

RED (2014/53/EU) Delegated Act CYBERSECURITY

- Article 3.3 d, e, f

- December 19th, 2024
- **Lluís Boda**





AGENDA

1. Regulations
2. Accreditations of Applus+
3. Applicability for (EU) 2022/30
4. Testing & Assessment
5. Evaluation & Certification
6. FAQs



Lluís Boada

**Wireless and EMC Certification Technical Manager at Applus+ Laboratories
Deputy Chairperson in RED CA**

More than 20 years of experience in RF Engineering, last 13 years working at Applus+ Laboratories.

Proficiency in device certification processes in industry certification. Radio and EMC. Deep background in RF and Senior Antenna engineer.

MISSION: Coordinate and optimize the material and human resources to perform technical tasks, assuming technical responsibility.

Coordinate the different certification committees and their certification systems. Supervise the activities entrusted to other bodies involved on the certification systems. Participate in the Particular Certification Committees and in the elaboration of the Particular Certification Systems.

Inform the relevant administrations of the activities carried out according to the established requirements.

Manage the control body and product certifications for the following schemes:

- TCB (US) Decision Maker - Telecommunication Certification Body (TCB ES0002)
- FCB (CANADA) Decision Maker- FCB ES0001 Radio Equipment Certification
- RE-D (EU) - (Radio Equipment Directive-Compliance Association). NB-0370
- EMC-D (EU) - European Union Association of Notified Bodies. NB-0370
- UKRER (UK) - (S.I. 2017 No.1206) AP-8508
- EMCR (UK) - S.I. 2016 No.1091) AB-8508
- MIC (JAPAN) - (registered certification body) RCB 220

1. Why Applus+ Laboratories?

WIRELESS TESTING & CERTIFICATION

- **Unlicensed and licensed radio equipment up to 40 GHz**
 - Generic SRD, UWB, WLAN/WPAN, BWA,
 - Cellular and Satellite Communications,
- **EU Notified Body under 2014/53/EU RED**
- **UK Approved Body under 2017 Radio Equipment Regulations**
- **Telecommunication Certification Body (TCB) for U.S., FCC Title 47**
- **Foreign Certification Body for ISED Canada**
- **Recognized Certification Body (RCB) for MIC Japan**
- **International Radio Type Approval**
 - All Countries worldwide, one-stop shop
 - Global Market Access for Radio Equipment

3000+ Radio Type Approvals granted by Applus+ as CB, per year



What is RED? Radio Equipment Directive, the main objective of **RED** is to establish a regulatory framework for the marketing and use of radio equipment within the European Union. Its primary objectives are to ensure the protection of human health and safety, as well as to promote the effective and efficient use of the radio spectrum, therefore includes the test requirement in:

EMC Directive 2014/30/EU electromagnetic compatibility testing, and

LVD Directive 2014/35/EU safety testing (without applying voltage limits).

Two main concepts with regards devices on EU market

Putting into service → activate the Radio Equipment (RE) for the first time by final user

Placing in the market → marketing for the first time a RE in the Union market

Access to the public document →



Radio equipment technologies examples

- Radiolocation (RADARs) Maritime, Aeronautical & Civil
- Broadcast (terrestrial) Tx / Rx
- Mobile Cellular
- Broadband Wireless Access
- Fixed Links
- Intelligent Transport Systems
- PMR/PAMR/TETRA
- PMSE (Programme making and special events)
- Short Range Device
- WLAN/RLAN/WPAN
- Satellite Systems / GNSS Receivers
- Cordless Telephones
- Equipment below 9KHz
- Others (Meteo radars, Radio Astronomy, ...)
- Combined equipment (SmartTV, Smartphones, etc...)



