How to raise the cybersecurity bar in Europe with the harmonized standards

International Telecommunication Day 2026

May 19th, 2026

Author: Davide Pratone
Security Standardization Expert, Huawei

2025 Better Together

Security Level: Public

Context

Over the last decade, cyberattacks targeting consumer Internet of Things (IoT) devices and mobile platforms have increased significantly across both the United Kingdom and Europe. The rapid expansion of connected consumer devices, smart home technologies, and mobile applications has enlarged the digital attack surface, contributing to a sustained rise in malware, phishing, credential theft, and exploitation of insecure IoT products.

The European Union Agency for Cybersecurity, ENISA, has consistently identified malware, ransomware, and threats against data availability among the most prominent cyber threats affecting European digital ecosystems (https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape).

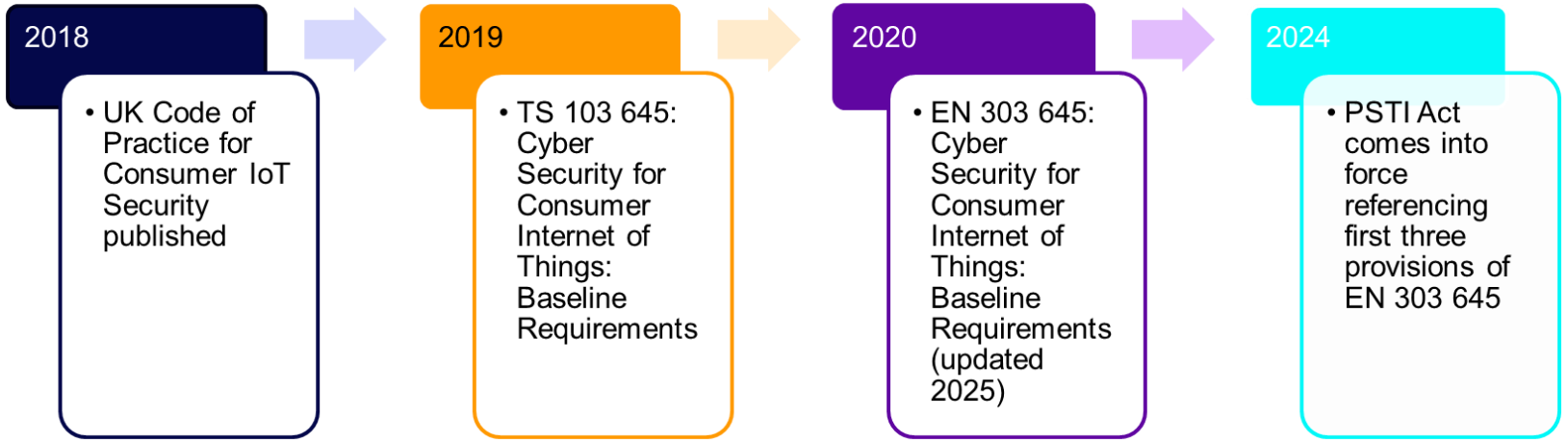
In the United Kingdom, the Department for Science, Innovation and Technology reported that the number of cyberattacks against IoT devices increased sharply alongside the adoption of consumer smart devices, including smart TVs, smart speakers, home security systems, and connected appliances (https://www.gov.uk/government/publications/cyber-security-of-consumer-iot-manufacturer-survey).

Mobile threats have followed a similar trajectory throughout Europe and the UK. ENISA threat landscape assessments and industry analyses have documented a continuous increase in mobile malware, banking trojans, spyware, and malicious mobile applications targeting smart phones

Which has been the answer?

UK approach to rise the cybersecurity bar on Consumer IoT devices

UK government participated in ETSI TC CYBER to develop an European Norm to cover cybersecurity requirements for Consumer IoT Devices



