Choose Scandinavian trust

Cybersecurity in Europe
The harmonized standard

Nemko

2025-02-25

Cybersecurity in Europe at a glance

- **1 Aug 2025** cybersecurity is part of CE marking for wireless products (RED)
- **11 Dec 2027** cybersecurity is part of CE marking for all products / SW (CRA)
- Compliance needs to be documented by use of **Harmonized Standards**

  – alternatively, by **Notified Body**
- **CSA** Cyber Security Act / EUCC
  Relevant primarily for Common Criteria

Scope (of 1 Aug 2025)

- Radio Equipment Directive, Art 3.3. d, e , f
  - 3 main topics: Network, Privacy, Money transfer

- Wireless, connected products –
  - Connected to internet *(directly or indirectly)*
  - childcare, toys or wearables (Art. 3.3 e)
  - Few exemptions & partly exemptions
    (e.g. Medical device, IVD, smart meters … & Vehicles, aviation …)

- Using harmonized standard - self declaration *(Still need to document compliance!)*
- If no harmonized standard is used = Notified Body

The standard

EN 18031-1, -2, -3

- Published Aug 2024, including reference to listing in Official Journal (OJ)
- EU consultants – negative outcome and suggested significant remake
- Today: harmonized and listed in OJ – with restrictions!

Restrictions – what restrictions?

The restrictions:

- The "rationale" and "guidance" sections in the harmonized standard do not guarantee compliance to the directive
- When using password, the option not to set password is not accepted
- Parental or guardian control is to be implemented on relevant products for EN 18031-2
- Notified Body is for all practical purposes required for EN 18031-3

Self declare or Notified Body? Yes, please …

- Self assessment may be used when documenting compliance to the relevant EN 18031 standard(s)
- A Notified Body is required if any of the restrictions are used
- Our experience
  - Nemko receives a lot of questions on the scope of RED and application of the EN 18031
  - Uncertainty about how to interpret the new standard brings many to use a notified body.
  - Notified Body certificate is the preferred way for many to demonstrate compliance

A cybersecurity evaluation process

- Not like testing for Safety, EMC, Radio …

- High involvement of the manufacturer

2 steps described by EN 18031

  - Conceptional evaluation *(Document compliance)*
  - Functional testing *(Verifying compliance)*

Nemko process

- Nemko will present EN 18031 guidance template
- Manufacturer to populate and Nemko to verify / Corrections
- Nemko to verify by testing / source code review
- Test report issued, and any certificates if requested, e.g. RED NB certificate

Evaluation Categories

- Overview of evaluation categories, also called mechanisms
- Much overlap, but there are differences in both number of requirement and the content.
- In total 14 mechanisms

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	✓	✓	✓

Assets and mechanism – what are they?

Assets

- Assets is introduced as the main target against which to apply the requirements.
- Different standard, different type of assets

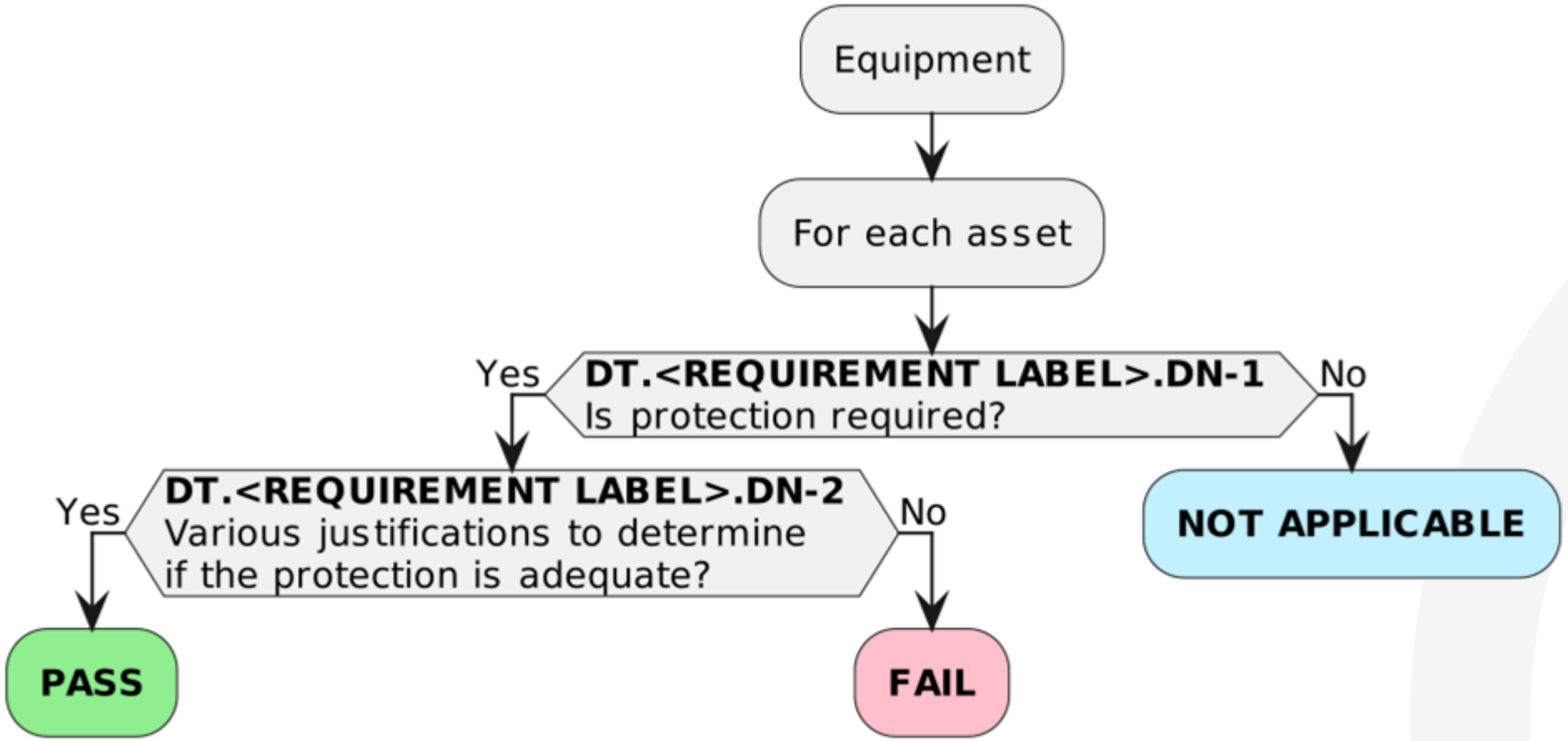
Essential requirement	3.3.d	3.3.e	3.3.f
Security asset	✓	✓	✓
Network asset	✓		
Privacy asset		✓	
Financial asset			✓

