European Standardization Organizations

CRA Standards Unlocked: Cybersecurity Requirements for Hardware Devices with Security Boxes

We start at 11:00 CET

Webinar moderator

Lucia LANFRI

Project Manager

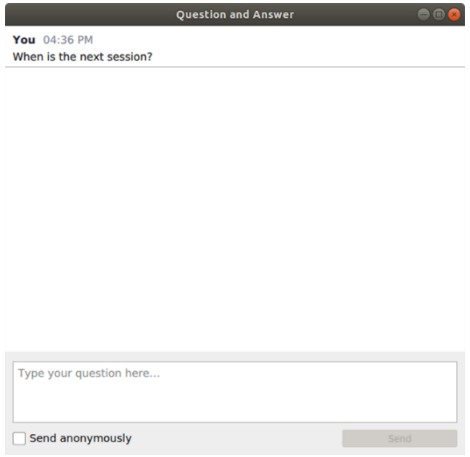
Electrotechnology

CEN-CENELEC

llanfri@cencenelec.eu

Get the most out of the webinar today

- You are muted
- Use the Q&A panel to submit your questions



- Talk about us with #training4standards #standards4CRA
  - On X @Standards4EU
  - On Bluesky @cen-cenelec.bsky.social
  - On LinkedIn www.linkedin.com/company/cen-and-cenelec

Your speaker today

Claire Loiseaux

Rapporteur CEN/TC 224 WG 17, work item for Line 39: Cybersecurity Requirements for Hardware Devices with Security Boxes

Agenda

- Introduction to the standard
- Scope of “HWSB”
- Challenges

- Architecture and main functions
- Security problem definition and Risk profiles
- Use cases

- Requirements
- Assessments
- Mapping with Essential requirements (Annex ZA)

- Next steps

Overview

- Annex I of the European Commission's standardisation request (41 standards)
- Standard n°39 developed in CEN/TC 224 WG17 under the CENELEC STAN4CR Project
- Definition from CRA Revised Annex 1.12.2025

ANNEX II

CRITICAL PRODUCTS WITH DIGITAL ELEMENTS

Category of product	Technical description
1. Hardware Devices with Security Boxes	Hardware products with digital elements that securely store, process, or manage sensitive data or perform cryptographic operations, and that consist of multiple discrete components, incorporating a hardware physical envelope providing tamper evidence, resistance or response as countermeasures against physical attacks. This category includes but is not limited to physical payment terminals, hardware security modules that generate and manage cryptographic elements, and tachographs that meet the above description.

Ongoing work

- Initiated in June 2025 (NWI)

- Scope definition
- Expert group sessions
- Cross verticals meetings
- Meetings with commission

- Draft submitted on December 18th, 2025 for commission review

Team

Expert group

Elżbieta Andrukiewicz National Institute of Telecommunications	Dieter Bong Utimaco	Guillaume Cesbron Idemia
Graham Costa Thales	Ignacio Dieguez, Pali Surdhar Entrust	Aivo Kalu Cybernetica AS
Claire Loiseaux (Rapporteur) Internet of Trust	Sebastian Schraml Cherry	Raul Sanchez-Reillo UC3m, ID testing Lab

Supporting team

Aylin Kip Afnor
Lucia Lanfri CENELEC
Marc Le Guin WG 17 convenor TUV-IT

Harmonized standards and CRA

- Compliance to CRA Essential Requirements will be mandatory by December 11th, 2027.
- Harmonized standards support the possible paths to achieve CRA compliance

Start from	Scratch	Security evaluation (CC, FIPS, PCI)	Your own assessments	Module H
Provide	Develop evidence directly from the Harmonized standard	Evaluation evidences + Fill the Gap with the Harmonized standard	Develop mapping and evidences. The Harmonized standard can serve as guideline, deviation possible	Develop the processes. The Harmonized standards can serve as guideline for specific product
CRA evaluation	Direct assessment according to the standard.	Direct assessment according to the standard.	Mapping, evidences and evaluation methodology must be assessed	The generic processes and their applicability to the specific product must be assessed.

Draft Structure

Body

- 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 assessment
- 7. Annexes
- 8. Bibliography

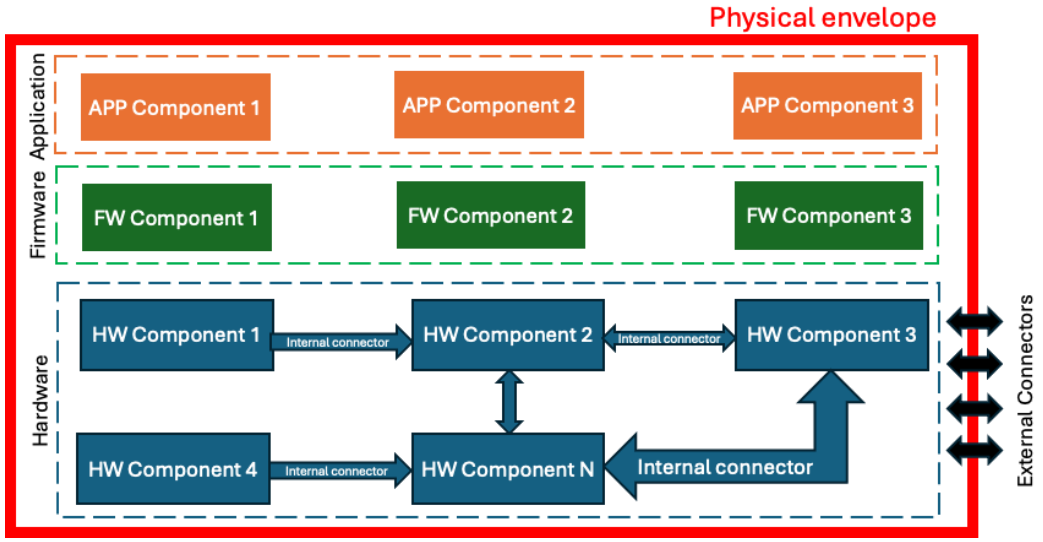
Annexes

- A - Extended SAR and SFR
- B - HWSB functional requirements in CC language
- C - HWSB assurance requirements in CC language
- D - Internal Mappings
- E - Security Problem definition
- F - Risk acceptance criteria and risk management methodology
- G - Life cycle
- H - Relationship with other verticals
- I – Vulnerability handling
- J - Use cases
- K - Cryptographic Algorithms
- L - Security Target
- ZA - Relationship between this European Standard and the essential requirements

What is the HWSB category?

