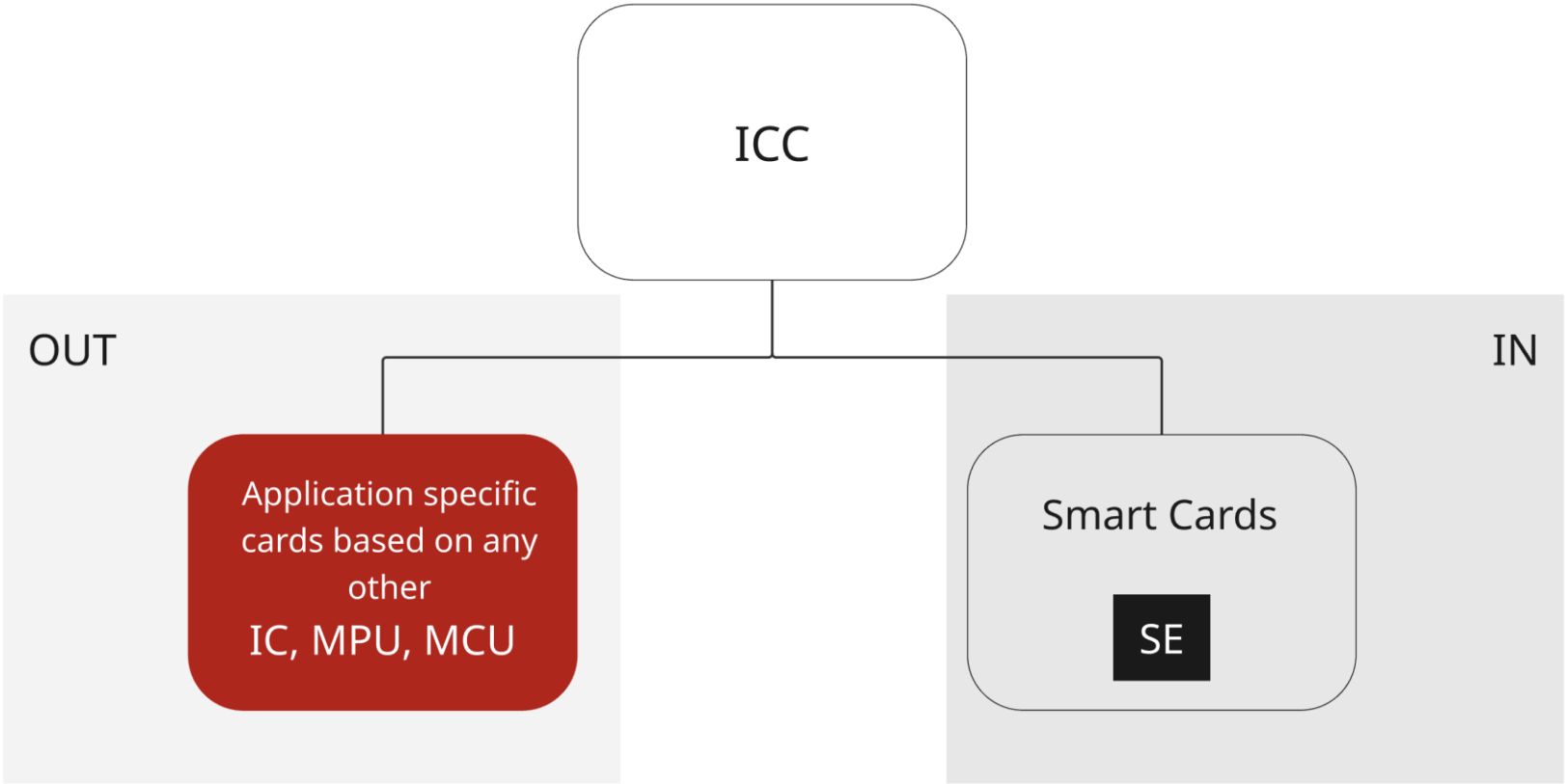
...of this standard...

What is not in the scope of this standard?

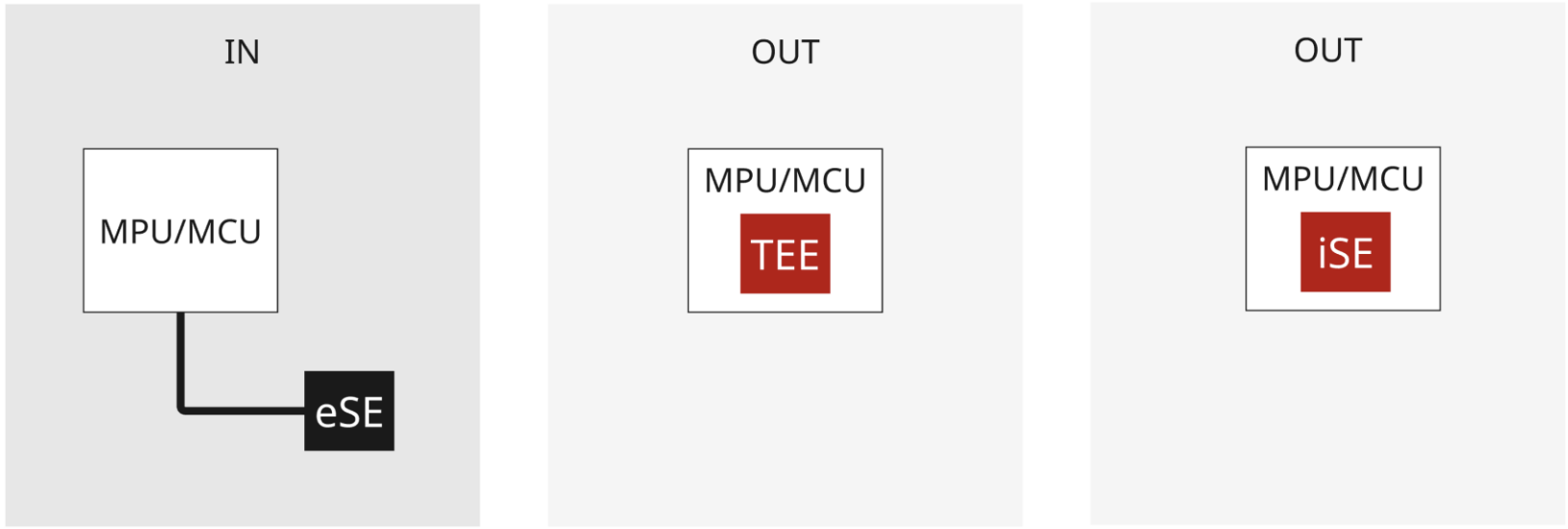


There are use-case-specific cards without (the need for) Secure Elements.