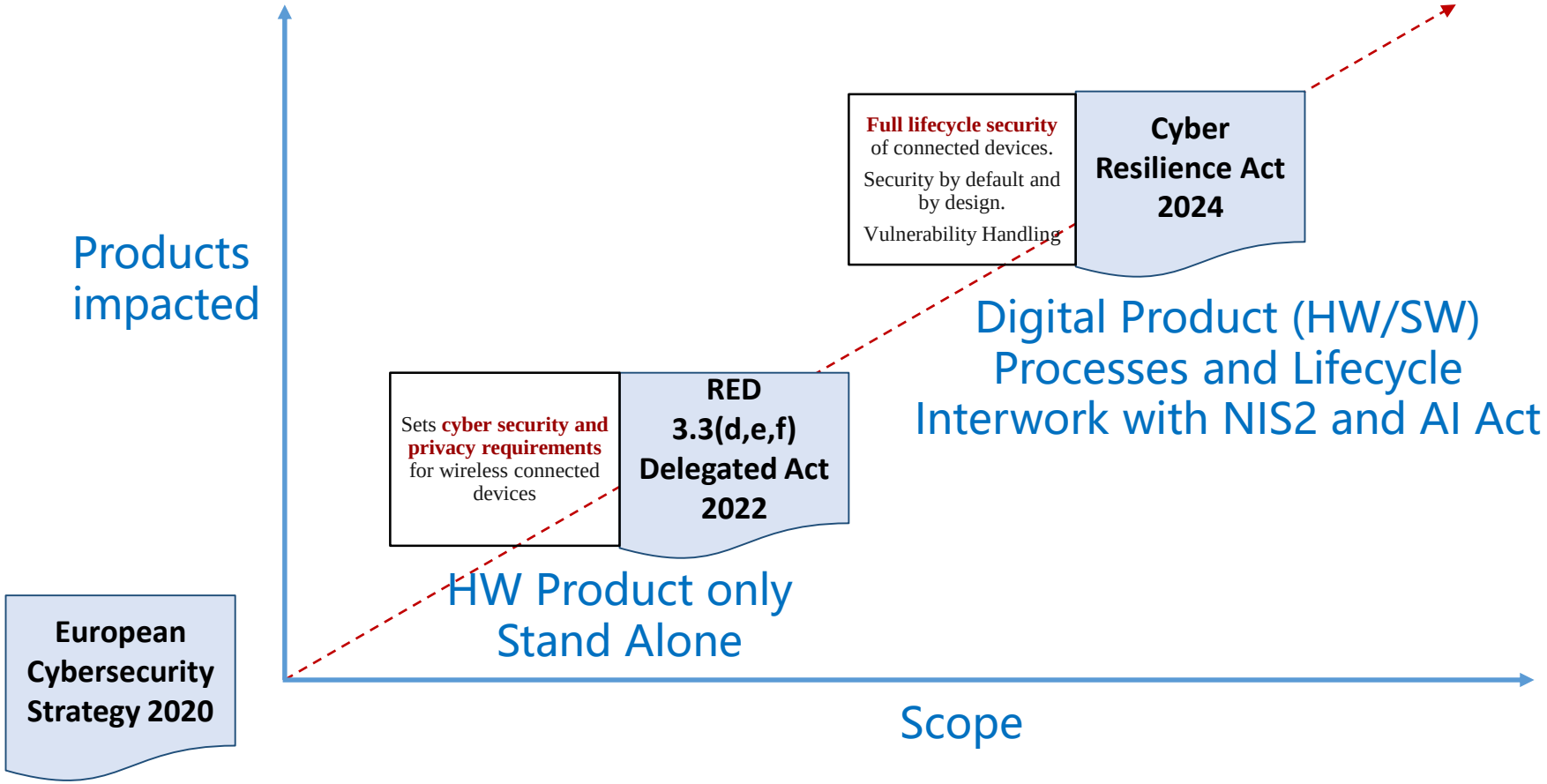
PSTI Requirement	ETSI EN 303 645 provision
1. Ban Universal default (and easily guessable) passwords	**5.1: No universal default passwords** • 5.1-1: Where passwords are used and in any state other than the factory default, all consumer IoT device passwords shall be unique per device or defined by the user • 5.1-2: Where pre-installed unique per device passwords are used, these shall be generated with a mechanism that reduces the risk of automated attacks against a class or type of device.
2. Publish information on how to report security issue	**5.2: Implement a means to manage reports of vulnerabilities** 5.2-1: The manufacturer shall make a vulnerability disclosure policy publicly available. This policy shall include, at a minimum: • contact information for the reporting of issues; and • information on timelines for: 1) initial acknowledgement of receipt; and 2) status updates until the resolution of the reported issues.
3. Publish information on minimum security updates periods	**5.3: Keep software updated** 5.3-13: The manufacturer shall publish, in an accessible way that is clear and transparent to the user, the defined support period

The EN 303 645 has been adopted worldwide and it has been used by several countries (including Finland) as bases for their voluntary and mandatory certification programs.