Hardware products with digital elements that

- securely store, process, or manage **sensitive data**
- or perform **cryptographic operations**,
- consist of **multiple discrete components**,
- incorporating a **hardware physical envelope** providing tamper evidence, resistance or response as countermeasures against physical attacks.



Payment terminal

HSM

Tachograph

What is not covered?

- HWSB parts
  - such as a crypto accelerator integrated circuit or empty envelopes are not considered as HWSB.
  - They may be used to build a HWSB, but they are not considered as such in the standard. The compliance to this category will be the responsibility of the integrator that will put the full HWSB on the market. Nevertheless, the integrator may require security properties to meet HWSB CRA requirements.

- Devices with enclosure that do not provide tamper evidence, resistance or response
  - such as enclosure that provide only environmental protection or removable ones
  - They belong to the category of their main functionality

- Secure elements
  - Such as smart cards
  - They belong to another category

What does critical imply?

- It is subject to a 3rd party assessment
- The assessment level depends on the risk profile
- It can be certified against a certification framework, but this is not mandatory unless another regulation mandates it

Challenges

- Existing requirements sets such as Protection Profiles do not include yet CRA Essential Requirements
- Multiple certification schemes, with multiple assurance and security levels apply
- All have fixed risk assessment

- Harmonized standards aim at providing a clear path to presumption of conformity for HWSB

How to formalise Requirements and Assessments

- Reuse EU scheme material
  - Existing sets of requirements (Protection Profiles)
  - Assessment methodologies (CEM and EUCC guidelines and SotA)

- Convert other security framework evidences
  - In sets of EUCC functional and assurance requirements + its extensions defined by ENISA

Normative references

- Common Criteria catalogues
  - 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

- CRA Horizontal standards
  - prEN 40000-1-2 (JT013089), Principles for cyber resilience
  - prEN 40000-1-3 (JT013090), Vulnerability handling

- Annex A Extended SAR and SFR (from ENISA CRA-via-EUCC document)
- Annex K (for cryptographic algorithms)

Other Key references

- ECCG – SotA & Guidance
  - Agreed Cryptographic Mechanisms - ACM [17]
  - Attack methods: JTEMS [1], JHAS [18]

- Protection Profiles
  - HSM [3]
  - POI [11]
  - Tachograph Vehicle unit [14]
  - Others PPs [8], [15], [16]

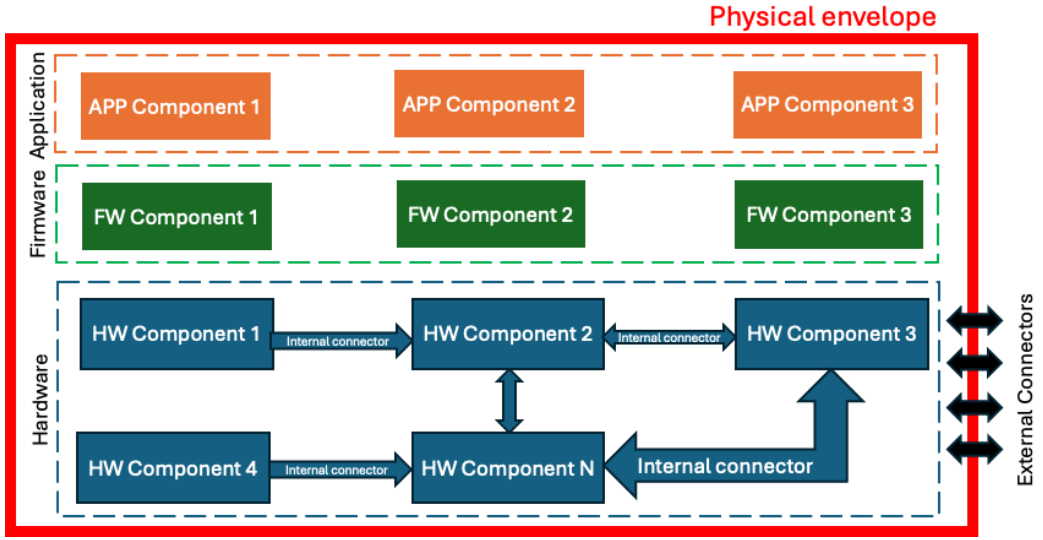
- FIPS 140-X [9, 10, 19]
- PCI – HSM and POI [7, 12]

- Other CRA vertical standards: Smart Meter Gateway, Secure Elements, OS, Boot, PKI Network functions: VPN, firewall,…

Architecture and main possible functions

The generic HWSB is composed of

- **Physical Envelope**
- **External connectors**
- **Hardware components**
- **Internal connectors**
- Firmware components
- Application components