A little bit more formally …



What is also not in the scope of this standard?



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

CRA & Product’s lifecycle

Activities expected in each phase

CRA compliance & Product Life Cycle

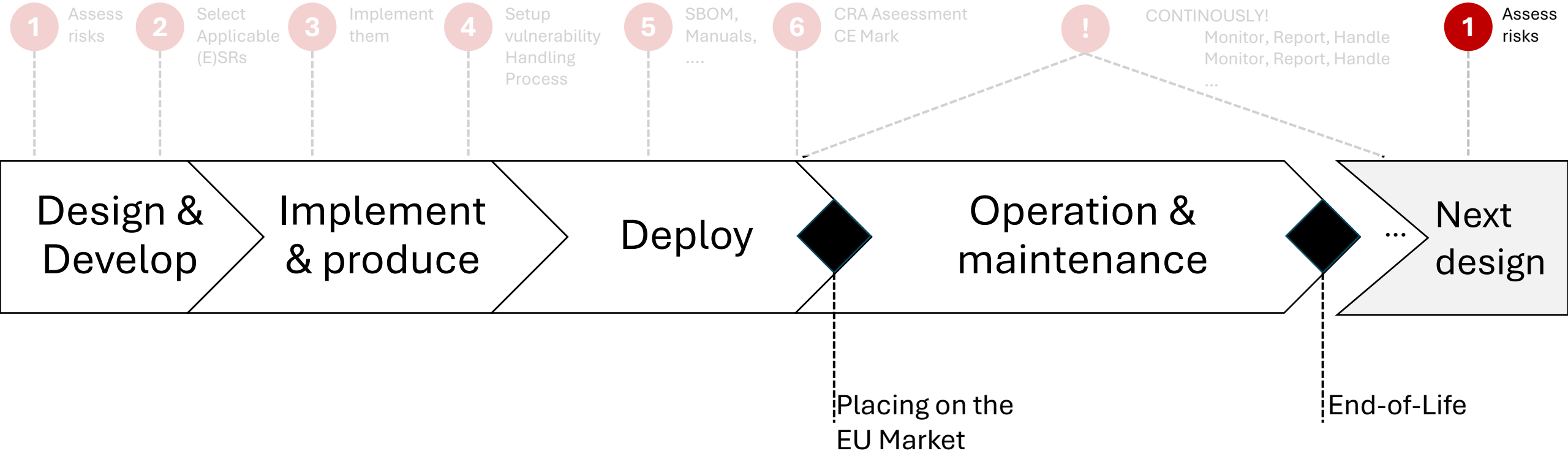
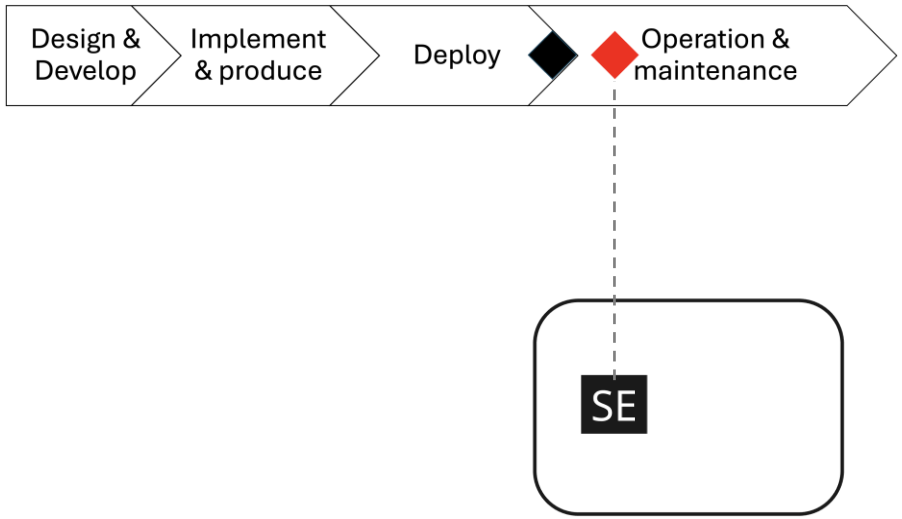
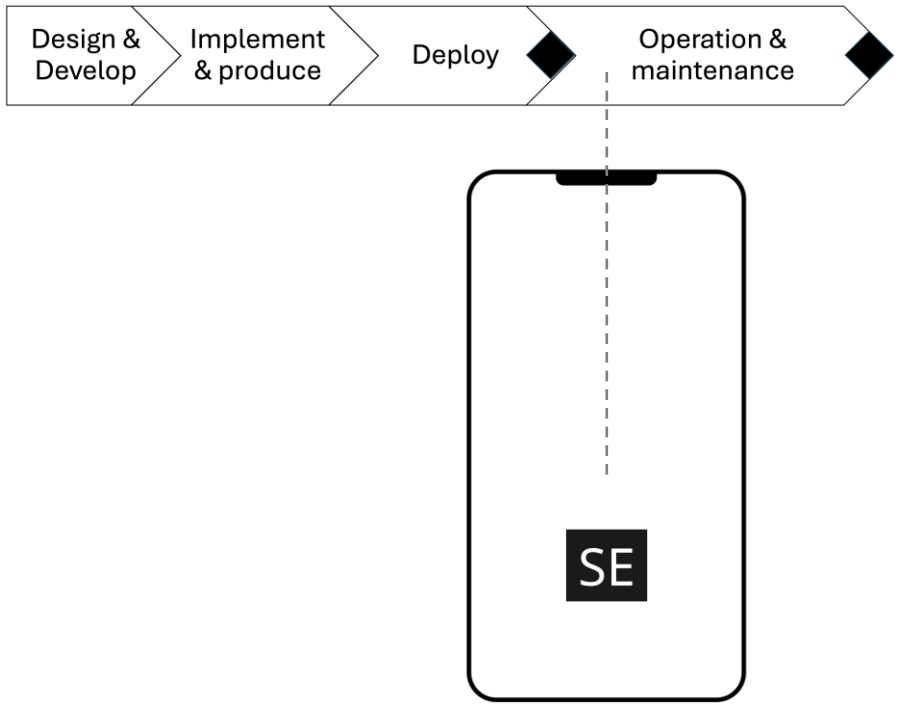


