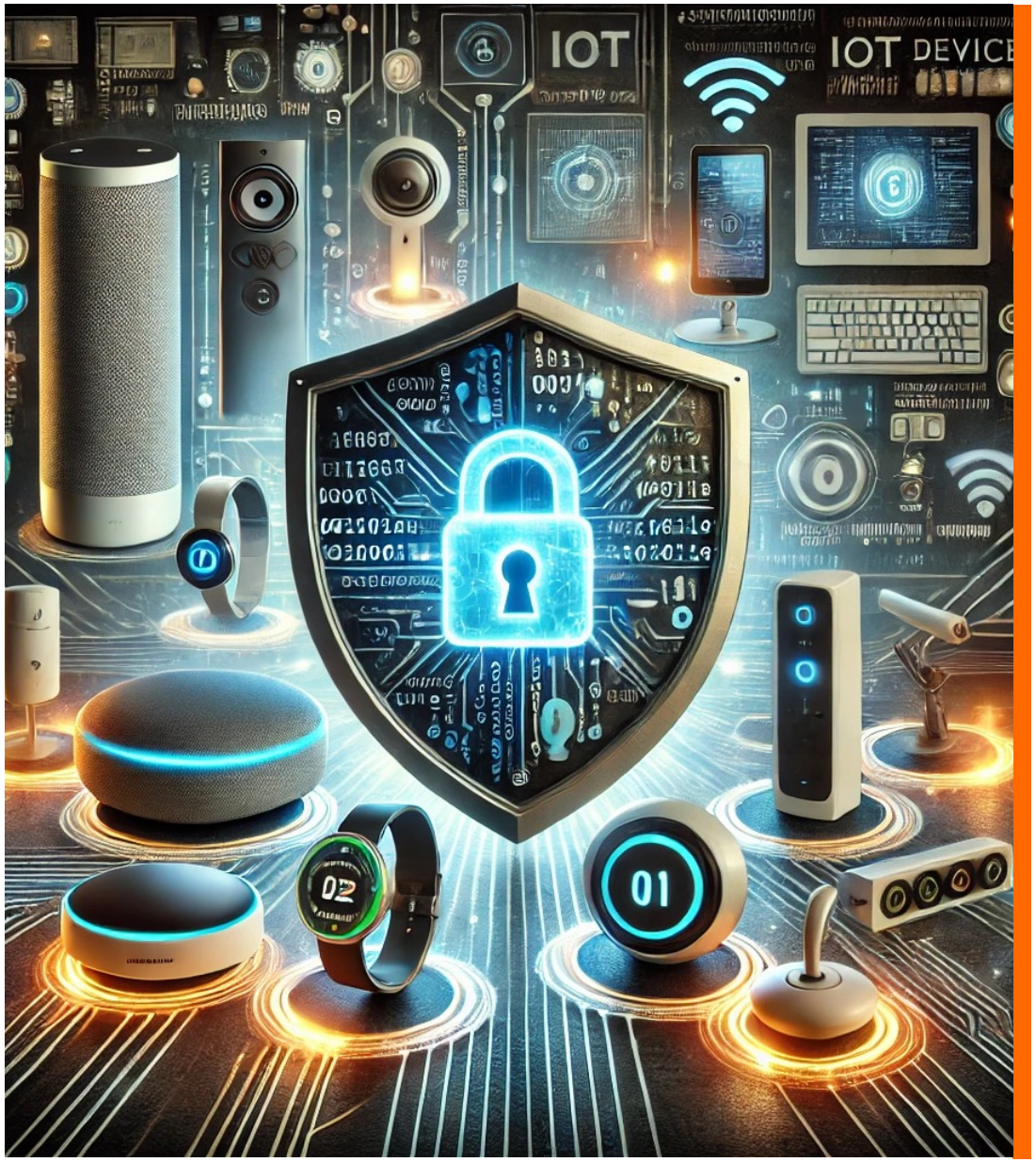
# RED Cybersecurity Delegated Act

## Understanding the cybersecurity requirements and EN 18031

25th of September 2025

**NÚRIA CARRIÓ**

**Public**



# AGENDA

## 01 INTRODUCTION

The RED delegated Act activates the cybersecurity articles for radio equipment connected to internet.