Radar antennas



Base stations



Smart TVs



Smartphones



Wireless microphones



Walkie-talkies



Vehicle infotainment systems



Vehicle communication equipment



Handheld GPS navigation devices



Network connectors



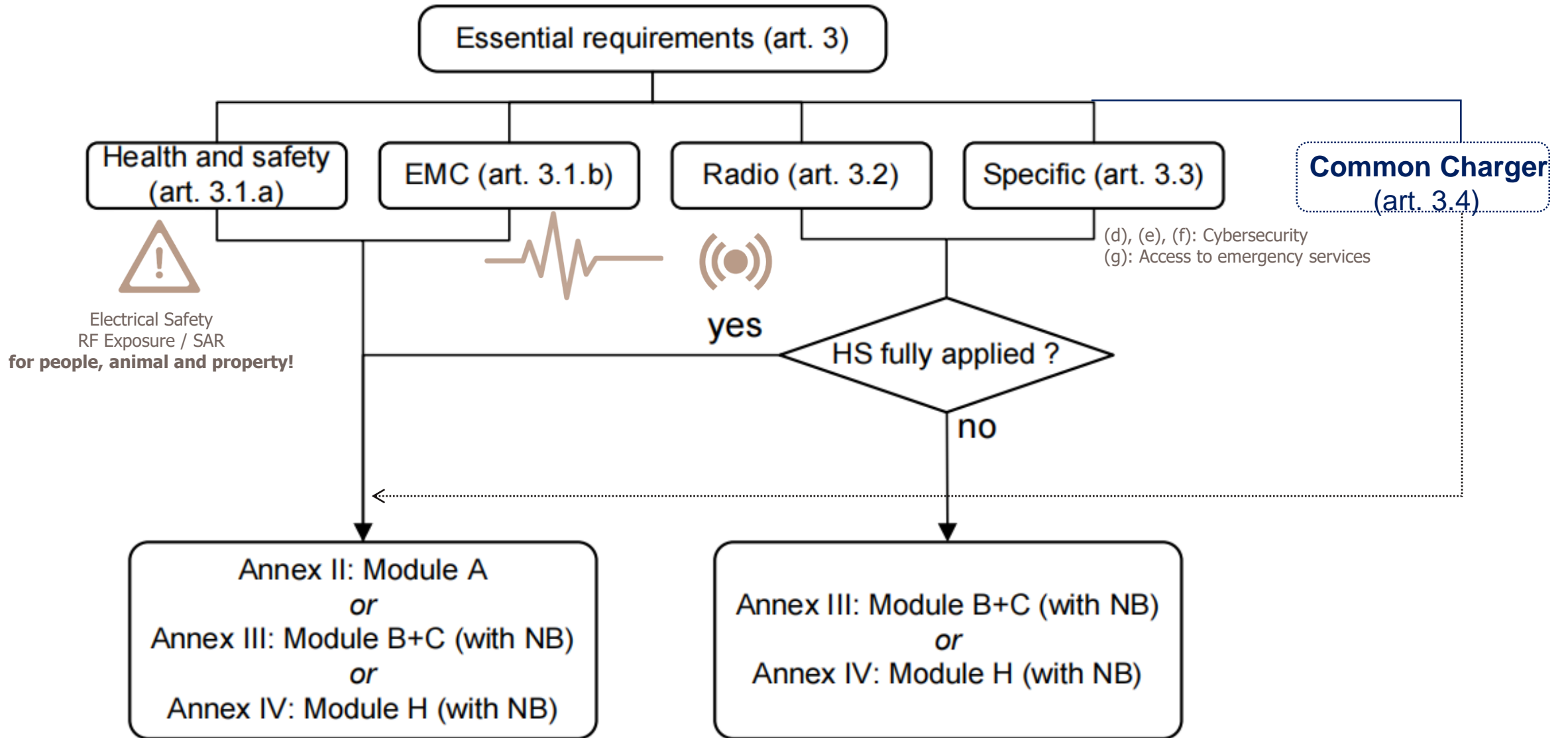
Cordless phones



Metal detectors



Handheld data terminals



Applus+ is **NOTIFIED BODY** for :


Body type	Legislation
NB	Regulation (EU) No 305/2011 - Construction products
NB	92/42/EEC Hot-water boilers
NB	Regulation (EU) 2016/426 Appliances burning gaseous fuels
NB	2006/42/EC Machinery
NB	Regulation (EU) 2016/425 Personal protective equipment
NB	Regulation (EU) 2019/945 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems
NB	2014/30/EU Electromagnetic compatibility
NB	2014/32/EU Measuring Instruments Directive
NB	2014/31/EU Non-automatic weighing instruments
NB	2014/53/EU Radio equipment

Data from NANDO System Database

**FOR A SINGLE PRODUCT
MODULE B**

APPLUS+ NOTIFIED BODY 0370
issues an
**EU-TYPE EXAMINATION
CERTIFICATE**

CE



**FOR A FAMILY OF PRODUCTS
MODULE H**



APPLUS+ NOTIFIED BODY 0370
issues a
**CERTIFICATE OF CONFORMITY
BASED ON FULL QUALITY ASSURANCE**

CE 0370

Restrictions (if applicable): N/A

2014/53/EU Radio Equipment

- Article 3.1.a
- Article 3.1.b
- Article 3.2
- Article 3.3.d
- Article 3.3.e
- Article 3.3.f
- Article 3.3.g
- Article 3.4 (in process)

The can check the validity of this certificate in our website

RED DA Applicability (scope):

RED Article 3.3(d) -applies to: *radio equipment that can communicate itself over the internet, whether it communicates directly or via any other equipment ('internet-connected radio equipment')*

RED Article 3.3(e) -applies to the following equipment is capable of **processing personal data** or **traffic data** and **location data**: **internet-connected radio equipment**, *radio equipment designed or intended exclusively for **childcare**, radio equipment falling under the **Toy Directive (2009/48/EC)**, **body-worn radio equipment***

RED Article 3.3(f): applies to: **internet-connected radio equipment**, *if that equipment enables the holder or user to **transfer money, monetary value or virtual currency**.*

- Internet-connected radio equipment
- Childcare devices
- Toy devices with (*Toys Directive- 2009/48/EC*)
- Body worn radio devices
- Internet-connected payment devices



☑ Toys or childcare wearable devices which are processing personal data, traffic data, and location data even if not connected to the internet also applies 3.3e

Examples:

➤ Internet-connected radio equipment

- Smartphones, tablets
- Smart TVs, household appliances
- Smart home gateways



➤ Childcare radio equipment

- Baby monitors
- Children's GPS trackers



➤ Toy radio equipment

- Smart robot toys (controllable via app)
- Interactive educational devices (controllable via app)
- Remote-controlled planes or cars with Wi-Fi cameras

➤ Wearable radio equipment

- Smartwatches
- Smart glasses
- Health monitoring bands (can record heart rate, sleep, and movement data)

➤ Internet-connected payment devices

- POS machines (Point of Sale Terminal) or dataphone



! Are there any exemptions?



- The following radio equipment is fully exempted from RED Articles 3.3(d), 3.3(e) and 3.3(f):
 - Medical devices (regulated in EU 2017/745 and EU 2017/746)
- The following radio equipment is exempted from RED Articles 3.3(e) and 3.3(f), but article **3.3(d)** still applies:
 - Regulation(EU)2018/1139(civil aviation);
 - Regulation(EU)2019/2144(type-approval of vehicles);
 - Directive(EU)2019/520(electronic toll collection systems).

Cybersecurity of these categories of products is guaranteed by existing pieces of dedicated EU legislation.

When will be applicable?

This Regulation shall apply from 1 August 2025.

What will happen with old devices?

- The delegated act will apply to all devices placed on the market once it becomes applicable. Old devices, which have already been placed on the EU market, can continue to be used without the need for specific adaptations until the end of their life cycle.
- New batch will need to be compliance with the new requirement.

RED DA defines "internet-connected radio equipment" as "equipment capable of communicating over the internet by itself, either directly or via any other equipment".

Common understanding of "Internet-connected radio equipment":

- Designed to communicate over the internet without any further modification, and
- Has the technical capability to communicate over the internet, which we refer to as "internet ready", and
- Supports specific communication protocols that allow it to communicate over the internet.