*illustration based on M. Wolf (BOSCH Security), presentation given on the IoT Cyber Compliance Day | Brussels | 2025-03-25

LCM – an example of practical differences related to application on the SE





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**.

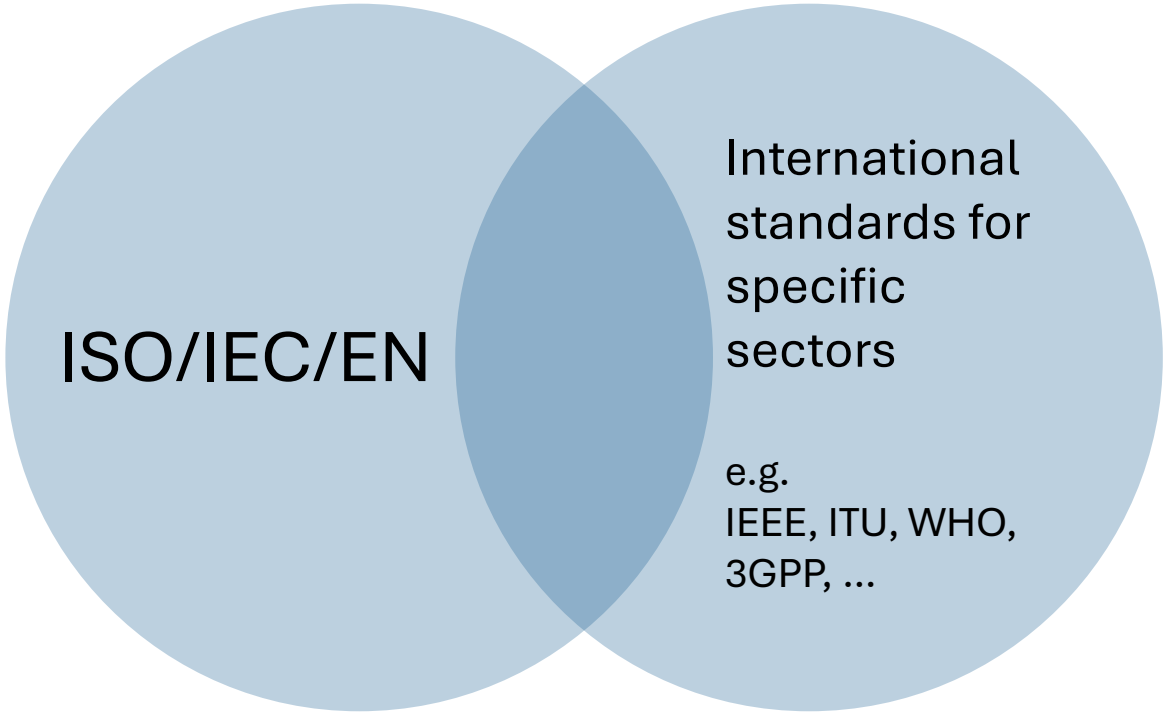
Structure

... of this standard

Chapters in this standard (preliminary)

1. Scope
2. Normative references
3. Definitions
4. Product context
   - 4.1 Intended purpose & foreseeable use
   - 4.2 Product Functions
   - 4.3 Product Architecture
   - 4.4 Operational Environment
   - 4.5 Distribution of security functions
   - 4.6 Users
   - 4.7 Use cases
5. Requirements
6. Conformity assesment
7. Annex(es)
8. Bibliography

Normative references - principle



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

Normative references for this standard

Normative (→ state of the art)

ISO/IEC **15408:2022-2**, Information security, cybersecurity and privacy protection — Evaluation criteria for IT security - Part 2: **Security functional components**

ISO/IEC **15408:2022-3**, Information security, cybersecurity and privacy protection — Evaluation criteria for IT security - Part 3: **Security assurance components**

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*

Other key references

- ECCG – ACM
- Smartcards – ISO/IEC 7816
- Other CRA vertical standards
- ENISA CRA-via-EUCC documents

- Use cases
  - eUICC
  - Payment
  - ePassports & eID
  - Mobile and IoT eSE

- Looking into
  - Global Platform aspects on SE for EUDI wallet application

Risk assessment principles

reminder from the webinar on 2025-07-25

Risk assessment – within the SE / Smart Card industry

Preliminary, subject to change

Level of threat	Level of severity	Risk profile

T2

High attack potential

ISO/IEC 15408:2022

T1

Moderate attack potential

ISO/IEC 15408:2022

S3

At risk: S2 + personal and/or member state and/or organizational **safety**

Impact: Confidentiality, integrity, or availability of data or systems

Mitigation: Mitigation and recovery may not be fully achievable

S2

At risk: S1 + significant value of assets and organizational data **privacy**

Impact: Substantial

Mitigation: Requires enhanced security controls and significant effort

S1

At risk: **Value** of personal and/or business assets, personal privacy

Impact: Limited

Mitigation: Achievable through standard security and recovery measures

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

Severity levels: relation to use cases – one example

ICAO9303
EAC

ICAO9303
BAC

S3

S2
+ organizational data privacy
+ safety of people / organizations / member states