What is RED-DA based on?

## 02 SCOPE

Understanding the scope of the RED-DA is crucial to understand its applicability in internet connected equipment products.

## 03 EN 18031: The hEN standard

EN 18031 is the harmonised standard applied to internet-connected radio equipment, including smart home devices, wearable technology, toys with wireless connectivity, and other consumer products that transmit or receive radio signals and connect to the internet.

## 04 REQUIREMENTS

EN 18031 mandates that internet-connected radio equipment must implement essential security measures to protect network integrity, user data confidentiality, and financial transaction security. The standard also specifies requirements for hardware security.

## 05 ASSESSMENT

The assessment process in EN 18031 combines clear, objective requirements with a technology-agnostic approach, allowing manufacturers flexibility in their implementations. Compliance is demonstrated through documentation detailing how requirements are met, serving as input for testing to verify the actual security of the equipment.

## 06 MAPPINGS

EN 18031 demonstrates how complying with the security provisions of ETSI EN 303 645 can serve as a helpful framework for radio equipment manufacturers to meet the corresponding security requirements outlined in EN 18031.


# 01 INTRODUCTION

The RED delegated Act activates the cybersecurity articles for radio equipment connected to internet.

What is RED-DA based on?

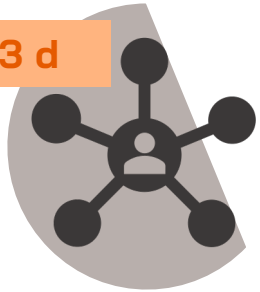
1st August **Applicable**

**January 2022** — **August 2024** — **August 2025**

**PUBLICATION**

**Extension** period for implementation of harmonized standards

**Article 3.3 d**

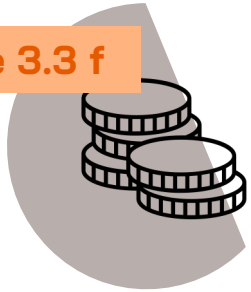


Network Security

**Article 3.3 e**

Personal Data and Privacy Protection

**Article 3.3 f**

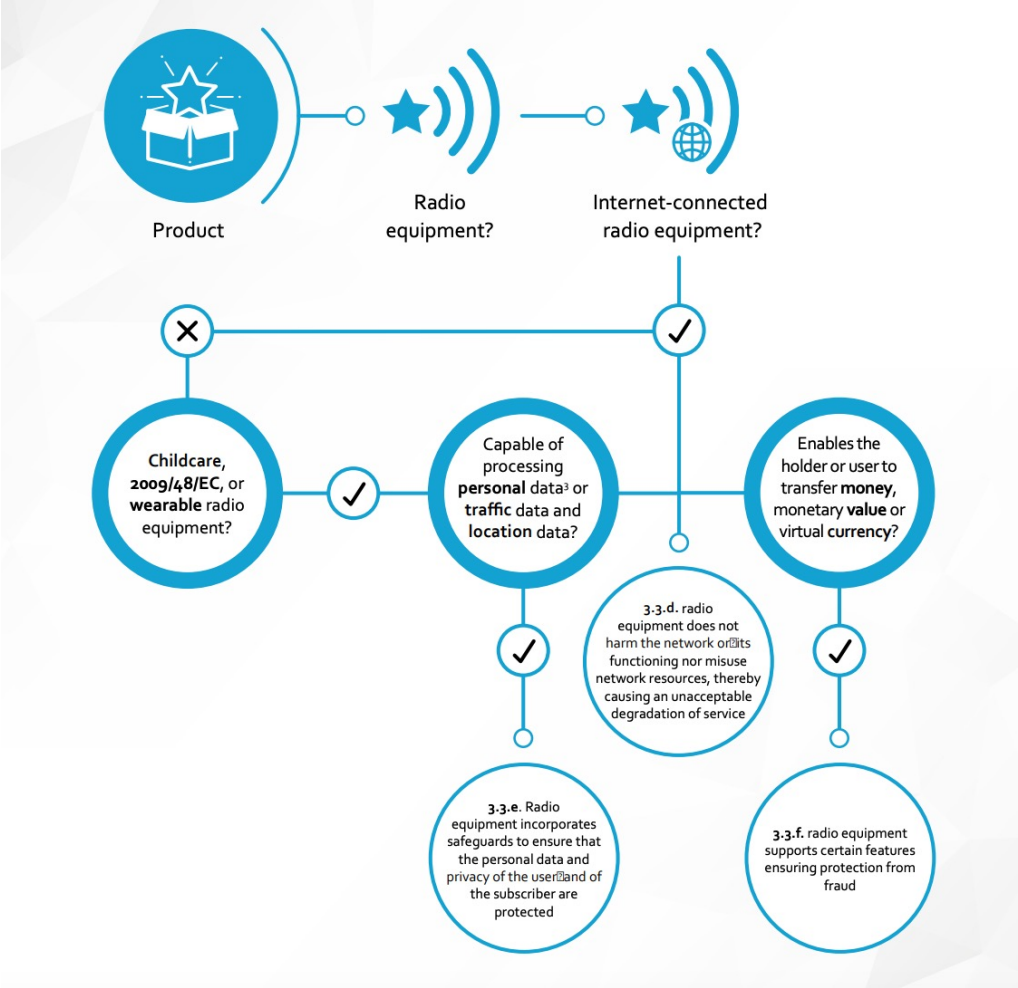


Protection from Fraud


# 02 SCOPE

Understanding the scope of the RED-DA is crucial to understand its applicability in internet connected equipment products.

# Which standard applies to my product?




Source: Orgalim, 13 September 2022, Common understanding of the term "Internet-connected radio equipment"