(for example:

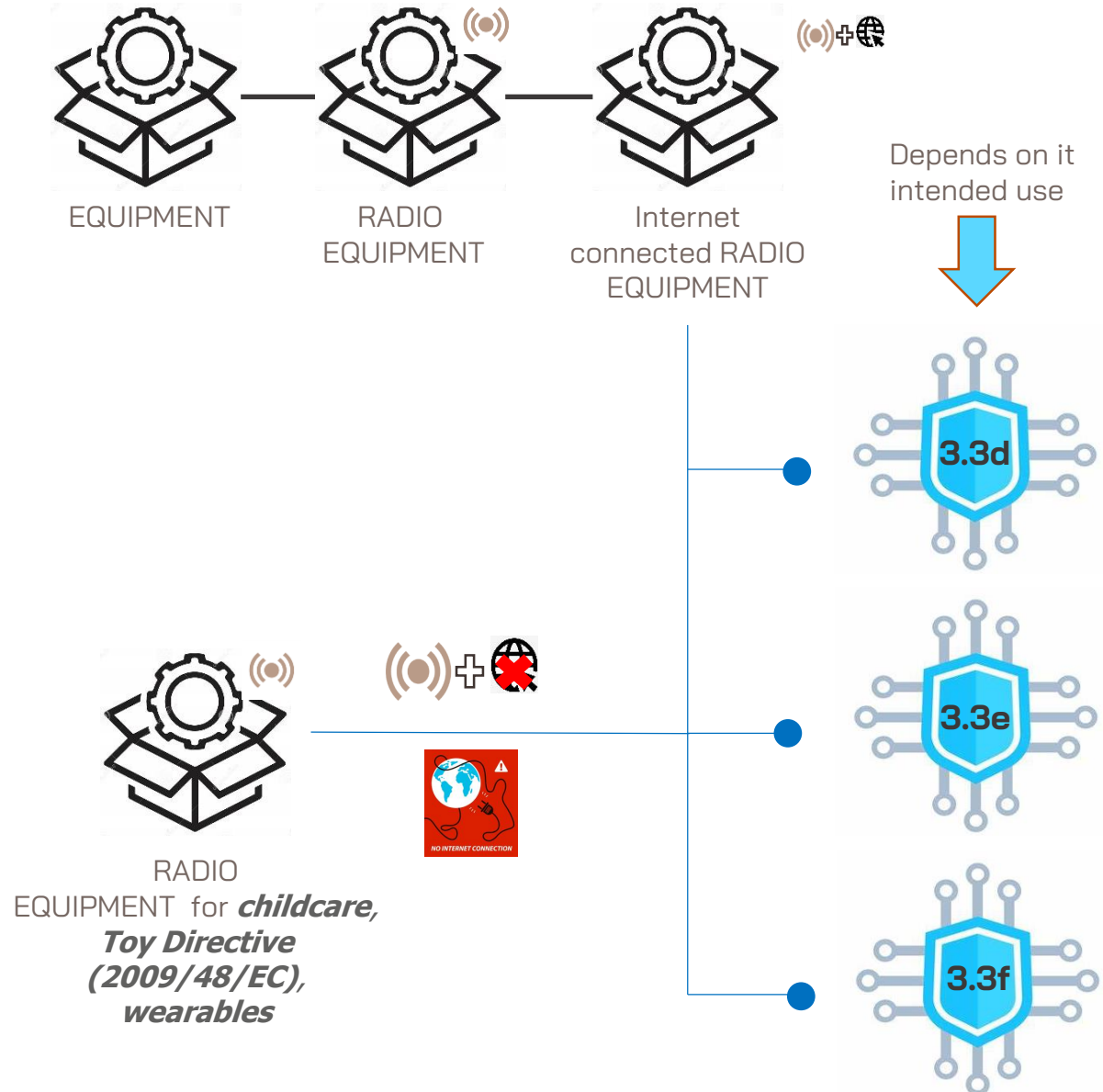
Internet protocols: TCP/IP, UDP, HTTP/HTTPS, FTP, SMTP, POP3/IMAP,

Wireless communication protocols: Wi-Fi, Bluetooth (some protocols), 3G/4G/5G, LTE-M/NB-IoT, NFC;

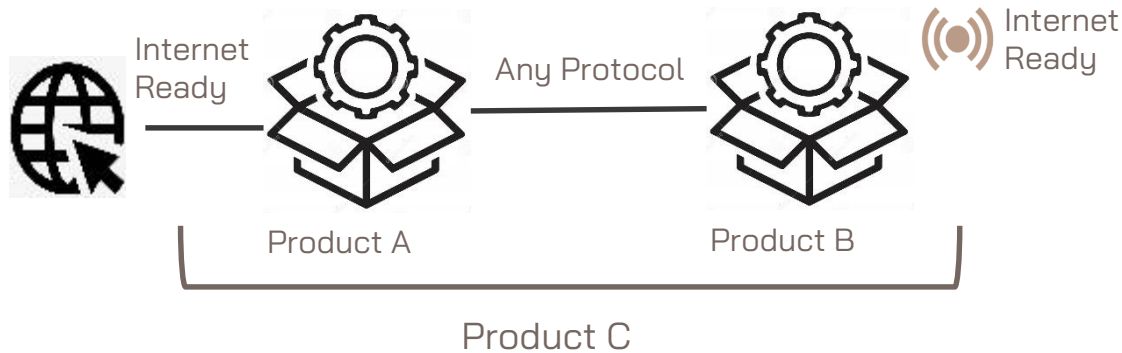
IoT protocols: MQTT, CoAP, etc.)

REMARK: internet-connected equipment → Is technology and protocol neutral

Regardless of whether they have "internet ready" capability, any products in the categories of childcare, toys, and wearable devices may still fall within the scope of the delegated regulation.



Representative examples for combined products



PRODUCT A	
Radio equipment according to 2014/53/EU?	NO The product has no radio interface and is not radio equipment according to the definition in 2014/53/EU.
"Internet-connected radio equipment"?	NOTAPPLICABLE
Product examples	Standalone network component, remotely controllable machinery

PRODUCT C	COMBINED EQUIPMENT
Radio equipment according to 2014/53/EU?	YES The product has a radio interface and is radio equipment according to the definition in 2014/53/EU.
"Internet-connected radio equipment"?	YES Regardless of whether Product A is within the scope of the delegated regulation, the combined equipment itself is capable of communicating over the internet via its radio interface ("wireless") and via its "wired" interface
Product examples	Combustion engine with a telematic device incorporated remote controllable machinery.

PRODUCT B	
Radio equipment according to 2014/53/EU?	YES The product has a radio interface and is radio equipment according to the definition in 2014/53/EU.
"Internet-connected radio equipment"?	YES The product itself is capable of communicating over the internet via its radio interface("wireless").
Product examples	Transmitter to a remote operating station.