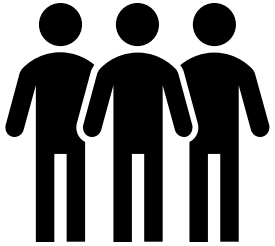
S2

S1
+ organizational data privacy
+ significant value of organizational + personal assets

S1

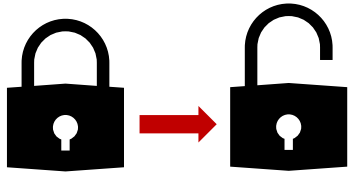
Personal privacy
Value of organizational + personal assets

Attack potential



Who could attack?

Does this individual/group/institution have
- Knowledge about the product?
- Access to the product?
- Access to documentation about the product?
- Equipment?
- Time to attack?



What would be attacked?

Where in the lifecycle is this product?
- Sample (open, protected)
- Product without personal data
- Product that is personalized
- Pre- or post-security update
- Security by design
- Open interfaces
- …

Informative reading: https://certification.enisa.europa.eu/publications/application-attack-potential-smartcards_en

Attack potential – example calculation

Elapsed time		
Factors	Identification	Exploitation
< one hour	0	0
< one day	1	3
< one week	2	4
< one month	3	6
> one month	5	8
> four months 8	6	10
Not practical		

Access to the TOE		
Factors	Identification	Exploitation
< 30 samples	1	2
< 100 samples	2	4
> 100 samples	3	6
Not practical		

Equipment		
Factors	Identification	Exploitation
None	0	0
Standard	1	2
Specialized	3	4
Bespoke	5	6
Multiple Bespoke	7	8

Expertise		
Factors	Identification	Exploitation
Layman	0	0
Proficient	2	2
Expert	5	4
Multiple Expert	7	6

Knowledge of the TOE		
Factors	Identification	Exploitation
Public	0	0
Restricted	2	2
Sensitive	4	3
Critical	6	5
Critical+	9	
Not practical		

Open samples / Samples with known secrets		
Factors	Identification	Exploitation
Public/Not required	0	NA
Restricted	2	NA
Sensitive	5	NA
Critical	9	NA
Not practical		NA

Let's suppose ...

Attack potential score: 33

T2

S3

RP3

Use case: if application is compromised, safetyof employees at stake

AVA_VAN.5
+
Responses to ESR

Details available in ENISA: APPLICATION OF ATTACK POTENTIAL TO SMARTCARDS AND SIMILAR DEVICES, Version 1.2, August 2023

Governmental use cases

ID Cards, electronic/biometric passports, driving licenses, … also on mobile devices.

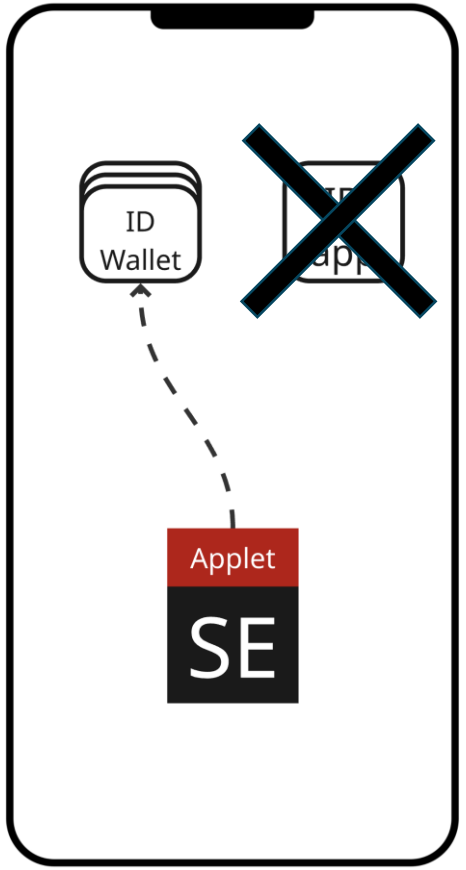
Governmental Official Documents in form of Cards or Booklets

- Passport
- ID Card
- Residence Permit Card
- Driver's License Card
- Health Card
- Vehicle Registration Card
- Tachograph Card
- Qualified Signature Card

- ID cards for government officials (police, military, financial sector, notaries, lawyers, medical professionals, etc)
- Work Permit Card
- Student Cards
- Weapon License Card
- …

Governmental Applications on Mobile Devices SE

- EUDI wallet
- Mobile ID / ICAO DTC
- Mobile (qualified) Signature
- Mobile Driving License
- Mobile Vehicle Registration
- Mobile Health Cards
- …



Governmental Official Documents – Current Situation

- Security certification of cards and similar devices for more than 25 years
- Highest security assurance levels in the certification market, EAL4+ to EAL 6+

Governmental Use Cases - Protection Profiles

Document Type	Common Specifications	EU Type Approval	PP available
Passport / ID Card	Yes		Yes, mandatory (*)
Residence Permit Card	Yes		Yes, mandatory
Driver's License Card		Yes	(Yes, optional)
Tachograph Card	Yes	Yes	Yes, mandatory
Qualified Signature Card	Yes		Yes, mandatory
Health Card	limited (EHIC), (1)		National solutions, few PPs exist (2)
Vehicle Registration Card	Yes		(3)
Smart Meter Gateway Security Module			Yes

(1) beside EHIC different functional implementations in many countries which are not interoperable

(2) few different national PPs

(3) no demand for security certification till now

(*) certification of ICAO BAC protocol is the only agreed exception from the AVA_VAN 4/5 requirement

Essential security requirements (CRA Annex I, part I)

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*

…reset to original state…
…vulnerability addressed by updates …
…opt-out …
…data minimization…
…remove & transfer data …

Less possible for cards.
Maybe on SE in mobiles.