## 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 Articles3.3(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.

## 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.

# HOW TO COMPLY WITH THE ARTICLES? HARMONISED STANDARDS

**HARMONISED STANDARDS**
*Published in the "Official Journal Of EU"*

provides...

**PRESSUMPTION OF CONFORMITY**

which means...

*"If your product is conformant with harmonised standards it is presumed that your product comply with the cybersecurity articles"*

# The hEn consist in three parts covering the different RED cyber articles 3.3(d,e,f):

## EN 18031-1

**RED: 3.3 (d)**

Ensure network protections: not harm the network nor misuse network resources

Common security requirements for general internet-connected radio equipment

Applicable to: all internet connected radio equipment.

Addressing security and network risks inherent in such devices

## EN 18031-2

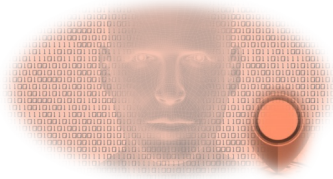
**RED: 3.3 (e)**

Ensure protection of personal data and privacy of the user / subscriber

Focused on radio equipment that processes personal, traffic, or location data.

Applicable to: all internet connected radio equipment, Childcare radio equipment, Toys radio equipment and Wearable radio equipment.

Addressing specific security and privacy risks associated with these devices.



## EN 18031-3

**RED: 3.3 (f)**

Ensure protection from fraud

Focused on Internet connected radio equipment processing virtual money or monetary value.

Applicable to: devices that transfer money, monetary value, or virtual currency.

Addressing security and financial risks inherent in such devices.

## YES! EN 18031 is hamonised BUT... WITH RESTRICTIONS!!


**DECISIÓN DE EJECUCIÓN (UE) 2025/138 DE LA COMISIÓN**

- Passwords.
- Childcare and parental control.
- Secure update mechanisms.

# 4 restrictions, 3 important to take into account

- **Passwords**

6) Las cláusulas 6.2.5.1 y 6.2.5.2 de las normas armonizadas EN 18031-1:2024, EN 18031-2:2024 y EN 18031-3:2024 tratan sobre las contraseñas por defecto. Estas cláusulas ofrecen a los fabricantes la posibilidad de permitir que un usuario no establezca ni utilice una contraseña. Se considera que, si se aplica esta opción, no se abordarán adecuadamente los riesgos de autenticación pertinentes y, por tanto, no se garantizaría la conformidad con los requisitos esenciales establecidos en el artículo 3, apartado 3, párrafo primero, letras d), e) y f), de la Directiva 2014/53/UE.