Family of standards - EN 18031

Each of the 3 standards address one of the essential requirements defined in articles 3.3d, 3.3.e and 3.3.f of Directive 2014/53/EU.

- EN 18031-1:2024 Common security requirements for radio equipment – Part 1: Internet connected radio equipment
- EN 18031-2:2024 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
- EN 18031-3:2024 Common security requirements for radio equipment – Part 3: Internet connected radio equipment processing virtual money or monetary value

Document	Covers the essential requirements of	Addresses security assets and risks	Addresses network assets and risks	Addresses privacy assets and risks	Addresses financial assets and risks
EN 18031-1 (JT013058)	3.3.(d)	✓	✓	✗	✗
EN 18031-2 (JT013059)	3.3.(e)	✓	✗	✓	✗
EN 18031-3 (JT013060)	3.3.(f)	✓	✗	✗	✓

Main requirements in the three standards

- EN 18031-1 Common security requirements for radio equipment – Part 1: Internet connected radio equipment
- EN 18031-2 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
- EN 18031-3 Common security requirements for radio equipment – Part 3: Internet connected radio equipment processing virtual money or monetary value

! Note that the details of the requirements, the assessment criteria and the sub-requirements differ between the 3 harmonized standards.

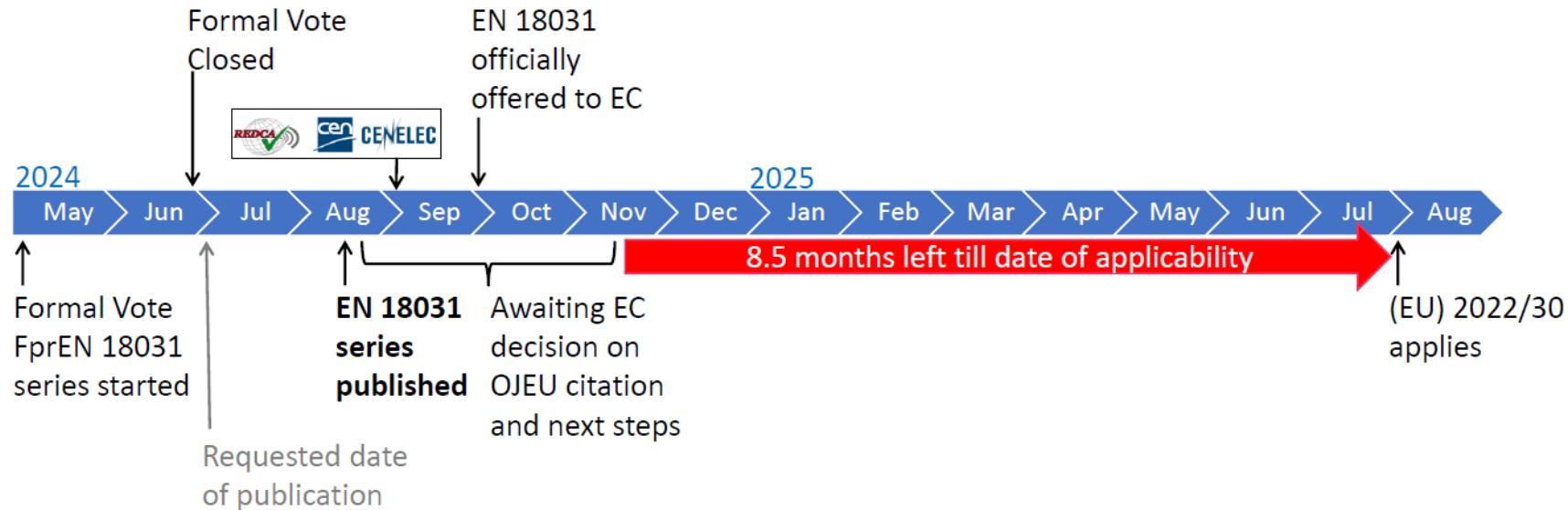
Requirement	-1	-2	-3
[ACM] Access control mechanism	✓	✓	✓
[AUM] Authentication mechanism	✓	✓	✓
[SUM] Secure update mechanism	✓	✓	✓
[SSM] Secure storage mechanism	✓	✓	✓
[SCM] Secure communication mechanism	✓	✓	✓
[LGM] Logging mechanism	-	✓	✓
[DLM] Deletion mechanism	-	✓	-
[UNM] User notification mechanism	-	✓	-
[RLM] Resilience mechanism	✓	-	-
[NMM] Network monitoring mechanism	✓	-	-
[TCM] Traffic control mechanism	✓	-	-
[CCK] Confidential cryptographic keys	✓	✓	✓
[GEC] General equipment capabilities	✓	✓	✓
[CRY] Cryptography	✓	✓	✓

ASSESSMENTS

The assessments are conducted by examining the documented assessment cases, not all assessment cases might be provided for every mechanism:

- **Conceptual assessment**
Examine if the provided documentation and rationale provide the required evidence (for example the rationale why a mechanism is not applicable for a specific network interface)
- **Functional completeness assessment**
Examine and test if the provided documentation is complete (for example use network scanners to verify that all external interfaces are properly identified, documented and assessed)
- **Functional sufficiency assessment**
Examine and test if the implementation is adequate (for example run fuzzing tools on a network interface to check if it is resilient to attacks with malformed data)