Essential security requirements (CRA Annex I, part II)

PP / ST may need to be updated!

… identify and document vulnerabilities…
… disclose vulnerabilities…
… publish fixed vulnerabilities …
…support 3rd party reporting …

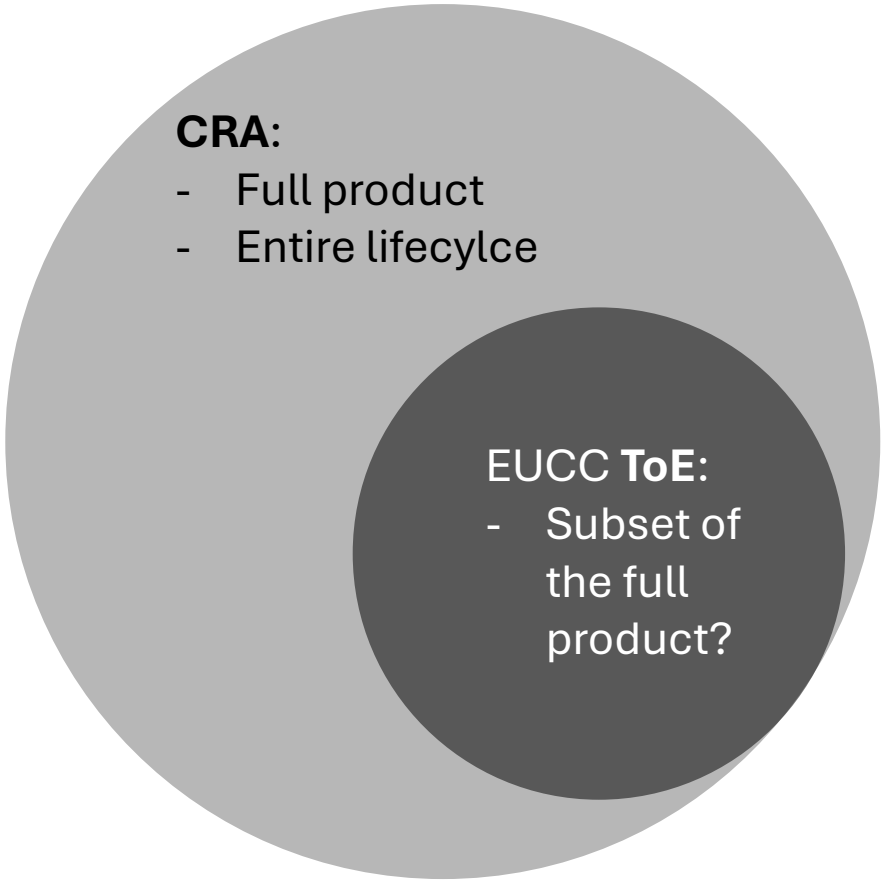
1. Identify and document components and vulnerabilities
2. Address vulnerabilities
3. Perform regular security testing
4. Publish fixed vulnerabilities
5. Implement and practice vulnerability disclosure policy
6. Support 3rd party reporting
7. Ensure secure distribution of updates
8. Dissemination of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

Requirements on vulnerability handling

Handling of GAPs – Update of PP/ST

ENISA Report *"Cyber Resilience Act implementation via EUCC and its applicable technical elements"*, published February 2025

CRA compliance via EUCC – the (potential) gap



ToE may have a focus on less than what is in the scope of the CRA.

Manufacturer should examine harmonized standard(s) and additional documentation.

Gaps are to be closed by new or updated Security Target / Protection Profile.

Otherwise, presumption of CRA conformity cannot be claimed.

CRA compliance requirements

...on applications on Secure Elements

CRA assessment vs. Evaluation vs. Certification – **important**

CRA compliance **does not** mandate any type of security evaluation & certification.

Including (EU)CC .

But the ‚other way around' – obtaining the *presumption of conformity* after an accomplished certification (for now only EUCC!) evaluation and certification is a viable option.

Just **mind the gap** there!

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 properties

Product 1: Security by design

Preliminary, subject to change

Description and activities:	
Security analysis of the application, determine the target risk environment and define the security problem in terms of threats and assumptions for operational environment specific to the application. The application manufacturer identifies and implements the applicable security requirements for their application.	ECCG Agreed Crypto Methodologies ISO/IEC 15408-3:2022: ASE_INT.1 for applications overview, reference, description ASE_SPD.1 defines security problems that application may encounter ASE_OBJ.2 for security objectives of the application itself ASE_REQ.1 defining security requirements of the application

Applicability:
Mandatory

Product 2: No known vulnerabilities

Preliminary, subject to change

Description and activities:	
Addressing known vulnerabilities including the ones described in ENISA vulnerability database, either by mitigating their exploitation by attackers with up to significant resources and skills.	ISO/IEC 15408-3:2022: AVA_VAN.4 Methodical vulnerability analisys AVA_VAN.5 Advanced methodical vulnerability analisys

Applicability:
Mandatory

Product 3: Secure by default when placed on EU market

Preliminary, subject to change

Description and activities:	
The default configuration of the application is secure, minimizing the need for end-user intervention to achieve a secure state. This includes disabling unnecessary services and interfaces, enforcing strong authentication and access controls, and enabling security features by default. Application also offers the ability to perform a factory reset command to enable the ability to restore the product to its original, secure-by-default state.	ISO/IEC 15408-3:2022: ADV_ARC.2 defining application functional specification with complete summary ISO/IEC 15408-3:2022: ADV_FSP.2 Security-enforcing functional specification ADV_TDS.1 Basic design FMT_SMF.1 specifying applications management fuctions

Preliminary, subject to change

Applicability:

Mandatory

Exceptions are possible for:

- tailor-made products under condition that exception is agreed by the **users** of such products
- operational environments where factory reset is not possible, in particular for smart card applications

Alternatives to FMT_SMF.1 may be chosen, for as long as they ensure at least equivalent specification of the application configuration management functions.