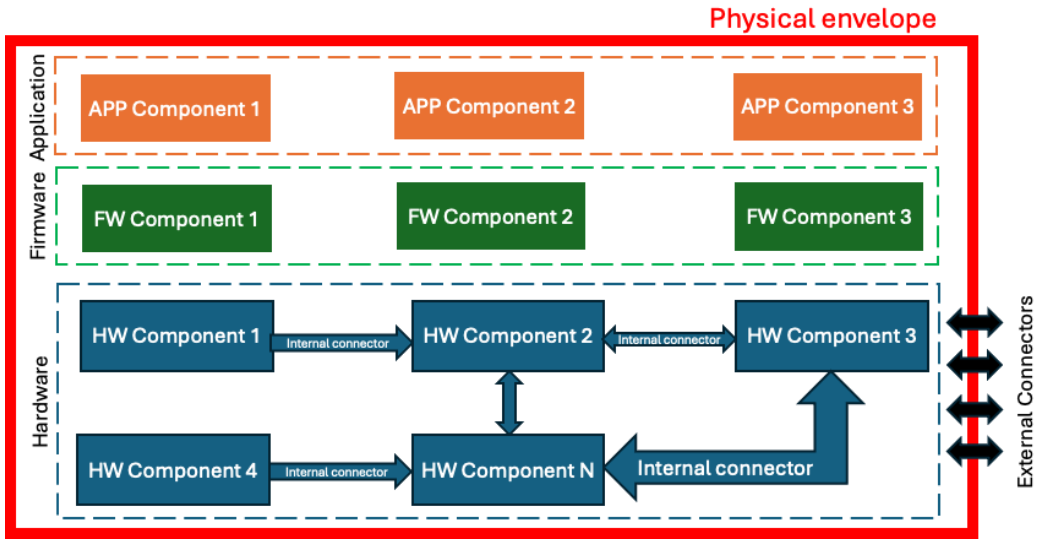


- **The Physical Envelope**
  - Constitutes the Physical Boundary
  - Encloses all components (HW/FW)
- **External connectors**
  - They depend on HWSB Type
  - PCIe, Ethernet, USB, Serial, Smartcard reader, Power socket, Intrusion latch interface
- **HW Components**
  - MCU/MPU, Crypto Processors or engines, Real Time Clock (RTC), RNG.TRNG/DRNG, Memory, FPGA, Tamper controller, Battery, Secure Key Store, Power Control, Buffer
- **Internal Connectors**
  - Internal bus, FPGA (connect MCU/MPU to RNG or other)

Architecture and main possible functions

The generic HWSB is composed of

- Physical Envelope
- External connectors
- Hardware components
- Internal connectors
- **Firmware components**
- Application components



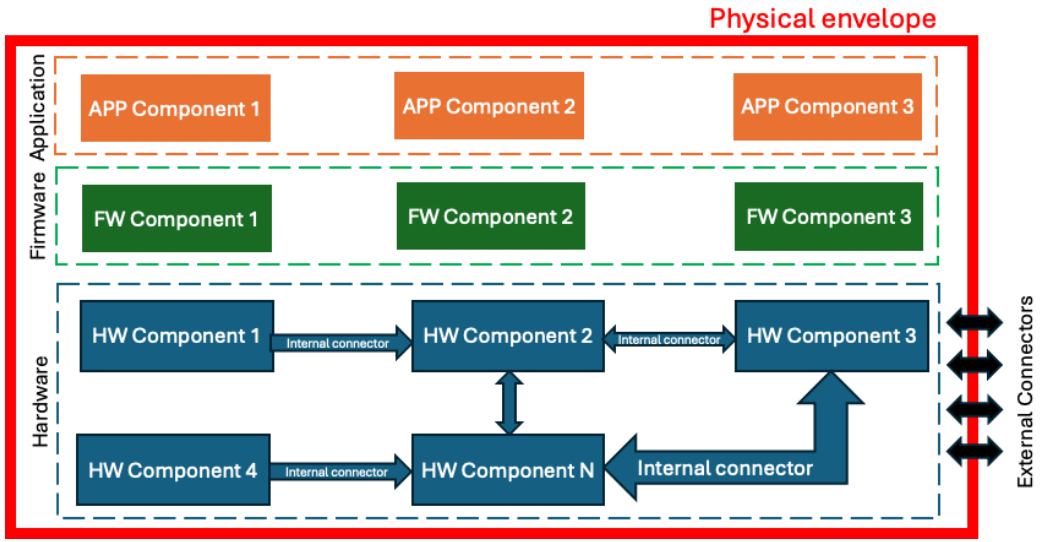
Firmware Components

- Boot and Integrity Management
  - Bootloader/Secure boot manager
  - FW Integrity Verification
  - Tamper State Handler
  - Version/Anti-rollback Control
- Cryptographic Engine and Key Management
  - Crypto Kernel (AES, RSA, ECC, SHA, HMAC, etc.)
  - Key Management (generation, wrap/unwrap, import/export, rotation, backup/restore, revocation, deletion, etc.)
  - RNG/Entropy Manager
  - Key Store Controller
  - Access Policy Engine
- Security services and policy enforcement
  - Authentication/Authorization Manager
  - Audit and logging module
  - Tamper & Environment Monitor
  - Self-test Module
  - Access control
  - Resource control
- Communication and interface layer
  - Command dispatcher / API layer
  - Network / Serial Interface drivers
  - Session & Transport Security (TLS, IPsec, etc.)
  - Firmware Update Service

Architecture and main possible functions

The generic HWSB is composed of

- Physical Envelope
- External connectors
- Hardware components
- Internal connectors
- Firmware components
- **Application components**



Application Components

Applications components are use-case dependent

- First focus is HSM
  - General purpose HSM
  - Payment HSM
  - Programmable HSM

- We are looking for experts with knowledges on
  - Payment terminals
  - Tachograph
  - Other kind of HWSB