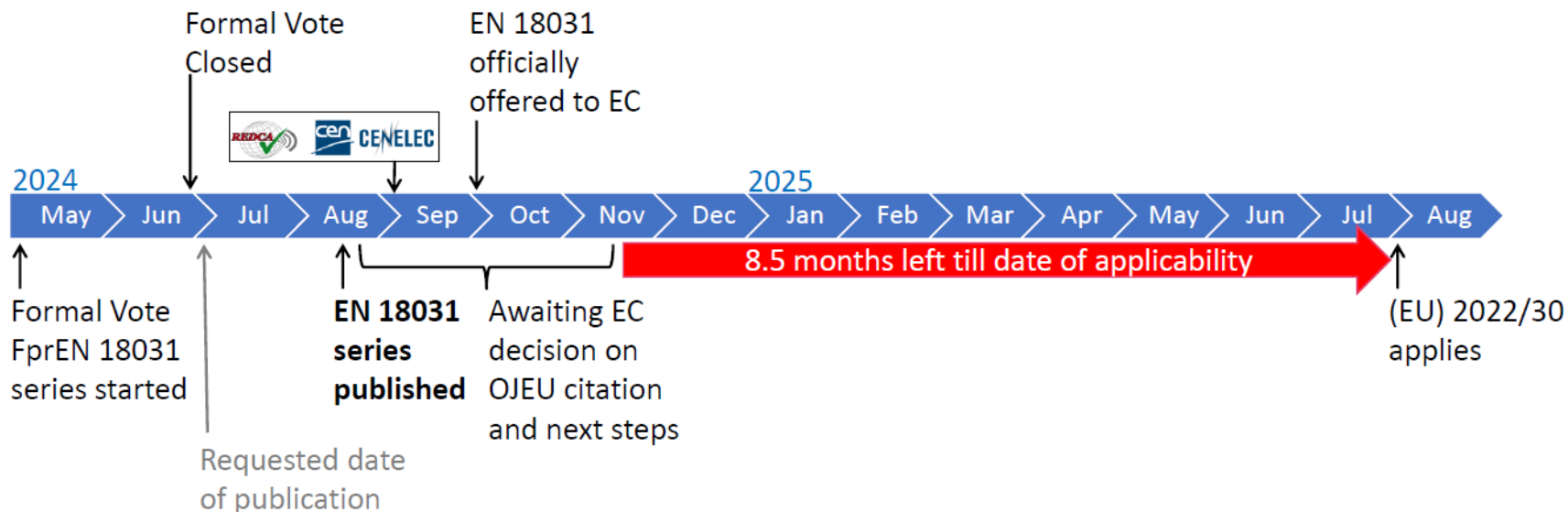
Timeline of the EN 18031 series



Despite the negative HAS assessment, CEN-CENELEC decided to move the three documents forward.

- ✓ The EN 18031-1:2024, EN 18031-2:2024 and EN 18031-3:2024 were published by CEN-CENELEC on the 14th of August 2024.
- ✓ The standards were directly (informally) provided to the commission.
- ✓ And officially offered to the commission on the 2nd of October.

Timeline of the EN 18031 series



If publication in the Official Journal of the European Union (OJEU) includes restrictions, the European Commission will provide guidance on how to interpret and implement these restrictions.

Now... We are awaiting decisions from the European commission (EC)

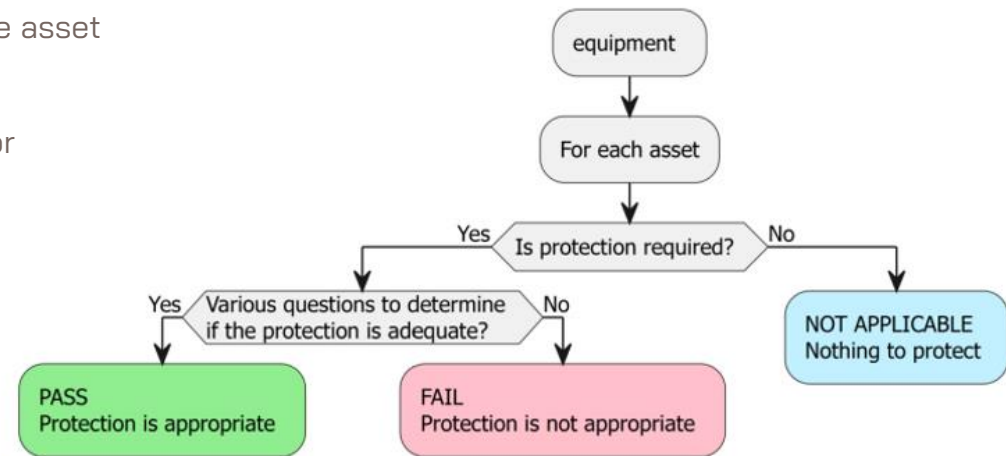
Regarding citation in the Official Journal of the European Union (OJEU) of the currently published standards, per standard the commission could decide to:

- ✓ Cite in full?
- ✓ Cite with restrictions?
- or
- ✓ Not to cite at all?

CEN/CENELEC defines a smart Decision tree for every mechanism

The “Decision Tree” restricts the freedom by asking “Yes/No” questions for the asset protection, intended use and intended operational environment of use.

More clear! Less confusing! It is added more specificity avoiding / reducing room for interpretation



However, this **new approach** also brings **challenges**, it is not intuitive to **define appropriate levels of security** where needed. **Work-intensive** as decision trees and classes have to be worked out and coordinated **edge cases** may appear for requirements under both “application” and “appropriateness”, which might exclude the intended use of specific equipment