Product 4: Security updates

Preliminary, subject to change

Description and activities:	
A secure update mechanism must verify authenticity and integrity using SOTA cryptography, prevent unauthorised changes, and support rollback or recovery. Security updates shall be automated, with an opt-out feature for authorised users.	ECCG Agreed Crypto Methodologies EUCC Version 1.1.1 form May 2021 Annex 15, Patch management ISO/IEC 15408-3:2022: ALC_DEL.1, ALC_FLR.3, AGD_OPE.1, AGD_PRE.1, ADV_FSP.2, ADV_TDS.2 ENISA: CRAimplementation via EUCC, 2025-01-27 ALC_FLR.4

Applicability:

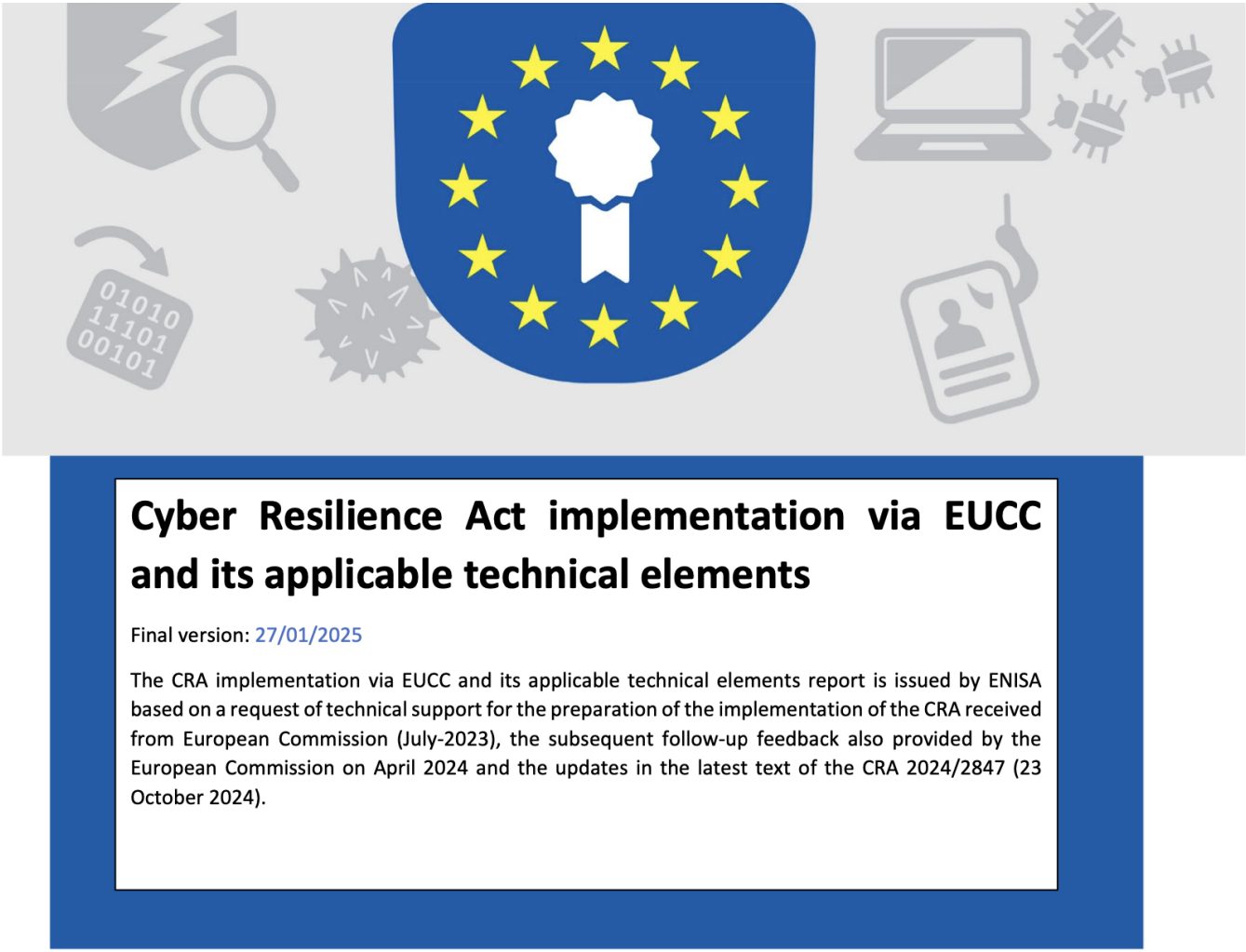
Mandtory;

Vulnerabilities shall be addressed through the replacement for the Product or through security updates, including, where applicable, through automatic security updates.

Introducing….

ENISA study / final version about CRA implementation via EUCC.

Annex to this document is aiming to close some gaps between Common Critieria and CRA requirements.



Product 5: Access control (to PwDE)

Preliminary, subject to change

Description and activities:	
A set of mechanisms to prevent unauthorized access to applications resources, data, and functionalities. This includes implementing robust authentication, access control policies, session management, and protection of sensitive data in storage and transit.	ISO/IEC 15408-3:2022: FIA_UAU.1, FIA_UID.1, FAU_SAA.1, FAU_STG.1, AGD_OPE.1 AGD_PRE.1, ADV_FSP.2, ADV_TDS.1, ALC_CMC.5, ATE_IND.2

Applicability:
Mandatory; If a reliable timing source is not available in a system with a Secure Element, notifications of unauthorized access events and logging related information can be performed in a sequential order, without reference to the actual time when the events occurred. Alternatives to FIA_UAU.1, FIA_UID.1, FAU_SAA.1, FAU_STG.1 may be proposed, for as long as they ensure at least equivalent security functionality.