Architecture and main possible functions

- See the previous slides as a toolbox

- The assessment will consider
  - That the capability is implemented or not
  - That the implementation can be in hardware, firmware, application layer or a mix of them
  - The role of the operational environment

Operational Environment

3 types of environments are considered (ISO/IEC 13491)

- Uncontrolled environment
  - e.g. unattended ATM, gas pump, kiosk
- Controlled environment
  - Minimally controlled
    - e.g. merchant location with PIN entry devices maintained inside a store
  - Controlled
    - e.g. computer room with access control. Interior and exterior surveillance.
  - Controlled-plus
    - e.g. installation with a secure cabinet where it is itself installed in a controlled environment
- Protected environment
  - e.g. Key Loading Facility (KLF) which is considered more secure than a controlled environment. Only individuals with authorized access to use the device have permitted access to the hosting environment (e.g. cabinet, room or safe)

Users

There are 2 category of users

- End users
  - Authorities who can be associated with secret keys and authentication/authorization data (Bank, signing authority, other)
  - An end user communicates with the HWSB using a client application

- Administrators
  - Administrator tasks include: HWSB initialization, HWSB configuration, Activation/Deactivation of security services, Secure update, Logs management, Log audit, Key management
  - Administrator tasks may be assigned to several administrative roles

Use cases

- UC0: Core HWSB
  - Manages sensitive data
  - Performs cryptographic operations
  - Has several discrete components
  - Incorporate a hardware physical envelope that protects against physical attacks

- Several flavours of HSM
  - UC1: General purpose HSM
  - UC2: Payment HSM

- To come
  - UC3: Programmable HSM
  - UC4: Payment terminals
  - UC5: Tachograph
  - Others

Assets

- User data
  - Protected in Integrity and/or confidentiality when recorded, stored and transferred
- Management data
  - Use-case dependent
    - For POI: Risk management data, payment transaction data
    - For Tachograph: Digital map, location data, calibration data, user activity data
- Cryptographic keys
  - Trusted channel keys (must be protected in confidentiality and integrity)
  - Software update keys
  - Private/public keys associated to secure services
- TOE Security Box (Envelope)
  - Protection sensors, Sensors linked to services, Interfaces with access control
- TOE Hardware and Software
  - Core HW, Core SW, Secure services, Software update image, Internal communications
  - Use-case specific HW or SW (e.g. internal clock for tachograph)

Threats

Threats are divided into categories:

Data Modification and disclosure	Threats on SW	Threats on HW	Threats on communications	Threats on keys	Threats on isolation	Other
• T.DataMod • T.Calibration_Parameters • T.Location_Data • T.Motion_Sensor • T.Output_Data T.Log • T.DataDisclose	• T.IllegalCodeInstall • T.Software • T.LogicalAttacks • T.Access • T.Tests	• T.Power_Supply • T.Hardware • T.Environment • T.Tests	• T.SecureCommunicationsLines • T.Card_Data_Exchange • T.Fake_Devices_Connections • T.Internal_Communication	• T.KeyDerive • T.KeyDisclose • T.KeyMisuse • T.KeyMod • T.KeyOveruse	• T.NonSeparation • T.ResidualInformation	• T.Usurpation • T.Availability

Risk Profiles

- Risk profiles are defined for Core HWSB and for each use-case

- So far, we took the risks profiles that have been selected by those who require the certifications: from eIDAS, payment industry, certificate authorities

- Risk Profiles consist in a list of
  - SARs for documentation requirements
  - SFRs for product requirements

Risk Profiles – Assurance requirements

	SAR	Core SAR for HWSB	Proposed SAR for FIPS level 3 HSM	Proposed SAR for PCI HSM	ANSSI-CC-PP-2016_05 (TSP) EAL4+
ADV	ADV_ARC	ADV_ARC.2 (Exception possible)	ADV_ARC.1	ADV_ARC.1	ADV_ARC.1
ADV	ADV_FSP	ADV_FSP.1 (if van.2)	ADV_FSP.1	ADV_FSP.1	ADV_FSP.4
ADV	ADV_IMP	ADV_IMP.1 (to fill secure by design Req)	ADV_IMP.1	ADV_IMP.1	ADV_IMP.1
ADV	**ADV_PDM (Ext)**	ADV_PDM.1	ADV_PDM.1	ADV_PDM.1	ADV_PDM.1
ADV	ADV_TDS	ADV_TDS.1	ADV_TDS.1	ADV_TDS.1	ADV_TDS.3
AGD	**AGD_DEC (Ext)**	AGD_DEC.1	AGD_DEC.1	AGD_DEC.1	AGD_DEC.1
AGD	AGD_OPE	AGD_OPE.1	AGD_OPE.1	AGD_OPE.1	AGD_OPE.1
AGD	AGD_PRE	AGD_PRE.1 (Exception possible)	AGD_PRE.1	AGD_PRE.1	AGD_PRE.1
ALC	ALC_CMC		ALC_CMC.2	ALC_CMC.2	ALC_CMC.4
ALC	ALC_CMS		ALC_CMS.2	ALC_CMS.2	ALC_CMS.4
ALC	ALC_DEL		ALC_DEL.1		ALC_DEL.1
ALC	ALC_DVS			ALC_DVS.1	ALC_DVS.1
ALC	ALC_FLR	ALC_FLR.1	ALC_FLR.1	ALC_FLR.1	ALC_FLR.1
ALC	ALC_LCD			ALC_LCD.0	ALC_LCD.1
ALC	**ALC_PSR (Ext)**	ALC_PSR.1	ALC_PSR.1	ALC_PSR.1	ALC_PSR.1
ALC	**ALC_SBM (Ext)**	ALC_SBM.1	ALC_SBM.1	ALC_SBM.1	ALC_SBM.1
ALC	ALC_TAT		ALC_TAT.1	ALC_TAT.1	ALC_TAT.1
ASE	ASE_CCL		ASE_CCL.1	ASE_CCL.1	ASE_CCL.1
ASE	ASE_ECD			ASE_ECD.1	ASE_ECD.1
ASE	ASE_INT		ASE_INT.1		ASE_INT.1
ASE	ASE_OBJ	ASE_OBJ.1	ASE_OBJ.1	ASE_OBJ.1	ASE_OBJ.2
ASE	ASE_REQ	ASE_REQ.1	ASE_REQ.1	ASE_REQ.1	ASE_REQ.2
ASE	ASE_SPD	ASE_SPD.1	ASE_SPD.1		ASE_SPD.1
ASE	ASE_TSS		ASE_TSS.1	ASE_TSS.1	ASE_TSS.1
ATE	ATE_COV		ATE_COV.1		ATE_COV.2
ATE	ATE_DPT				ATE_DPT.1
ATE	ATE_FUN	ATE_FUN.1	ATE_FUN.1	ATE_FUN.1	ATE_FUN.1
ATE	ATE_IND				ATE_IND.2
AVA	AVA_VAN	Probably AVA_VAN.2	AVA_VAN.2	AVA_VAN.2	AVA_VAN.5