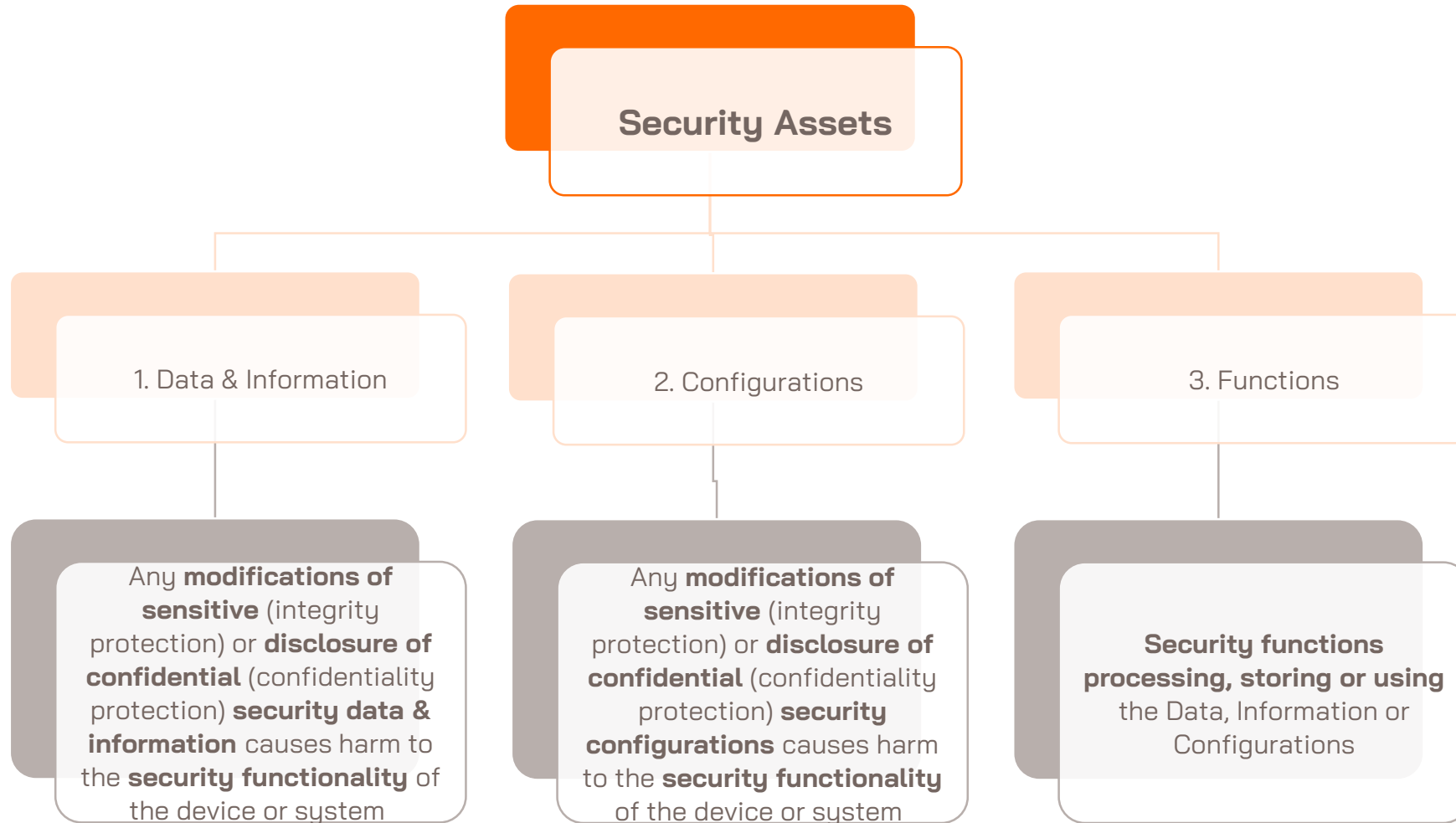


Effects on assessment criteria: Old approach required manufacturer to create a **risk analysis for each requirement** in the harmonized standard including intended use and environment.

New approach requires “evaluator” to utilize the information of the manufacturer's technical documentation and to go through the predefined **decision tree**

The evaluator typically has subject-specific expertise and a respective role with the manufacturer

EN18031 Asset Sorting Logic



EN18031 Asset Sorting Logic

Security assets

a **Security Functions**

- Access control mechanism
- Authentication mechanism
- Secure update mechanism
- Secure storage mechanism
- Secure communication mechanism
- Resilience mechanism
- Network monitoring mechanism
- Traffic control mechanism
- ...

b **Security Parameters**

- sensitive security parameter
- confidential security parameter

c **Confidentiality encryption keys**

- Symmetric encryption keys
- Asymmetric private keys
- Session keys
- Key derivation parameters
- ...

d **Security Config.**

- Firewall rules
- Encryption keys
- Access control lists
- Passwords/PINs
- Security logs
- ...

EN18031 Asset Sorting Logic

Network assets

a Network function and services

- Routing
- Switching
- Firewall
- VPN
- DNS
- Web
- Email
- File transfer
- Remote access
- ...

b Sensitive network function configurations

- Access control list (ACL) config
- Routing table configurations
- Firewall rules
- VLAN configurations
- QoS settings
- IDS and IPS settings
- Wireless network security settings
- Remote access and authentication policy configurations
- Network monitoring mechanism configurations
- Traffic control mechanism configurations...

c Confidential network function configurations

- VPN passwords
- Wi-Fi passwords
- Encrypted communication settings
- Encryption algorithm and key management configurations
- Privileged access management configurations
- Security log and audit configurations
- Data leak prevention (DLP) system settings
- CCK) configurations
- Security communication mechanism (SCM) configurations, including integrity, authenticity, and confidentiality protection
- ...

EN18031 Asset Sorting Logic

Privacy assets

a Sensitive privacy assets

- a) Personal basic information:
 - Name
 - Contact information (phone number, email address)
 - Address
- b) Device identification information:
 - Device ID
 - MAC address
 - IP address
- c) Location data
 - GPS coordinate history
- d) Settings for collecting privacy data
 - ...

b Confidential privacy assets

- a) Authentication credentials:
 - hashes diegist
 - Biometric data (fingerprint, facial recognition data)
 - Two-factor authentication keys
- b) Location data:
 - Common location information
 - Location tracking data
- ...

c Assets related to children's privacy devices

- a) Children's privacy function settings
 - Parental control functions
 - Content filters
 - Dedicated children's mode
- b) Personal information processed by the device related to children
 - Children's identity information
 - Usage history
 - Location data
- ...

EN18031 Asset Sorting Logic

Financial assets

a Confidential financial assets

Manipulating such financial data could lead to fraud

Account balances

Transaction details

Payment settings

...

b Sensitive financial assets

Leaking such financial data could lead to fraud

Credit card full numbers, CVV codes,

Digital wallet information:

Cryptocurrency private keys,

Wallet addresses,

Transaction signature keys,

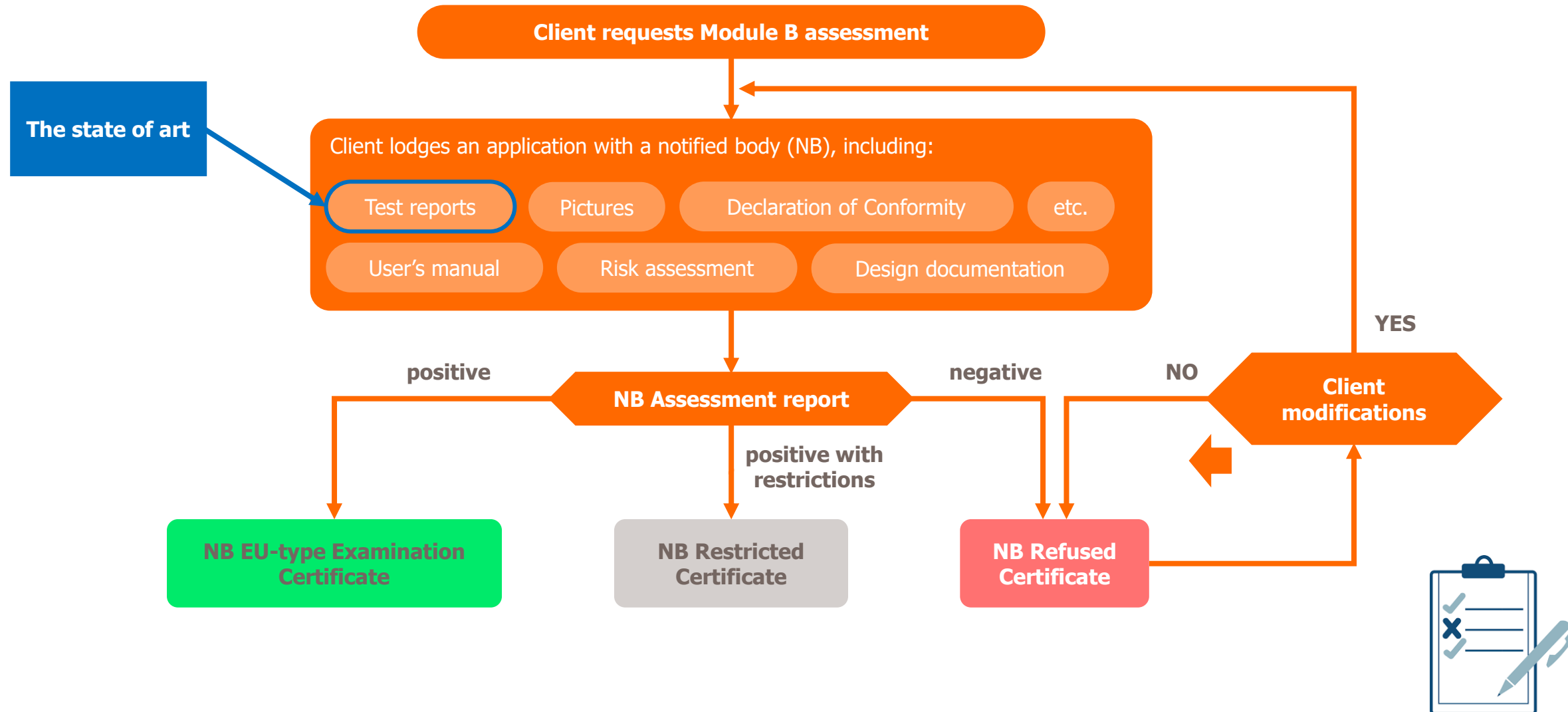
Payment vouchers:

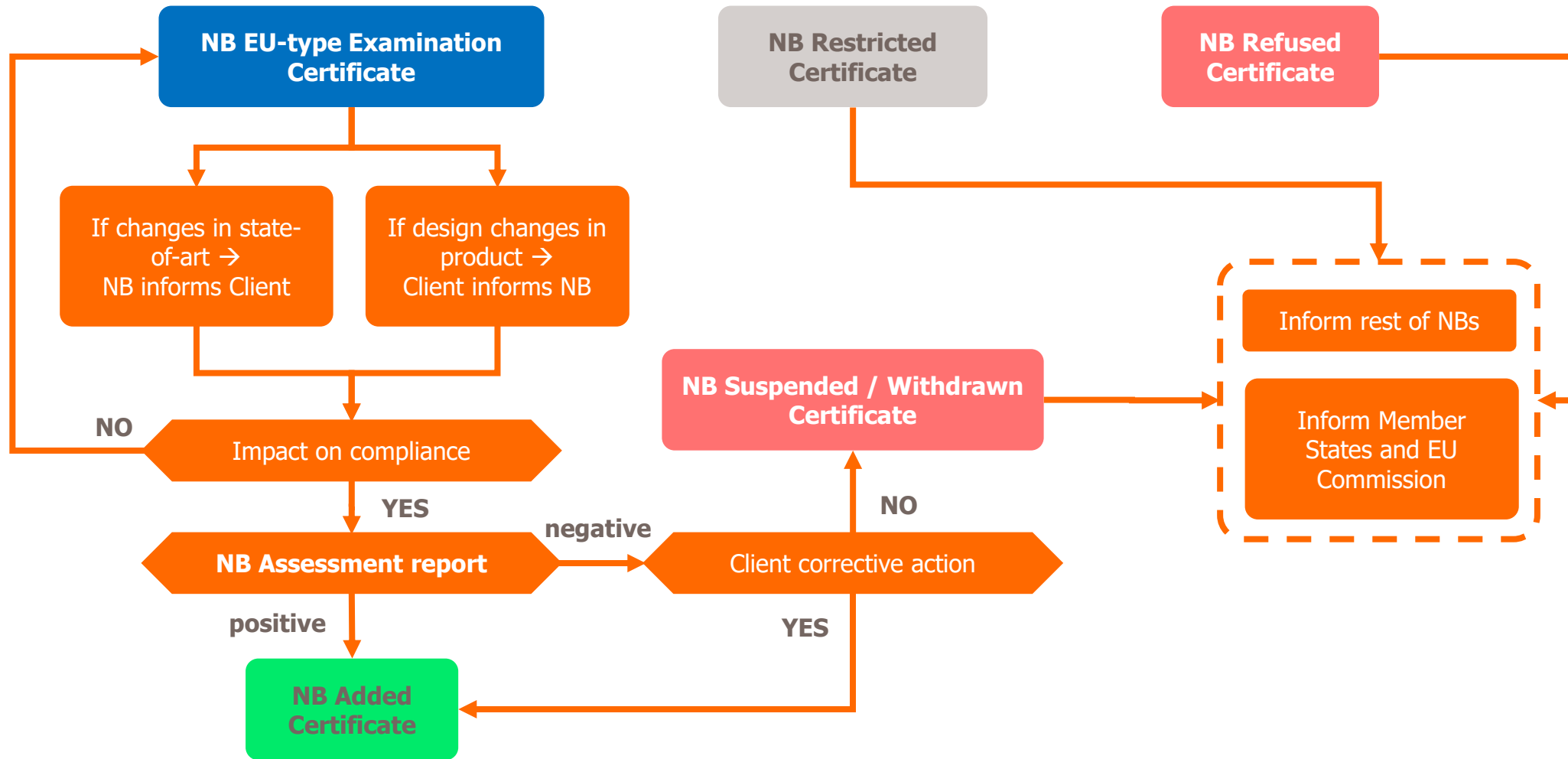
Payment tokens

Electronic check information

Digital signatures

• ...