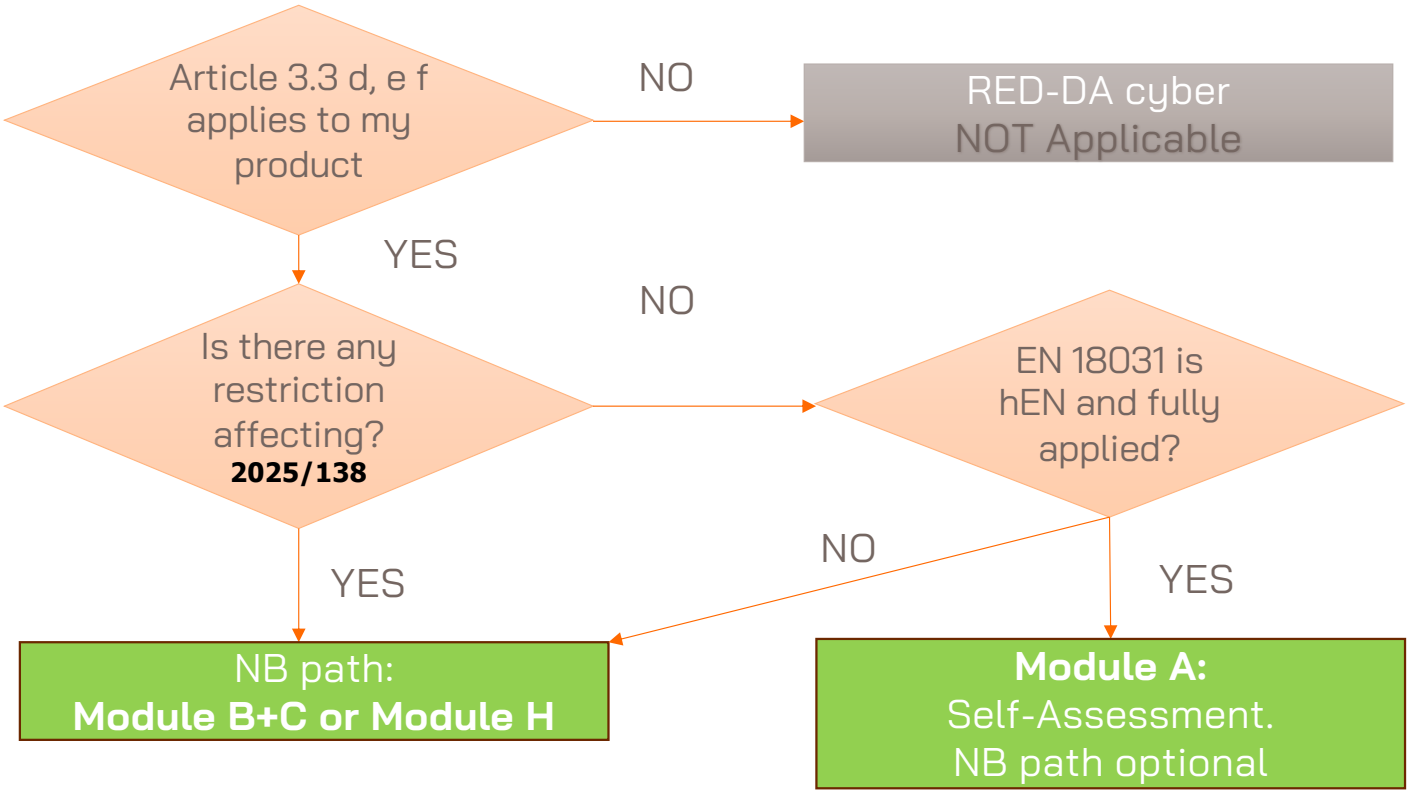
- **Toys and Childcare parental control**