CRA-Specific evidence

- Annex C: Interpretation of HWSB assurance requirements in CC language
  - CC Part 3 SAR (+ Extended) mapping to
    - HWSB Core requirements
    - HSM PP
    - FIPS 140-3 level 3 HSM
    - PCI HSM

Risk Profiles – Functional requirements

- Annex B: CC part 2 SFR (+ Extended requirements) mapping to
  - HWSB Core requirements
  - HSM Protection Profile requirements

Category	Classification / Requirement	Core requirements (source ENISA)	HWSB Core requirements	UC1 requirements (source HSM PP)	CC requirement
Physical Protection	General	x	Put into Introduction: At least one physical mechanism	Put into Introduction	N/A
Physical Protection	Resistance to Physical Attack		when applicable	mandatory	FPT_PHP.3
Physical Protection	Passive detection of Physical Attack		when applicable	mandatory	FPT_PHP.1
Physical Protection	Documentation		guidance + ARC	guidance + ARC	AGD
Cryptographic Support	Key Update		Protected if existing	Protected if existing	policy
Cryptographic Support	Key Injection		Protected if existing	Protected if existing	FDP_ITC.2
Cryptographic Support	Key Activation/Deactivation		Protected if existing	Mandatory	Access control (FDP_ACC
Cryptographic Support	Key Exportation		Forbidden or protected	Forbidden or protected	FDP_ETC.2
Cryptographic Support	Key Storage	x (part of data integrity/confidentiality)	Protected if existing	mandatory	FDP_SDC FDP_SDI
Cryptographic Support	Key Backup and Restore	?	Protected if existing	mandatory	N/A
Identification, authentication and Access Control	Access control - Security attribute based access control - backup	**x (without refinement)**	mandatory	mandatory	FDP_ACF.1
Correct operation	Secure by Default	x	mandatory	mandatory	AGD (MSA.3)
Correct operation	Reset to original state	x	mandatory	mandatory	to be defined
Correct operation	Processed data minimisation	x	mandatory	mandatory	ADV_PDM.1
Correct operation	Essential and Basic Functions	x	to be checked (find the minimal requirement)	to be checked (ex: Max failure counter, Authenticating, on the appliance level, open interface)	to be defined
Correct operation	Secure Boot		mandatory (as it is a critical product)	mandatory	ARC/FPT_INI.1
Correct operation	Tests - Self-tests	**x (without refinement)**	mandatory	from PP	FPT_TST.1
Correct operation	Tests - Conditional Tests		optional	mandatory	FPT_TST.1
Correct operation	Secure Configuration	to be checked (if secure by default)	mandatory	mandatory	AGD
Correct operation	Secure Updates	to be checked	mandatory if existing	mandatory	task force
Correct operation	Secure Execution		mandatory	mandatory	self-protection), FPT_PHP
Correct operation	Detection of TOE hardware or software failures		mandatory (check with other potential overlapping requiremen	datory (check with other potential overlapping requiremen	C (for SW), FPT_PHP.1 (H
Correct operation	Resistance to abnormal conditions		mandatory (check overlap with fail secure, provide minimal condi	tory (check overlap with fail secure, provide minimal condi	AGD , FPT_PHP, AVA
Correct operation	Fail Secure	x	mandatory	mandatory	FPT_FLS.1
Correct operation	Secure Backup		Protected if existing	to be checked	HSM PP
Logging	Audit data generation and opt-out	x	mandatory	mandatory	FAU_GEN.1
Logging	Management of TSF Data - Audit Log		mandatory	mandatory	FMT_MTD.0

CRA-Specific Requirements

Requirements

- **Requirements on documentation** fall into 5 categories
- **Product requirements** fall into 6 categories

- Each requirement is composed of 4 sections:
  - Applicability: Applicable use-case(s)/capabilities
  - Requirement: The content of the requirement
  - Rationale: What is the risk that the requirement is covering. Link to threats.
  - Example: if it clarifies