Product 6: Confidentiality protection

Preliminary, subject to change

Description and activities:	
Ensure the confidentiality of applications sensitive data during storage, processing, and in transit. This includes the use of the SOTA cryptographic mechanisms to protect data from unauthorized disclosure, enforcement of access controls, and secure handling of cryptographic keys.	ISO/IEC 15408-3:2022: FDP_SDC.1, FCS_COP.1, ADV_FSP.2, ADT_TDS.1 ENISA: CRA implementation via EUCC, 2025-01-27 FTP_TRP.1

Applicability:
Mandatory; Alternatives to FDP_SDC.1, FCS_COP.1 may be chosen, for as long as they ensure at least equivalent security functionality.

Product 7: Integritiy protection

Preliminary, subject to change

Description and activities:	
Ensure the application maintains data integrity during storage, processing, and transmission. Uses SOTA cryptographic methods and other techniques such as checksums, CRC, ECC, redundancy, replication, and version audit verification to detect and prevent unauthorized or accidental data changes.	ECCG Agreed Crypto Methodologies ISO/IEC 15408-3:2022: FDP_SDI.1, FAU_GEN.1, FDP_SDI.2, FTP_ITC.1, FTP_TRP.1, FCS_COP.1, ADV_FSP.2, ADT_TDS.1

Applicability:

Mandatory;

Alternatives to FDP_SDI.1, FAU_GEN.1, FDP_SDI.2, FTP_ITC.1, FTP_TRP.1, FCS_COP.1 may be chosen, for as long as they ensure at least equivalent security functionality.

Product 8: Data minimization

Preliminary, subject to change

Description and activities:	
Ensure that application processes only personal and other data that are adequate, relevant, and limited to what is necessary in relation to the intended purpose of the product with digital elements. This includes implementing controls, such as but not limited to data collection restriction, purpose limitation enforcement, data retention and sharing and sharing limitations	ENISA: CRAimplementation via EUCC, 2025-01-27 ADV_PDM.1

Applicability:
Mandatory; An alternative to ADV_PDM.1 may be chosen, for as long as the proposed alternative provides equivalent or better data minimization method.

Product 9: Basic functionality available despite of incident

Preliminary, subject to change

Description and activities:	
Ensures that essential functions remain available, even after security incidents, by implementing resilience measures like redundancy, failover, backups, load balancing, automated recovery, incident response, and protection against DoS/DDoS attacks	ISO/IEC 15408-3:2022: FRU_FLT.2, ADV_FSP.2, ADT_TDS.1

Applicability:
Mandatory; A security incident may temporarily or permanently stop certain functions, but such interruptions are considered to be basic, specified features. An alternative to FRU_FLT.2 may be chosen, for as long as the proposed alternative provides equivalent or better method for assurance of essential and basic functionality.

Product 10: Minimize negative impact around PwDE

Preliminary, subject to change

Description and activities:	
The application must be designed to prevent disruptions to other connected devices or networks by managing resource use, controlling traffic, and implementing safeguards against interference and failures. Mechanisms may include: ▪ Asset management and isolation (e.g., sandboxing, memory quotas, secure channels) ▪ Communication controls (command rate limits, integrity checks, flood detection) ▪ Fault detection and mitigation (error checking, rollback mechanisms) ▪ Redundancy and recovery (state validation, redundant storage, fail-safe defaults)	ISO/IEC 15408-3:2022: FPT_INI.1, FPT_TST.1, ADV_FSP.2, ADV_TDS, ADV_ARC.1

Preliminary, subject to change

Applicability:

Mandatory;

Alternatives to FPT_INI.1, FPT_TST.1 may be chosen, for as long as the proposed alternative provides equivalent or better method for minimization of service disruption.

Product 11: Limit attack surface

Preliminary, subject to change

Description and activities:	
Ensure the application is designed to minimise its attack surface by reducing exposed interfaces, disabling unnecessary services and ports, enforcing strict input validation, and isolating critical components. Protect external interfaces using authentication, access control, and secure communication protocols.	ISO/IEC 15408-3:2022: ADV_FSP.2, AGD_PRE.1, AGD_OPE.1
Applicability:	
Mandatory	

Product 12: Mitigation of incidents

Preliminary, subject to change

Description and activities:	
Ensures that the application is designed and developed to minimise security risks by including exploitation mitigation techniques such as memory protection, sandboxing, privilege separation, secure coding, runtime protections, and attack sensory modules, as guided by platform documentation. These measures should restrict attackers' ability to escalate privileges, persist, or move laterally within the system, even if a vulnerability is exploited.	ISO/IEC 15408-3:2022: FPT_FLS.1, FPT_RCV.2, ADV_FSP.2, ADV_TDS., ADV_ARC.1

Applicability:
Mandatory; An alternative to FPT_FLS.1 and FPT_RCV.2 can be chosen, for as long as the proposed alternative provides equivalent or better method for mitigation of the incident impact.

Product 13: Recording & monitoring

Preliminary, subject to change

Description and activities:	
Ensure recording and monitoring of relevant application-internal activities, including access to or modification of data, services, or functions. This logging capability shall support security auditing, incident detection, and forensic analysis. The system shall provide users with a clear and accessible opt-out mechanism for non-essential monitoring, in compliance with privacy and data protection regulations.	ISO/IEC 15408-3:2022: FAU_GEN.1, FMT_SMF.1, FMT_SMR.1, ADV_FSP.2, ADV_TDS.1, ADV_ARC.1

Applicability:

Mandatory;

An alternative to FPT_FLS.1 and FPT_RCV.2 can be chosen, for as long as the proposed alternative provides equivalent or better method for mitigation of the incident impact.