(7) Las cláusulas 6.1.3, 6.1.4, 6.1.5 y 6.1.6 de la norma armonizada EN 18031-2:2024 incluyen especificaciones sobre el mecanismo de control de acceso de los equipos radioeléctricos para juguetes y de los equipos radioeléctricos para el cuidado infantil. Más concretamente, las categorías de aplicación descritas en las subsecciones «criterios de evaluación» son las siguientes: control de acceso basado en funciones, control de acceso discrecional, control de acceso obligatorio u otros. Algunas de estas categorías podrían no ser compatibles con el control parental o de los tutores. En ese caso, se considera que, si no se aplica el control parental o de los tutores, no se abordarán los riesgos de autenticación pertinentes y, por tanto, no se garantizaría la conformidad con el requisito esencial establecido en el artículo 3, apartado 3, párrafo primero, letra e), de la Directiva 2014/53/UE.

- **Secure Update**

(8) La cláusula 6.3.2.4 de la norma armonizada EN 18031-3:2024 incluye criterios de evaluación para las actualizaciones seguras. Se establecen cuatro categorías de aplicación diferentes, basadas en las firmas digitales, los mecanismos de comunicación seguros, los mecanismos de control de acceso u otros. Ninguno de los métodos por sí solo es suficiente para el tratamiento de los activos financieros. Se considera que los criterios de evaluación no abordan adecuadamente los riesgos de autenticación pertinentes y, por tanto, no pueden garantizar la conformidad con el requisito esencial establecido en el artículo 3, apartado 3, párrafo primero, letra f), de la Directiva 2014/53/UE.

## Third party (NB) or self-assessment?



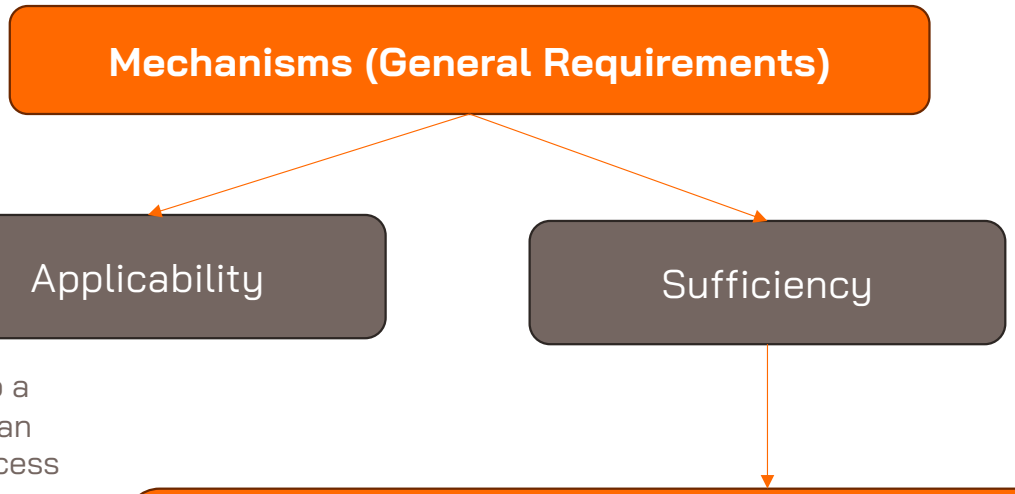

# 03 EN 18031: The hEN standard

EN 18031 is the harmonised standard applied to internet-connected radio equipment, including smart home devices, wearable technology, toys with wireless connectivity, and other consumer products that transmit or receive radio signals and connect to the internet.

- The security requirements presented in this **EN 18031 standard** are developed to improve the ability of radio equipment to protect its assets against common cybersecurity threats and to mitigate publicly known exploitable vulnerabilities.

- The **EN 18031 standard** specifically addresses a set of technical requirements that manufacturers must meet to demonstrate compliance with the essential requirements of the RED. By following this harmonized standard, manufacturers can benefit from a **presumption of conformity,** streamlining their path to market.

- Became mandatory on **August 1st, 2025**.