Requirement on evidences

- Documentation related to the Security Target
  - ASE_OBJ/REQ/SPD/CCL/ECD/INT/TSS
- Documentation related to development
  - Functional specification ADV_FSP.X
  - Security Architecture ADV_ARC.X
  - TOE Design: ADV_TDS.X
- Documentation related to Guidance
  - Operational user guidance AGD_OPE.1
  - Preparative procedures AGD_PRE.1
  - Decommissioning Procedures AGD_DEC.1
- Evidence related to tests
  - Analysis of Coverage ATE_COV.2
  - Depth and Independent testing ATE_DPT/IND
  - (Functional testing ATE_FUN.X)
- Documentation related to the life cycle
  - Flow remediation, Periodic Security Review, software bill of material ALC_FLR.X/PSR/SBM
  - Configuration scope and management, TOE Delivery, Developer environment security, Life-cycle definition, Development Artefacts, Tools and Techniques, Integration: ALC_CMC/CMS/DEL/DVS/LCD/TDA/TAT/COMP
- Other evidences
  - Source code (Implementation representation ADV_IMP.X)
  - (Data minimization ADV_PDM.1)

Extended SAR

Example

Functional specification (ADV_FSP)

Applicability

- This requirement applies to all HWSB.

Requirement

- A functional specification of the external interfaces shall be available for assessment activities. It shall
  - Describes the purpose and method of use for all interfaces
  - Identifies and describes all parameters associated with each interface
  - Describes all actions associated with each interface
  - Describes all error messages that may result from an invocation of each interface
- Requirements specified in ISO/IEC 15408-3:2022 for the developer (D) and content (C) shall be followed:
  - ADV_FSP.1 in general and ADV_FSP.4 for UC1 (QSCD)

Rationale

The objective is to verify that all the claimed functions are well identified and described.

Example

When a public specification exists, it can be referred. Only option selections and deviations must be described

Product Requirements

Physical Protection	Cryptographic Support	Identification, Authentication and Access Control	Correct Operation	Logging	Data Integrity and Confidentiality Protection
- Passive detection of Physical Attacks - Resistance to Physical Attacks - Resistance to non-invasive Attacks	- Cryptographic Operation - Random Number Generation - Cryptographic Key Generation - Timing and Event of Cryptographic Key Destruction - Key Injection - Key Activation/Deactivation - Key Exportation - Key Storage - Key Backup and Restore	- Security Roles - Timing of Identification - Authentication per role - Timing of Authentication - Authentication failure handling - Re-Authenticating - Subset Access control – Key/Backup - Security Attribute-Based Access Key/Backup - Secure Interface for Sensitive Operation - Management of TSF Data – Unblock - Specification of Management Functions - Management of Security Attributes - Static Attribute Initialization - Unique Identification	- Self-Tests - Degraded Fault Tolerance - Initialization - Secure by Default - Reset to Original State - Secure Boot - Secure Configuration - Secure Updates - Secure Execution - Detection of TOE Hardware or Software Failures - Resistance to Abnormal Conditions - Secure Backup - Manual Recovery - Fail Secure - Separation	- Audit Data Generation and Opt-Out - Management of TSF Data – Audit Log - User Identity Association - Audit Data Storage - Action in case of possible Audit Data Loss - Audit review - Timestamps	- Stored Data Integrity - Trusted Path – Local - Trusted Path – External - Subset Information Flow Control - Simple Security Attributes - Residual Information Protection - Import of User Data Without Security Attributes - Export of User Data without Security Attributes - Export of Security Data With Security Attributes

HWSB Definition Added for CRA

Example

Secure Boot

Applicability

- This requirement applies to all HWSB

Requirement

- The product shall verify the authenticity and integrity of all code (bootloader, firmware, embedded software) before it is executed, using a cryptographically strong digital signature or equivalent mechanism anchored in a trusted root. Execution shall not proceed if the verification fails.
- Requirements specified in ISO/IEC 15408-2:2022 shall be followed:
  - FPT_INI.1
- In addition to ADV_FSP.X and ADV_TDS.X, the below requirement specified in ISO/IEC 15408-3 for the developer (D) and content (C) shall be followed:
  - ADV_ARC.1

Rationale

Ensuring that only verified code executes prevents attackers from injecting or modifying software that could bypass or disable security functions. Compromised startup code would undermine all subsequent protections.

Example

At power-on, the boot ROM checks an ECDSA signature on the firmware image using a public key embedded in one-time-programmable memory. If the signature check fails, the device halts and signals a tamper or error state.

Assessment

- **Assessment reference.** Identifies the link to the exact requirement. ID.
- **Assessment objectives.** Defines the security, property or capability that shall be verified and showing that the assessment remains focused on the intent of the requirement.
- **Assessment preparation.** Describes the environment setup and preconditions required before executive the test. Tools guidance.
- **Assessment activities** provide execution steps to be performed. Activities are designed to cover the necessary legal depending on whether requirement is basic, elevated or advanced test and results.
- **Assignment of a verdict**. Define Pass/Fail criteria. The assessment is considered successful if the requirements protection goals are demonstrably met.
- **Supporting evidence** lists the artefacts to be collected and documented, such as log, Configurations files, Screenshot, Vendor documentation and test results. Evidence ensures traceability.