Mechanism

- Step 1: Applicable?
- Step 2: Appropriate enough?

[ACM] Access control mechanism
[AUM] Authentication mechanism
[SUM] Secure update mechanism
[SSM] Secure storage mechanism
[SCM] Secure communication mechanism

Decision tree



Documenting security

- Summary of documenting security .. So far:
  - Identify and describe the asset (what is being protected)
  - Identify and describe the mechanism (how is the asset protected)

Testing(?)

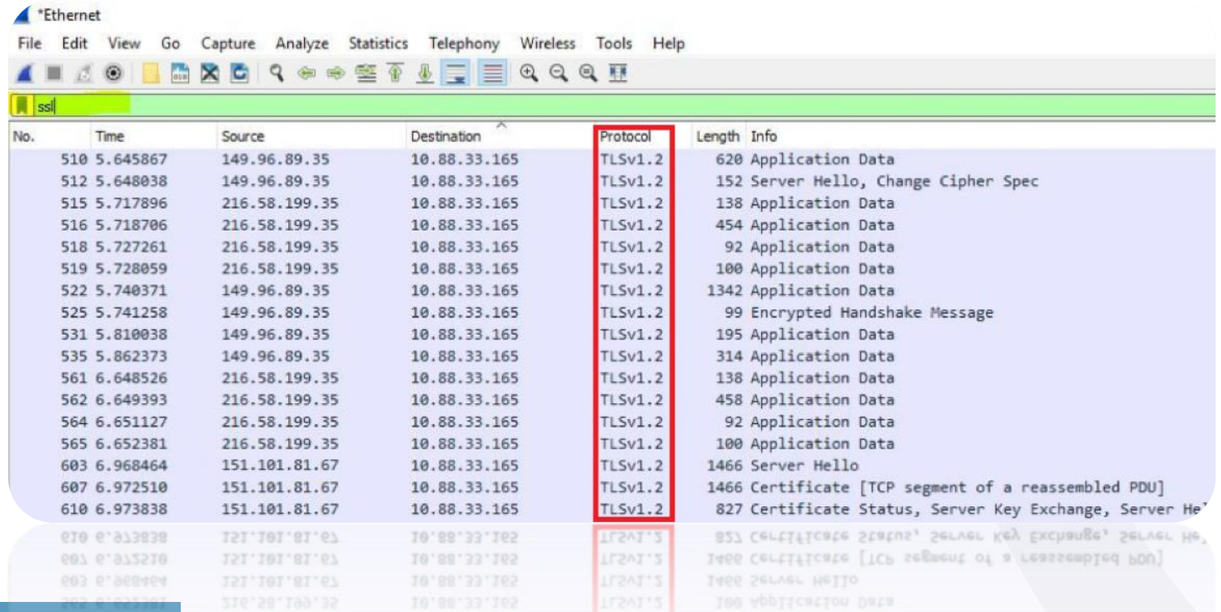
→

SCM-1: Secure communication

- **Requirement:** The equipment shall always use secure communication mechanisms for communicating security assets and network assets with other entities via network interfaces.
- *Note: There are exceptions to this requirement if:*