- Which access control does it have?
  - **Password**
  - **Secure channel**

- Access control Mechanism to a confidential file, it is this file an asset? Does this file have access control?

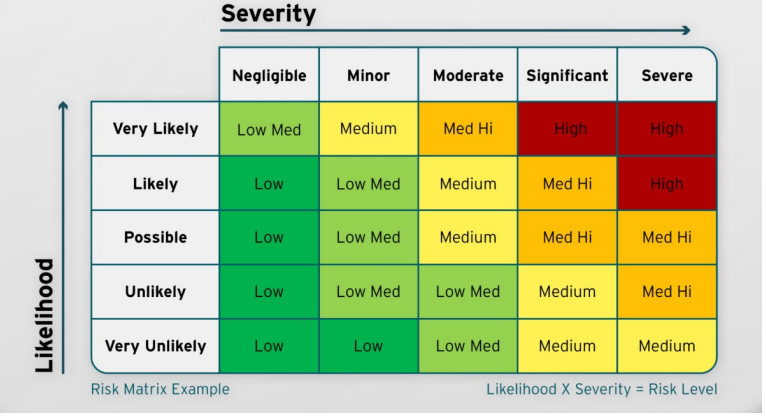
- This decision process is applied to each individual item or aspect of the equipment. For example, the need for a particular security mechanism might be different for each external interface on the device**. Testing on robustness of the existence** of the password, best practices...


# 04 REQUIREMENTS

EN 18031 mandates that internet-connected radio equipment must implement essential security measures to protect network integrity, user data confidentiality, and financial transaction security. The standard also specifies requirements for hardware security.

## I'm A MANUFACTURER WHERE TO START?

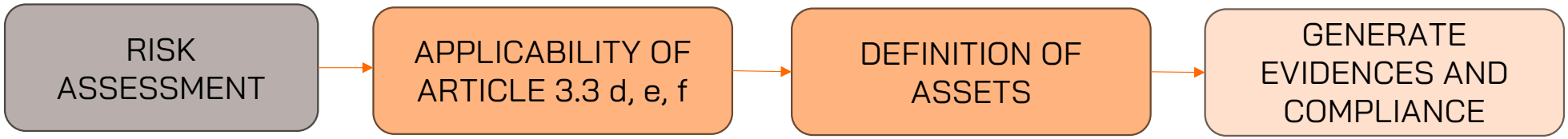
- **Risk-Based Approach**: All parts emphasize a risk-based approach, requiring **manufacturers** to assess and mitigate cybersecurity risks throughout the product lifecycle.





**MANDATORY** RISK ASSESSMENT TO BE PERFORMED by THE MANUFACTURER.

YOU CAN USE THE METHOD YOU WANT☺




## RISK ASSESSMENT

The manufacturer shall perform a **risk assessment** which would allow to them to determine:

- The product security measures to be implemented to cover cybersecurity.
- Applicability of Art. 3.3 d, e or f.
- Definition of assets.
- Choose appropriate compliance standard (ETSI 303 645, EN 18031...)

## Risk assessment and Assets

- **Security Asset**: This encompasses any data, system, or resource that is critical for maintaining the confidentiality, integrity, and availability of information. **Security assets are subject to all three essential requirements (3.3.d, 3.3.e, and 3.3.f).**
- **Network Asset**: This category includes all the components that make up a network infrastructure, such as servers, routers, switches, firewalls, and other network devices. **Network assets are primarily associated with requirement 3.3.d.**
- **Privacy Asset**: This refers to any information that relates to an individual's personal identity and privacy, such as names, addresses, social security numbers, health records, and financial information. **Privacy assets are primarily subject to requirement 3.3.e.**
- **Financial Asset**: This category encompasses any monetary resources or assets that have financial value, such as cash, investments, bank accounts, and financial instruments. **Financial assets are subject to requirement 3.3.f.**

| Essential requirement | 3.3.d | 3.3.e | 3.3.f |
|---|---|---|---|
| Security asset | ✓ | ✓ | ✓ |
| Network asset | ✓ | | |
| Privacy asset | | ✓ | |
| Financial asset | | | ✓ |