Preliminary, subject to change

Applicability:

Mandatory;

Exceptions regarding the recording and monitoring may be considered only for cases where monitoring of application-internal activities would exhaust computational, communication and storage resources of the application environment (chip / OS platform) in the way that would violate compliance to CRA ESR 9 (Esential and basic functions) and 10 (Minimize service disruption)

Exceptions from the opt-out-mechanism may be tolerated only in cases of applications where users:

- don’t own the application and Secure Element (example: governmental ID cards, MRTD) or the data in question
- access to applications functionality is permanently prevented for security reasons (example: read-only smart cards), in which case user may physically destroy the Secure Element

An alternative to FAU_GEN.1, FMT_SMF.1, FMT_SMR.1 for as long as the proposed alternative provides equivalent or better method monitoring of the security activities.

Product 14: Deletion of data & settings by end-user

Preliminary, subject to change

Description and activities:	
Provides users with the ability to securely and easily delete all personal data and settings stored in application on a permanent basis. Where applicable, the application shall also support the secure transfer of such data to other products or systems, ensuring confidentiality and integrity during the transfer process.	ISO/IEC 15408-3:2022: FMT_SMF.1, FDP_RIP.1, FDP_ETC.2, FTP_ITC.1, ADV_FSP.2, ADV_TDS.1

Preliminary, subject to change

Applicability:

Mandatory;

Exceptions may be tolerated only in cases of applications where users:

- don’t own the application and Secure Element (example: governmental ID cards, MRTD) or the data in question
- access to applications functionality is permanently prevented for security reasons (example: read-only smart cards)
- may physically destroy the Secure Element

An alternative to FMT_SMF.1, FDP_RIP.1, FDP_ETC.2, FTP_ITC.1 may be chosen, for as long as the proposed alternative provides equivalent or better secure erasure method.

Vulnerability handling

Vulnerability handling 1: Identify and document components and vulnerabilities

Preliminary, subject to change

Description and activities:	
Maintain an up-to-date list of vulnerabilities and all application-related software components (SBOM) in the application on the Secure Element, whether the application is installed at launch or added later. Keep the SBOM current, update it with security changes, and use it to track and assess vulnerabilities throughout the product lifecycle.	ENISA: CRAimplementation via EUCC, 2025-01-27 ALC_SBM.1 Optionally also: Joined Interpretation Library, Security Architecture Requirements, Appendix 1, ADV_ARC, Version 2.1, July 2021
Applicability:	
Mandatory;	

Vulnerability handling 2: Address vulnerabilities

Preliminary, subject to change

Description and activities:	
Shall establish procedures for timely remediation of vulnerabilities and issuance of application related security updates. Where technically feasible, these updates should be applied independently from the new or enhanced functional updates. In circumstances where automated updates are not feasible, security updates may be implemented through a replacement of the SE or a device containing SE.	ISO/IEC 15408-3:2022 ALC_FLR.3 that mandates systematic flaw remediation ENISA: CRA implementation via EUCC, 2025-01-27 ALC_FLR.4

Applicability:
Mandatory;

Vulnerability handling 3: Perform regular security testing

Preliminary, subject to change

Description and activities:	
Performing regular security reviews and tests of the application until the end-of-life of the application on the Secure Element, smart card or a similar device, after their placement on the EU market, which predicates CRA compliance.	ENISA: CRA implementation via EUCC, 2025-01-27 ALC_PSR.1

Applicability:
Mandatory;

Vulnerability handling 4: Publish fixed vulnerabilities

Preliminary, subject to change

Description and activities:

Disclosures must include a detailed vulnerability description, impact and severity estimation, identification procedure for affected applications, and clear remediation steps.

Public disclosure should occur as soon as security updates are available.

If immediate disclosure would reduce security benefits, in alignment with manufacturers of SEs, smart cards, or similar devices disclosure may be delayed – but only for a defined period after documenting the reason and notifying the new disclosure date.

Applicability:

Mandatory;

Vulnerability handling 5: Implement and practice vulnerability disclosure

Preliminary, subject to change

Description and activities:

Define and implement a coordinated vulnerability disclosure policy prior to the placement of the SE application on the market.

Applicability:

Mandatory;

Vulnerability handling 6: Support 3rd party reporting

Preliminary, subject to change

Description and activities:	
Establish and maintain clear, publicly accessible channels through which vulnerabilities in their products or in included third-party components can be reported, Implement effective processes to triage, track, and resolve reported vulnerabilities in a timely and organized manner.	ISO/IEC 15408-3:2022 ALC_FLR.2 that regulates flaw reporting procedure from users to the manufacturer

Applicability:
Mandatory;

Vulnerability handling 7: Ensure secure distribution of updates

Preliminary, subject to change

Description and activities:	
Implement own or use an existing mechanism for a secure distribution of security updates. Provide guidance to integrators and service providers on secure update deployment, status monitoring, and verification of applied updates	ISO/IEC 15408-3:2022 ALC_FLR.3 that mandates systematic flaw remediation

Applicability:
Mandatory;

Vulnerability handling 8: Dissemination of updates

Preliminary, subject to change

Description and activities:

distribute security updates promptly and free of charge, ensuring they are accompanied by clear advisory messages explaining the update, providing mechanisms to identify affected products, and support for required actions to apply them.

The free of charge obligation may not include cost of the service or device replacement; it is narrowed only to the cost of the security update.

Applicability:

Mandatory, for all cases except for tailor-made products.

Additional requirements

Definition in progress

Requirements on remote data processing solutions	Requirements on product composition	Requirements on application manufacturer environment security
• Contact, contactless, wireless to any device communication • Direct connection to MPU/MCU (in compositions) • Indirect to on-premise or cloud service	• SW composition – application on platform • SE composition, as a component in other products	• Security maturity • Development • Operations

JOIN OUR WORK!

Accellerating towards completion:

- Field experts welcome to join via national standardization bodies

Q&A

Presentation will be uploaded for consultation and we will appreciate detiled comments.

Thank you!

CEN/CENELEC TC224 WG17, Task Force 41b