EN 303 645 generated several dedicated verticals for Consumer products such as **Home Gateway**, **Smart Door Lock**, **Smart Voice Controlled Devices**; but only the first 3 EN 303 645 provisions were referenced in the PSTI Act

Source: ETSI Security Conference 2025 DSIT presentation.

EU approach to rise the cybersecurity bar on most of the products placed on the European market (1/2)



Originated by the European Cybersecurity Strategy 2020 to strengthen EU's technological sovereignty and increase the cybersecurity level of the European market, the RED and CRA have been introduced in the past 5 years to define cybersecurity technical requirements for product market placement.

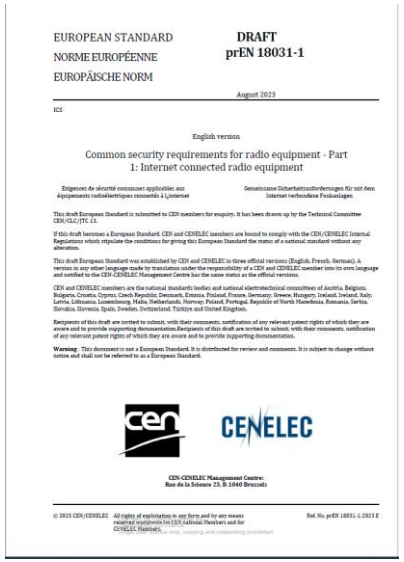
CRA complexity level is extremely higher then RED.

Introduction in the compliance process lifecycle activities such as the Risk Assessment, the Security by Design and by Default and the Vulnerability Handling, increases the manufacturers effort to reach the compliancy with the aim to increase as well the cybersecurity level of the products.

EU approach to rise the cybersecurity bar on most of the products placed on the European market (2/2)

Sets **cyber security and privacy requirements** for wireless connected devices

RED 3.3(d,e,f) Delegated Act 2022


EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

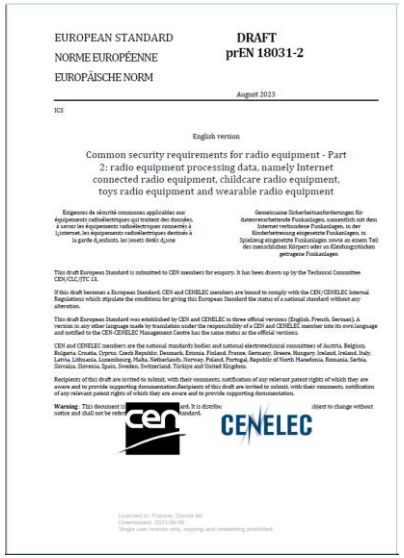
DRAFT
prEN 18031-1

August 2023

ICS

English version

Common security requirements for radio equipment - Part 1: Internet connected radio equipment


EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

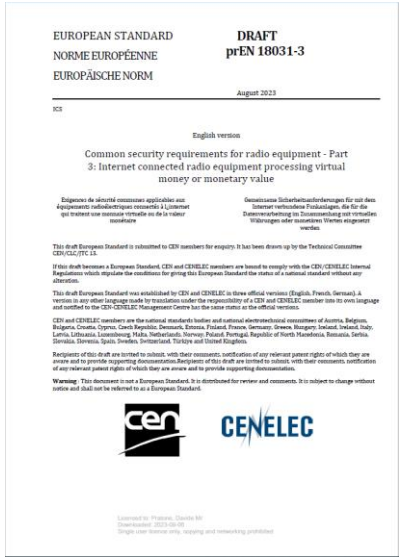
DRAFT
prEN 18031-2

August 2023

ICS

English version

Common security requirements for radio equipment - Part 2: radio equipment processing data, namely Internet connected radio equipment, childcare radio equipment, toys radio equipment and wearable radio equipment


EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

DRAFT
prEN 18031-3

August 2023

ICS

English version

Common security requirements for radio equipment - Part 3: Internet connected radio equipment processing virtual money or monetary value

Since 1st August 2025, many products have been declared compliant with the EU Radio Equipment Directive Delegated Regulation (EU) 2022/30 using the harmonised standards:

EN 18031-1: network protection

EN 18031-2: protection of personal data and privacy

EN 18031-3: fraud prevention for financial transactions

Covering the RED essential requirements 3.3(d,e,f).