Requirement on evidence assessment example

- **Assessment reference** ADV_FSP
  - Applies to all functional requirements
- **Objective**
  - Determine whether the interfaces are completely and accurately described.
- **Preparation**
  - Availability of the functional specification
- **Activities**
  - Following assessment measures specified in ISO/IEC 15408-3:2022 shall be performed:
  - ADV_FSP.1XE in general and ADV_FSP.4XE for UC1 (QSCD)
- **Supporting evidence**
  - User Guidance
  - Security Target
  - Functional specification

Product requirement assessment example

- **Assessment reference: tamper evidence and resistance**
  - Applies to requirements REQ-PHY-DETINV, REQ-PHY-RESINV and REQ-PHY-NONINV
- **Objective**
  - Demonstrate that the product is resistant to an attacker with an attack potential determined by the UC.
  - Demonstrate that the product is resistant to all physical attacks that do not require the use of specialist tools to directly probe a silicon substrate to access or modify sensitive assets.
  - The evaluation shall demonstrate that the external enclosure is resistant to attackers with selected attack potential. The attacks that are listed in [JEDS] section 3.1.1.
- **Activities**
  - Following assessment measures specified in ISO/IEC 15408-3:2022 shall be performed while focusing on tamper evidence and resistance:
  - AVA_VAN.5 for UC1 (QSCD)
  - AVA_VAN.2/3 for less critical deployment
- **Verdict**
  - The verdict is PASS if the quotation of the successful attacks are all above the attack potential selected.
- **Supporting evidence**
  - Samples
  - Current information regarding public vulnerabilities
  - Security target
  - Functional specification, Architecture, Design, Implementation subset
  - Guidance

Annex ZA

Mapping between this standard and the essential requirements of CRA regulation

▶ Mapping with Annex I, Part I

Essential requirements of CRA regulation - Annex I, Part I	Clause(s)/sub-clause(s) of this EN
(1) Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks.	Annex E - Security Problem Definition Annex L - Security Target, Security Objectives Annex L - Security Target, Security Requirements Rationale
(2)(a) Be made available on the market without known exploitable vulnerabilities.	6.5 - Pen-testing (AVA) Annex I - Vulnerability Handling
(2)(b) Be made available on the market with a secure by default configuration, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, including the possibility to reset the product to its original state.	Security Architecture (ADV_ARC) Resistance to Physical Attack (REQ-PHY-RESINV) Resistance to non-invasive attacks (REQ-PHY-NONINV) Secure Boot (REQ-COP-SECBOOT) Secure Execution (REQ-COP-SECEXE) Detection of TOE Hardware or Software Failures (REQ-COP-DETFAIL) Seperation (REQ-COP-SEP) **Specification of Management Functions (REQ-IAA-SEPCMF)** **Annex A.2.1: ADV_ARC.2 Secrutiy Architecture with default security configuration (Extended)**
(2)(c) Ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates that are installed within an appropriate timeframe enabled as a default setting, with a clear and easy-to-use opt-out mechanism, through the notification of available updates to users, and the option to temporarily postpone them.	Secure Updates (REQ-COP-SECUP)
(2)(d) Ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorised access.	Timing of Identification (REQ-IAA-TIMI) Authentication per role (REQ-IAA-AUTHROL) Timing of Authentication (REQ-IAA-TIMA) Authentication Failure Handling (REQ-IAA-AUTHFH) Re-Authenticating (REQ-IAA-REAUTH) Subset Access Control - Key Usage (REQ-IAA-SUBKEYUS) Security Attribute-Based Access Control - Key Usage (REQ-IAA-ATTKEYUS) Subset Access Control - Backup (REQ-IAA-SACBACK) Security Attribute-Based Access Control - Backup (REQ-IAA-ATTBACK) Secure Interface for Sensitive Operation (REQ-IAA-SENSOP) Cryptographic Support (REQ-CRY-XXX)
(2)(e) Protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms, and by using other technical means.	Key Storage (REQ-CRY-KEYSTO) Passive detection of Physical Attack (REQ-PHY-DETINV) Resistance to Physical Attack (REQ-PHY-RESINV) Detection of TOE Hardware or Software Failures (REQ-COP-DETFAIL) Data Integrity and Confidentiality Protection (REQ-DPR-XXX)
(2)(f) Protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, and report on corruptions.	Data Integrity and Confidentiality Protection (REQ-DPR-XXX) Cryptographic Support (REQ-CRY-XXX) Audit Data Generation and Opt-out (REQ-LOG-AUDGEN) Import of User Data without Security Attributes (REQ-DPR-IMPSECATT) Trusted Path - Local (REQ-DPR-TRPLOC) Trusted Path - External (REQ-DPR-TRPEXT)

Essential requirements of CRA regulation - Annex I, Part I	Clause(s)/sub-clause(s) of this EN
(2)(g) Process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the product with digital elements (data minimisation).	Annex A.2.2 ADV_PDM.1: Processed Data Minimization
(2)(h) Protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks.	Degraded Fault Tolerance (REQ-COP-FLTTOL) Fail Secure (REQ-COP-FAILSEC)
(2)(i) Minimise the negative impact by the products themselves or connected devices on the availability of services provided by other devices or networks.	Initialization (REQ-COP-INIT) Self-tests (REQ-COP-TEST) Subset Information Flow Control (REQ-DPR-SUBFC) Simple Security Attributes (REQ-DPR-SECATT)
(2)(j) Be designed, developed and produced to limit attack surfaces, including external interfaces.	6.5 - Pen-testing (AVA) Annex I - Vulnerability Handling 5.1.2.1 Functional Specification (ADV_FSP) 5.2 Product Requirements (REQ-XXX-XXX) 5.1.3.1 Operational user guidance 5.1.3.2 Preparative procedures
(2)(k) Be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques.	6.5 - Pen-testing (AVA) Annex I - Vulnerability Handling 5.1.2.1 Functional Specification (ADV_FSP) 5.1.2.2 Security Architecture (ADV_ARC) Resistance to Physical Attack (REQ-PHY-RESINV) Resistance to non-invasive attacks (REQ-PHY-NONINV) Correct Operation (REQ-COP-XXX) Separation (REQ-COP-SEP) Annex A.2.1: ADV_ARC.2 Secrutiy Architecture with default security configuration (Extended)
(2)(l) Provide security related information by recording and monitoring relevant internal activity, including the access to or modification of data, services or functions, with an opt-out mechanism for the user.	Specification of Management Functions (REQ-IAA-SPECMF) Security Roles (REQ-IAA-SECR) Logging (REQ-LOG-XXX)
(2)(m) Provide the possibility for users to securely and easily remove on a permanent basis all data and settings and, where such data can be transferred to other products or systems, ensure that this is done in a secure manner.	Specification of Management Functions (REQ-IAA-SPECMF) Residual Information Protection (REQ-DRP-RIP) Key Exportation (REQ-CRY-KEYEXP) Export of User Data without Security Attributes (REQ-DPR-EXPNOSECATT) Export of User Data with Security Attributes (REQ-DPR-SECATT)