Obligations to manufacturers

Ensure compliance:

- Ensure that the design and manufacture of radio equipment comply with the essential requirements in Article 3.
- Ensure that radio equipment can be used normally in at least one Member State without violating radio spectrum regulations.

Technical documentation and compliance assessment:

- Prepare technical documentation and carry out the appropriate compliance assessment procedure.
- Retain technical documentation and EU Declaration of Conformity for at least 10 years.

Product identification, conformity marking, and declaration:

- CE marking [768/2008/EC]
- EU Declaration of Conformity, and retain for 10 years
- Mark the model, batch/serial number on the product, and the name/registered trademark/address of the manufacturer

Product information and instructions:

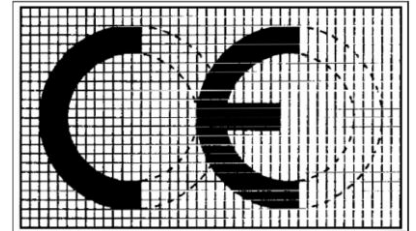
- Instructions for use and safety information in understandable language
- Provide information on the intended use, frequency bands used, and maximum transmission power

Importers and distributors' responsibilities:

- When placing on the market under their own name or trademark, they assume the manufacturer's responsibilities.
- Ensure that modifications to the product still comply with the Directive requirements.

Authorized representatives:

- Can appoint authorized representatives to perform certain specific tasks, but not the core responsibilities of ensuring product compliance and preparing technical documentation.



BE	BG	CZ	DK	DE	EE
UK	EL	ES	FR	HR	IT
LV	LT	LU	HU	MT	NL
PL	PT	CH	RO	SI	SK
IE	CY	AT	FI	SE	TR
IS	LI	RS	NO		

RED (2014/53/EU) Article 10.10
 Information on restrictions

RED DA Certification Strategy:

1. Certification Strategy for Combined Products:

Devices that can be tested independently are certified separately; devices that cannot be tested independently are based on the overall combination, and a DoC (Declaration of Conformity) is issued for multiple independent devices.

Products sold in combination need to assess the impact of individual devices on the whole.

2. Improvement of Certification Efficiency:

Certifying wireless modules separately can simplify the evaluation process.

host products can undergo incremental testing and evaluation based on the certified modules with networking capabilities and security features.

3. Standard Applicability:

The EN 18031 series of standards will be used for EU RED certification, which is currently under discussion;

Before EN 18031 is harmonized, EN 303 645 and EN 62443-4-2 will still be considered for consumer IoT products and industrial products. If there is no harmonized standards, certification bodies will consider using appropriate specifications for cybersecurity certification. However, the current versions of the published 18031 series include appendices (informative) which disclose the mapping to EN IEC 62443-4-2: 2019 and ETSI EN 303 645.

4. The Main Differences Between EN 18031 and EN 303 645 Include:

EN 18031 is based on a decision tree for assessment, conducting risk assessment/threat modeling according to the identification of four types of assets.

EN 18031 does not have IXIT or ICS as in EN 303 645; certification bodies will provide new relevant templates. The document logic is based on a decision tree, but the content is similar.

RED DA Certification Strategy: Mapping EN IEC 62443-4-2 and ETSI EN 303 645

EN IEC 62443-4-2 (Source Annex A EN 18031-1:2024)

Req.ID	EN IEC 62443-4-2:2019
GEC-1	Not covered by a CR in EN IEC 62443-4-2:2019

EN IEC 62443-4-2 (Source Annex A EN 18031-2:2024)

Req.ID	EN IEC 62443-4-2:2019
ACM-3; ACM-4; ACM-5; ACM-6; UNM-1; UNM-2; GEC-1	Not covered by a CR in EN IEC 62443-4-2:2019

EN IEC 62443-4-2 (Source Annex A EN 18031-3:2024)

Req.ID	EN IEC 62443-4-2:2019
GEC-1	Not covered by a CR in EN IEC 62443-4-2:2019

ETSI EN 303 645 (Source Annex A EN 18031-1:2024)

Req.ID	ETSI EN 303 645 Provision: rationale
AUM-3; SCM-2; NMM-1; TCM-1; CCK-1; GEC-3; GEC-4	Not covered in EN 303 645

ETSI EN 303 645 (Source Annex A EN 18031-2:2024)

Req.ID	ETSI EN 303 645 Provision: rationale
ACM-3; ACM-4; AUM-3; SCM-2; LGM1; LGM-2; LGM-3; LGM-4; CCK-1; GEC-3; GEC-4	Not covered in EN 303 645

ETSI EN 303 645 (Source Annex A EN 18031-3:2024)

Req.ID	ETSI EN 303 645 Provision: rationale
AUM-3; LGM1; LGM-2; LGM-3; LGM-4; CCK-1; GEC-3; GEC-4;	Not covered in EN 303 645



Is it mandatory for the manufacturer certify their product under Cyber article 3.3 d/e/f?



Yes, but not before 1st of August 2025

Is it mandatory to go through the Notified Body or DoC will be enough?



NB will be mandatory In case that non-HSs have been published or if the manufacturer doesn't fully apply those HSs. If HS's are available then DoC or NB on a voluntary basis will be ok.



Which products are under this scope of Cyber?



First of all, the new delegated act 2022/30 Cyber only applies to Radio products, if so, then the manufacturer must evaluate the intended use of their device against the articles 3,3 d/e/f.

Are there any impacts on existing/legacy devices?



Old devices, which have already been placed on the EU market, can continue to be used without the need for specific adaptations until the end of their life cycle.



Thanks!



Join us on



TESTING AND CERTIFICATION CENTER

www.appluslaboratories.com