This standards have been derived form the EN 303 645 and they have been modified adding dedicated security requirments an mainly defining the assessment criteria.

The standards have been cited with restrictions; this means that a product not affected by the restriction can declare its presumption of conformity otherwise it has to go to a Notified Body.

Next step of EU approach to rise the cybersecurity bar on product with digital elements: Cyber Resilience Act (1/2)

JTC13 WG9 Horizontal Standards
- **PT1 Risk assessment**
- **PT2 Horizontal requirements**
- **PT3 Vulnerability Handling**

Critical Products

CLC TC47x WG3 and CEN TC 224 WG17 TF41
Smart Cards such as **eUICC** and **eSE**

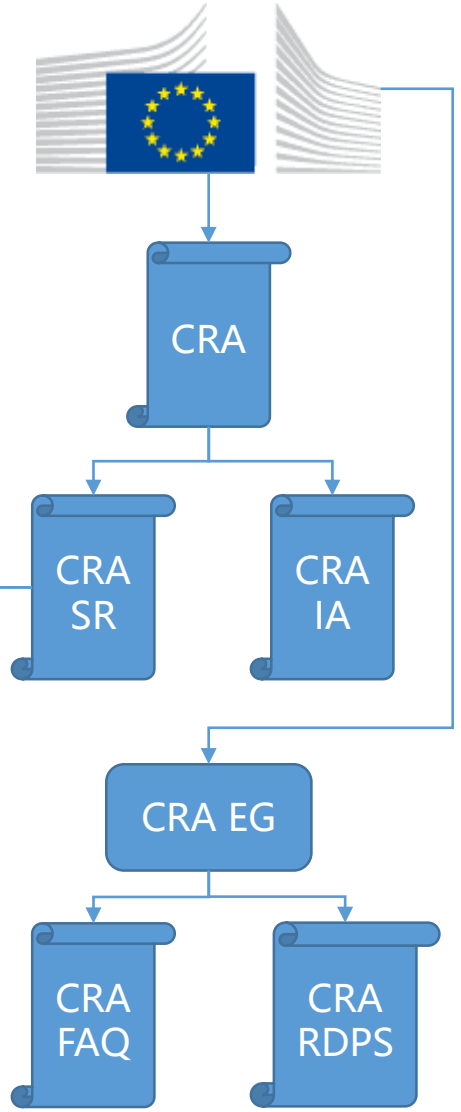
Important Products Class II

CLC TC47x WG1 and WG2
Tamper resistant microprocessor or microcontroller e.g. **TEE**

Important Products Class I

ETSI TC CYBER EUSR WG
Several Work Items dealing with:
- **Browsers**
- **Password Managers**
- **Antivirus SW**
- **Boot Managers**
- **PKI Infrastructures**
- **Physical and virtual network interfaces**
- **Operating Systems**
- **Routers and Modem**
- **Secure microprocessor and microcontroller**
- **Consumer IoT devices**

CEN TC 224 WG17
- **Biometric readers**



Default Products

Default Products are those that are not listed in the Important and Critical products. Examples are:
- **Smartphones**
- **Tablets**
- **Noteboks**

However these products includes several important and critical products to which the manufacturer shall grant their CRA compliancy.

Next step of EU approach to rise the cybersecurity bar on product with digital elements: Cyber Resilience Act (1/2)