## Access Control Mechanism (ACM)

**The equipment shall have appropriate access control mechanisms to manage access to security/network assets and shall ensure only authorize entities have access.**

## Authentication Mechanism (AUM)

**Authentication Mechanism shall be present for managing access to read, modify or use network function configuration or security parameters.**

## Secure Updates (SUM)

**Secure update mechanism is present and new software can be installed with integrity and authenticity.**

## Secure Storage Mechanism (SSM)

**Secure Storage mechanism shall be present to protect assets for confidentiality and integrity properties.**

## Secure Communication Mechanism (SCM)

**Secure Communication mechanism shall exist to protect communication of assets and be a secure mechanism to gain integrity, authenticity confidentiality and anti-replay properties.**

## Resilience Mechanisms (RSM)

**Mitigate effects of DDoS (Denial of Service)**

## Network Monitoring Mechanism (NMM)

**To detect attacks of DDOs.**

## Traffic Control Mechanism (TCM)

**Mechanism to detect malicious behavior.**

## Confidential cryptographic keys (CCK)

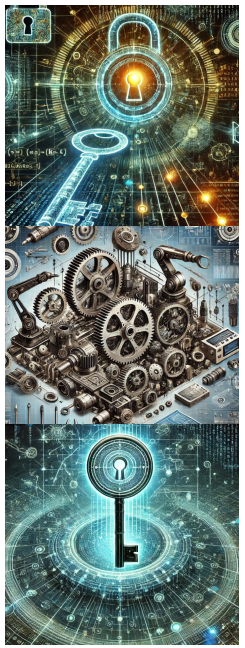
Verify the appropiateness of the keys, of the generation mechanisms, preventing static values of the keys

## General equipment capabilities (GEC)

Up-to-date software and hardware with no publicly known exploitable vulnerabilities  and limit exposure services via related network interfaces as well as configuration of optional servcies, exposure of physical interface only when needed.

## CRY: Cryptography (CRY)

Best practice cryptography




# 05 ASSESSMENT

The assessment process in EN 18031 combines clear, objective requirements with a technology-agnostic approach, allowing manufacturers flexibility in their implementations. Compliance is demonstrated through documentation detailing how requirements are met, serving as input for testing to verify the actual security of the equipment.

- **Assessment Approach**

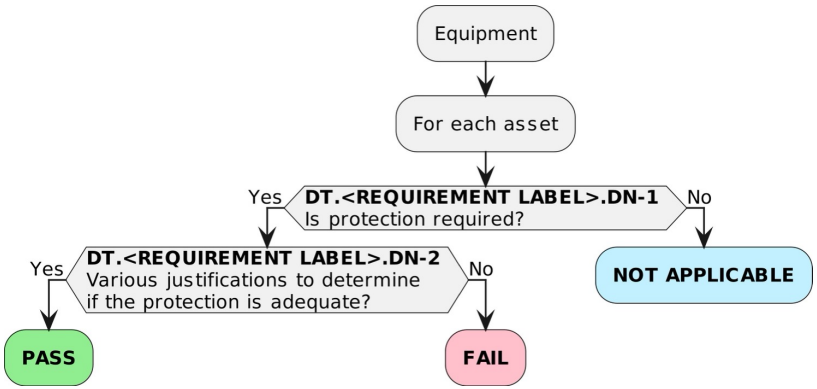
➢ **Documentation Review:** Manufacturers must provide detailed **technical documentation** that describes the security measures they have implemented.

➢ **Testing:** The equipment undergoes **actual testing (functional testing + security testing)** to verify that it behaves as documented and meets the security objectives.

| Clause # | Title |
|---|---|
| 6.x | XXX Mechanism |
| 6.x.1 | XXX-1 Applicability of mechanisms |
| 6.x.1.1 | Requirement |
| 6.x.1.2 | Rationale |
| 6.x.1.3 | Guidance |
| 6.x.1.4 | Assessment criteria |
| 6.x.1.4.1 | Assessment objective |
| 6.x.1.4.2 | Implementation categories |
| 6.x.1.4.3 | Required information |
| 6.x.1.4.4 | Conceptual assessment |
| 6.x.1.4.5 | Functional completeness assessment |
| 6.x.1.4.6 | Functional sufficiency assessment |