Annex ZA

Mapping between this standard and the essential requirements of CRA regulation

- Mapping with Annex I, Part II

Essential requirements of CRA regulation - Annex I, Part II	Clause(s)/sub-clause(s) of this EN
(1) Identify and document vulnerabilities and components contained in products with digital elements, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the products;	Annex A.2.4 ALC_FLR.4: Flaw remediation with distinction between security and functional flaws Annex A.2.3 ALC_SBM: Software Bill of Materials
(2) In relation to the risks posed to products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates; where technically feasible, new security updates shall be provided separately from functionality updates;	Annex A.2.4 ALC_FLR.4: Flaw remediation with distinction between security and functional flaws Secure Updates (REQ-COP-SECUP)
(3) Apply effective and regular tests and reviews of the security of the product with digital elements;	Annex A.2.5 ALC_PSR.1: Periodic Security Review and Testing
(4) Once a security update has been made available, share and publicly disclose information about fixed vulnerabilities …	Annex A.2.4 ALC_FLR.4: Flaw remediation with distinction between security and functional flaws
(5) Put in place and enforce a policy on coordinated vulnerability disclosure;	Annex A.2.4 ALC_FLR.4: Flaw remediation with distinction between security and functional flaws
(6) Take measures to facilitate the sharing of information about potential vulnerabilities …	Annex A.2.4 ALC_FLR.4: Flaw remediation with distinction between security and functional flaws
(7) Provide for mechanisms to securely distribute updates …	Annex A.2.4 ALC_FLR.4: Flaw remediation with distinction between security and functional flaws Secure Updates (REQ-COP-SECUP)
(8) Ensure that, where security updates are available … they are disseminated without delay …	Annex A.2.4 ALC_FLR.4: Flaw remediation with distinction between security and functional flaws Secure Updates (REQ-COP-SECUP)

Bibliography

[1] Application of Attack Potential to Hardware Devices with Security Boxes, Version 3.1, 2023.

[2] EUCC_state_of_the_art_Application of attack potential to hardware devices with security boxes v2 (draft).

[3] Guidance for Hardware assessment in EN419221-5 (HSM PP), May 2021

[4] CRA Implementation via EUCC, January 2025. https://certification.enisa.europa.eu/publications/cyber-resilience-act-implementation-eucc-and-its-applicable-technical-elements_en

[5] Guidance for Hardware assessment in EN419221-5 (HSM P), May 2021 https://www.sogis.eu/documents/cc/pp/hardware_devices/hsm/Guidance%20for%20HW%20assessment%20in%20EN%20419221-5%20(HSM%20PP)%20v1.0_final.pdf

[6] [PP HSM QSCD] EN 419221-5:2018 Protection profiles for Trust Service Provider Cryptographic modules - Part 5: Cryptographic Module for Trust Services

[7] [PCI HSM] Payment Card Industry (PCI) PIN Transaction Security (PTS) Hardware Security Module (HSM), V4.0, December 2021

[8] Protection Profile V2X Hardware Security Module - EAL4 augmented with ALC_FLR.1 and AVA_VAN.4., Nov 2021.

[9] ISO/IEC 19790:2025, Information security, cybersecurity and privacy protection — Security requirements for cryptographic modules

[10] ISO/IEC 24759:2025, Information security, cybersecurity and privacy protection — Test requirements for cryptographic modules.

[11] [PP POI] ANSSI-CC-PP-2015/0X. Point of Interaction Protection Profile.

[12] [PCI POI] Payment Card Industry (PCI) PIN Transaction Security (PTS) Point of Interaction (POI), Modular Security Requirements, Version 6.2, January 2023

[13] ISO 13491-1:2024. Financial services – Secure cryptographic devices. Edition 4, 2024.

[14] [PP TachoVU] Digital Tachograph Vehicle Unit (VU PP). BSI-CC-PP-0094-V2-2021.

[15] [PP eHCT] Common Criteria Protection Profile Electronic Health Card Terminal (eHCT) BSI-CC-PP-0032-V3-2022

[16] Protection Profile for Smart Meter Minimum Security requirements, Version 1.0, Oct 2019

[17] European Cybersecurity Certification Group – Subgroup on Cryptography – Agreed Cryptographic Mechanisms, version 2.0 – April 2025

[18] EUCC SCHEME SotA Application of attack potential to smartcards and similar devices. Version 2, February 2025.

[19] FIPS PUB 140-3, Security Requirements for Cryptographic Modules, March 22, 2019

[20] Refer other verticals: Smart Meter Gateway, secure Elements, OS, Boot, PKI Network functions: VPN, firewall, ...

What next?

- Presentation will be uploaded for consultation
- Provide us with your first feedback and questions, in the coming days
- A deep-dive session is planned on January 22nd with the expert group to address your questions and our main challenges
- Field experts are welcome to join the group via their national standardization bodies to accelerate towards completion

Thank you !

Claire Loiseaux

claire.loiseaux@internetoftrust.com

www.cencenelec.eu

Follow us:

Tag us @Standards4EU

Q&A