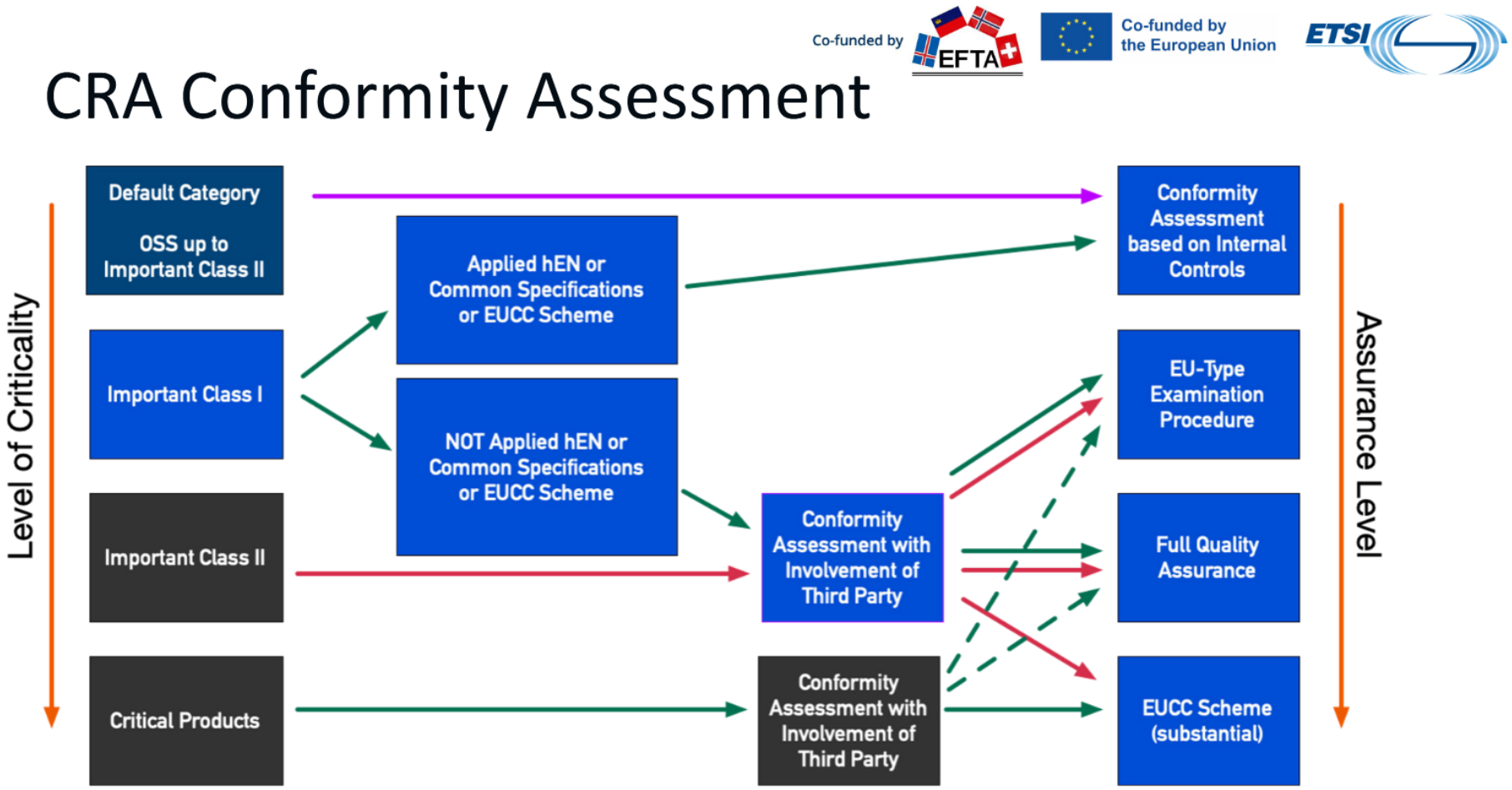
Mobile applications can be:

- **Default products**
- **Important products**

The COMMISSION IMPLEMENTING REGULATION(EU) 2025/2392 clarified the product category definition giving guidance to the standardization makers on the scope of each of the vertical standards expected to be devoloped.

The Guidance issued in March 2026 provided clarification about scope, open source software, support period, concept of core functionality, risk assessment and remote data processing solution.

The importance of the harmonized standards



CRA Important class I product example: Personal Wearables (EN 304 634)

Technical Description Implementing Regulation (EU) 2025/2392 Annex I #19

- Personal wearable products to be worn or placed on a human body that have a health monitoring (such as tracking) purpose and to which Regulation (EU) 2017/745(2)or (EU) 2017/746 of the European Parliament and of the Council do not apply, or personal wearable products that are intended for the use by and for children:
  - "Personal wearable products to be worn or placed on a human body that have a health monitoring purpose are products with digital elements that are worn on the body directly or via clothing or accessories and that can, regularly or continuously, sense and further process information, including body metrics, relevant to the user' s health, excluding products that fall within the scope of Regulation (EU) 2017/745 or of Regulation (EU) 2017/746.
    - This category includes but is not limited to fitness trackers, smartwatches, smart jewellery, smart clothing and sports apparel that meet this description."
  - "Personal wearable products that are intended for the use by and for children are products with digital elements which can be worn or placed on the body, directly or via clothing or accessories, of individuals under the age of 14.
    - This category includes but is not limited to child safety wearables.."