- **Justification Evaluation (Decision Tree)**

➢ **Guide Security Assessments:** Decision trees help determine if specific security requirements are applicable and, if so, whether the implemented protection is adequate for a particular piece of equipment and its intended use.




| Clause # | Title |
|---|---|
| 6.x | XXX Mechanism |
| 6.x.1 | XXX-1 Applicability of mechanisms |
| 6.x.1.1 | Requirement |
| 6.x.1.2 | Rationale |
| 6.x.1.3 | Guidance |
| 6.x.1.4 | Assessment criteria |
| 6.x.1.4.1 | Assessment objective |
| 6.x.1.4.2 | Implementation categories |
| 6.x.1.4.3 | Required information |
| 6.x.1.4.4 | Conceptual assessment |
| 6.x.1.4.5 | Functional completeness assessment |
| 6.x.1.4.6 | Functional sufficiencv assessment |


# 06 MAPPING

EN 18031 demonstrates how complying with the security provisions of ETSI EN 303 645 can serve as a helpful framework for radio equipment manufacturers to meet the corresponding security requirements outlined in EN 18031.

- Mappings with other well-known standards are in EN 18031:
  - SESIP.
  - ETSI 303 645.
  - IEC 62443-4-2.
  - NB or client can also perform their own mappings provided there are some cybersecurity certifications already being used in the market.


# 07 CONCLUSION

RED-DA conclusions and best practices

## Best practices to have in mind

- **Design with Security in Mind, security by default and define your risk assessment.**
  Integrate cybersecurity from the earliest design stage (*security by design*), not as an afterthought.
- **Ensure your product is delivered with no vulnerabilities.**
  The product shall be delivered with no known vulnerabilities.
- **Protect your assets. Make a list and define strong countermeasures. These includes user's data and privacy.**
  Safeguard your intellectual property, cryptographic keys, firmware, and internal processes against tampering or theft.
  This also reduces the risk of counterfeit products and helps maintain trust in your brand.
- **Enable secure updates.**
  Provide a way to update devices securely so vulnerabilities can be fixed throughout the product's lifecycle.
- **Apply Harmonised Standards when possible**
  Use harmonized EU standards (like the EN 18031 series) as guidance to demonstrate compliance.
- **Document and Demonstrate Compliance**
  Keep clear records (risk analysis, test reports, design decisions) to show authorities that requirements are met.


- If you are a manufacturer, follow the first steps:
  - Make a **risk assessment.**
  - Prepare the **evidence** lists and structure content.
  - Check **supporting documents** such as 'Blue guide'.

"THE RED **HAS BEEN REPEALED** BY 2027, BUT CRA (Cyber Resilience Act) is on the CORNER. Get prepared"

- **BLUE GUIDE and RED GUIDE**: EU Commission 'Blue Guide' on the implementation of EU product rules, 2022 for single market. What does place on the market means and other rules to enter the single market.
  Blue Guide: https://single-market-economy.ec.europa.eu/news/blue-guide-implementation-product-rules-2022-published-2022-06-29_en
  RED Guide: https://ec.europa.eu/docsroom/documents/33162
- Risk Assessment methods defined by ETSI. What methods of risk assessment exist?
  - https://www.etsi.org/deliver/etsi_tr/103900_103999/103935/01.01.01_60/tr_103935v010101p.pdf
- Eu Risk Assessment Methodology general:
  - https://ec.europa.eu/docsroom/documents/17107
- Impact Assessment on Increased Protection of Internet-Connected Radio Equipment and Wearable Radio Equipment
  - https://ec.europa.eu/docsroom/documents/40763
- Applus webinars for RED-DA compliance :
  - https://www.youtube.com/watch?v=J20nr8RXh3o
  - https://www.youtube.com/watch?v=vDk5aMwhmgE

# 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**


Applus laboratories

Applus laboratories

# Q&A

Thanks!

Applus laboratories