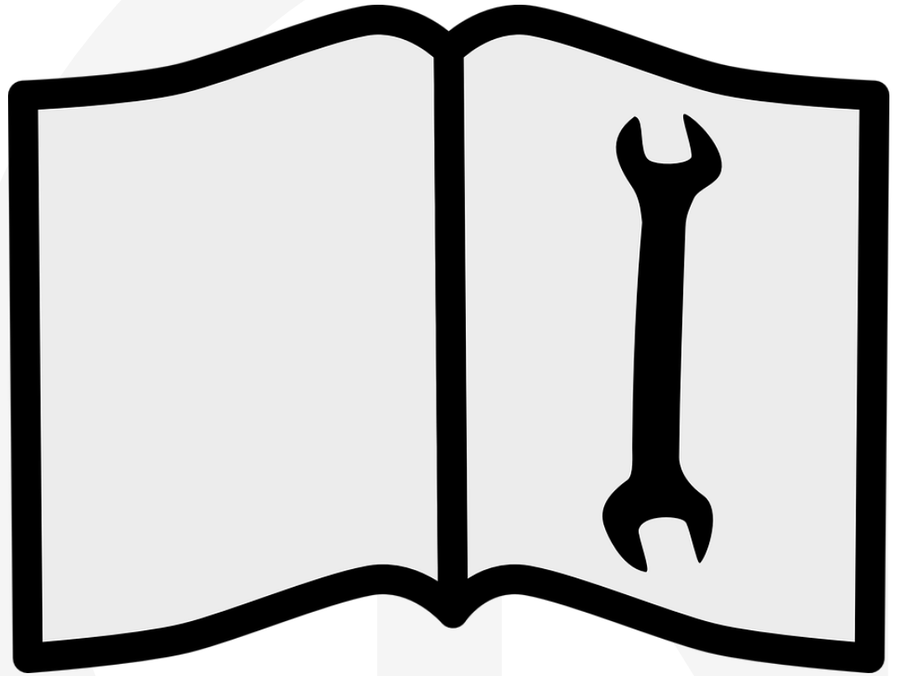
1. *Assets communicated are protected by physical or local measures in the targeted environment or;*
2. *Where exposure of the asset is part of establishing or managing a connection*

- When assets are communicated, they must be protected with a mechanism that protects the asset's integrity and confidentiality. This can be done with cryptographic protocols such as Transport Layer Security (TLS).
- Testing whether the equipment protects assets during communication can be done with tools such as Wireshark.
- Wireshark is a network analysis tool that can identify network traffic and communication protocols used by analyzing data packets.



Document security … part 2

- Summary of documenting security :
  - Identify and describe the asset (what is being protected)
  - Identify and describe the mechanism (how is the asset protected)
  - Testing
    - Functional tests results
- … and that’s how to document the security of a product



Updates

- Confirmation of RED cyber from 1 Aug 2025

- Scope
  - Directly / indirectly connected to internet (this is the only definition)
    - No technology or protocols are exempted or included by default
    - Includes wireless products with wired internet connection
    - Risk analysis to identify scope relevance case-by-case
    - For deciding scope, protective measure is not an argument
    - Nemko frequently makes scope assessments as a service

The (whole) timeline

Decide	Test & Document	Redesign product	Manufacture	Ship	Put on market
Feb ‘25					Aug ‘25.

CRA - Cyber Resilience Act

Mandatory from 11 December 2027 (reporting from 11 Sept ‘26)

Typical CE marking regulation

- Describes essential requirements – referring to harmonized standards
- Prescribes the use of CE marking
- Requires Declaration of Conformity and Technical File
- Describes obligations of Economical Operators like Manuf., Aut.repr., Imp., Dist.
- Rebranding or modifying product = becoming manufacturer
- Market surveillance

CRA - Cyber Resilience Act *(some differences)*

- Wide scope, also software
  excludes MDR, IVD, vehicles, aviation, marine, defense, ..
- Software bill of materials
- Requirement of keeping the product updated after putting on market
  i.e. updates to close vulnerabilities (5 years)
- Security updates available for min. 10 years
- Only latest update need to comply (conditions)
- Reporting of active exploits of vulnerabilities
- Heavy fines for breaches (up to 15M EUR / 2.5% of rev)
- Self declaration, but NB required for some products (e.g. critical industrial equipment)
- CRA may cover cybersecurity requirements of high-risk AI
- Certification to RED / EUCC cybersecurity may demonstrate compliance to CRA (Art 27 / 8)

How to address cybersecurity requirements

- Include cyber security from design phase (Most compliance work is done here!)
- Standardize cyber security solutions for multiple products (modules?)
- Use international standards to document security (e.g. EN 18031 for Europe)
- Prepare well in advance for coming regulatory requirements, such as CE marking
- Minimum first step: Do a GAP analysis, workshops guidance if necessary
- Mitigate uncertainty of the harmonized standard by using a RED Notified Body (with cyber in scope)

Getting late to be early!

ISO/IEC 27400

ISO/IEC 27402

ISO/IEC 27403

ISO/IEC 27404

Q & A