Considerations

- Overlaps concerning parental control and geo-localization functionalities between personal wearable products that are intended for the use by and for children (falling under #19) and internet connected toys (falling under #18) .

CRA Important class I product example: Personal Wearables (EN 304 634)

Smartwatches

Heart rate monitor belt

Fitness bands

Smart socks

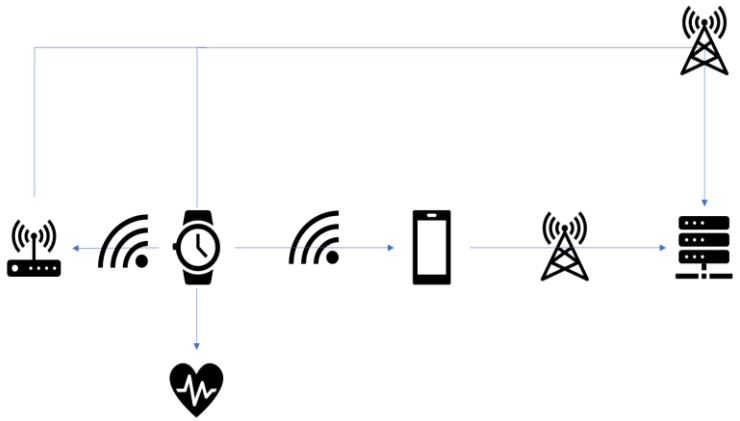
Smartwatch with GPS tracking and Parental control

Complete baby monitoring system

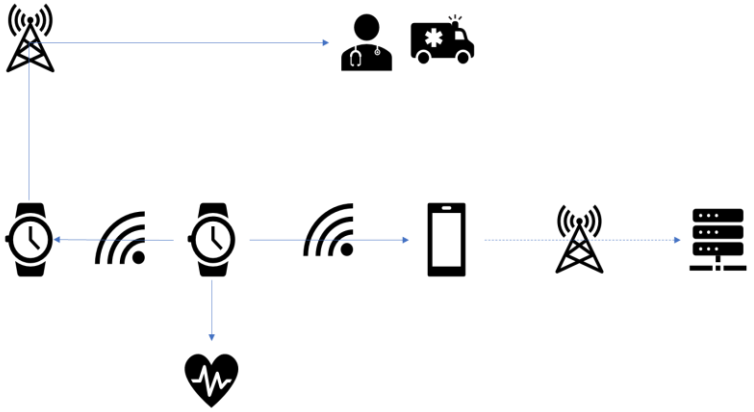
Considerations

- The category includes a broad range of products with different use cases and therefore different security profiles.
- The Implementing Regulation (EU) 2025/2392 talks about individual under the age of 14 years old. There is a clear separation between the product for babies under 2/3 years old, for which the monitoring is much more extensive but without the need of parental control, and the preadolescent child where GPS tracking and parental control are key functionalities and where the scenario seems to be an extension of the wearable for health monitoring.

CRA Important class I product example: Personal Wearables (EN 304 634)



Health monitoring wearable architecture



Wearable used by and for children architecture

Product Context definition

Product functions (Clause 4) in the standard:

The present document addresses the following essential functionalities of products:

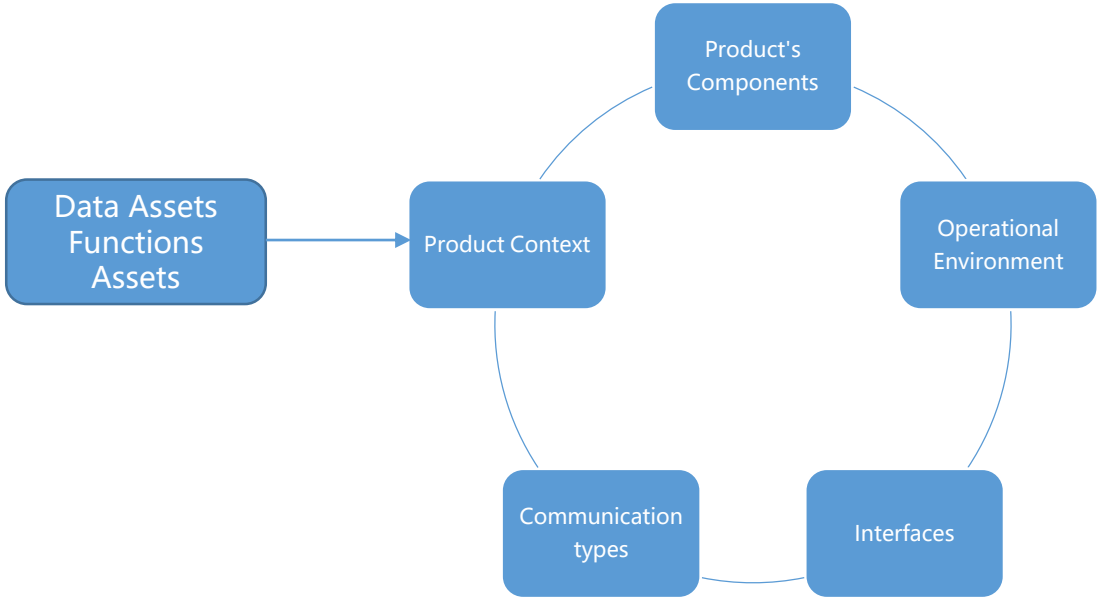
- Health monitoring functionalities
- Health monitoring functionalities (for babies use)
- Location-based functionalities
- Location-based functionalities (for children use)

The essential and supporting functionalities might process the following data assets:

- health data;
- fitness data;
- input data from sensors;
- location data, including device location data;
- …

CRA Important class I product example: Personal Wearables (EN 304 634)

The Risk Assessment



Requirements

Clause	heading	Clause	heading
5.1.1	Known exploitable vulnerabilities	5.1.7	Availability protection
5.1.2	Default configuration	5.1.8	Impact minimization
5.1.3	Authentication and access control mechanisms	5.1.9	Limit attack surface
5.1.4	Integrity protection	5.1.10	Logging and monitoring mechanisms
5.1.5	Confidentiality protection	5.1.11	Deletion mechanisms
5.1.6	Data minimization	5.1.12	Other product's technical requirements specifications

Table 7: Assignment of protection mechanisms strength level for the confidentiality of communicated data.

			confidential data impact class		
			IMP.CONF.Low	**IMP.CONF.Medium**	**IMP.CONF.High**
Attack Surface determined by COM, IF and POE of RDPS or MP that communicates confidential data	COM.Local via IF.Machine or IF.HumanLogical	POE.FullyControlled	N/A	N/A	CONF.COM.Normal
		POE.PartiallyControlled	N/A	CONF.COM.Basic	CONF.COM.Normal
		POE.Uncontrolled	CONF.COM.Basic	CONF.COM.Normal	CONF.COM.Enhanced
	COM.Adjacent via IF.Any	POE.Any	CONF.COM.Enhanced	CONF.COM.Enhanced	CONF.COM.Enhanced
	COM.Public via IF.Any		CONF.COM.Enhanced	CONF.COM.Enhanced	CONF.COM.Enhanced

Conclusion

- **2020** - The first approach to try to raise the cybersecurity bar of the products in Europe start in ETSI with the development of EN 303 645. It has been a success used in several certification program worldwide.
- **2023** - European Union decided to use the legislation related to the product market placement and activate the RED articles 3.3(d,e,f) for network protection. protection of personal data and privacy and fraud prevention for financial transactions; **these are the first European cybersecurity harmonized standards!** But:
  - The scope is limited to radio equipment
  - The scope is limited to product only
- **2024** - The Cyber Resilience Act legislation enter in force and its scope covers every product with digital elements (HW and SW) take into account the entire product lifecycle. **Horizontal (3) and Vertical (>20) harmonized standards** are under development to create the state of the art of the product cybersecurity in Europe!
- **2027** – These harmonized standard will start to be used to help manufacturers to get CRA compliance and those for Important Class I product, if cited by the European Commission, will provide Presumption of Confomity! .

Participate to develop the harmonized standard

- Good standards need stakeholder feedback
- Feel encouraged to get in touch with the Rapporteurs when you have questions/need clarifications
- For ETSI harmonised standard Use the commenting guidelines and commenting format you can find here https://docbox.etsi.org/cyber/EUSR/Open for providing formal feedback or participate in the ETSI TC CYBER EUSR WG if you are ETSI member
- For CEN and CENELEC TC participate trough your National Standardization Body

Thank you.

2025 Better Together