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**

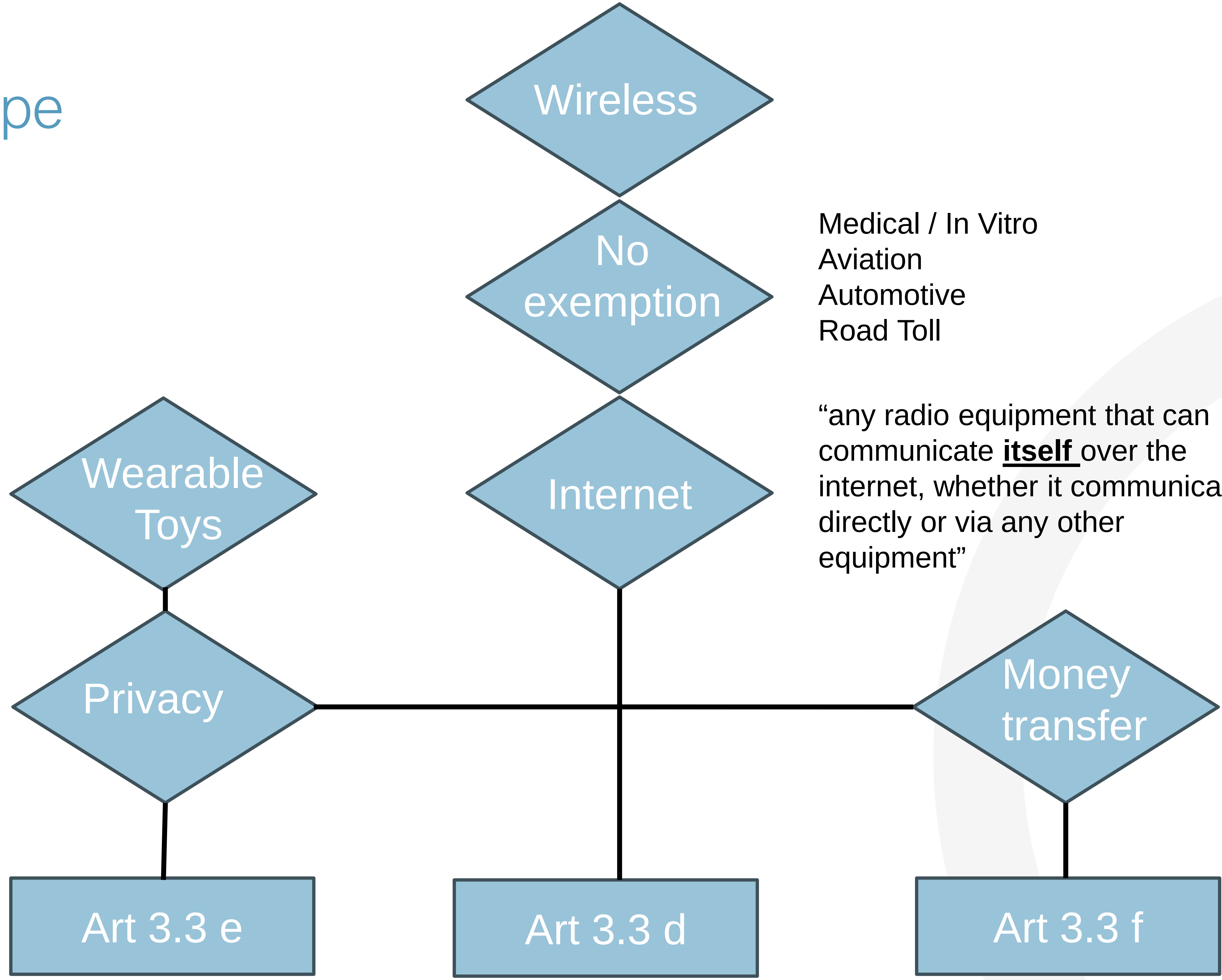
- **CSA** Cyber Security Act / EUCC Relevant primarily for Common Criteria (not covered in this presentation)

Scope

- Radio Equipment Directive, Delegated Act
  - Art 3.3. d) Network protection
  - Art 3.3. e) Privacy
  - Art 3.3. f) Money transfer

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

Scope



Medical / In Vitro
Aviation
Automotive
Road Toll

“any radio equipment that can communicate **itself** over the internet, whether it communicates directly or via any other equipment”

How to comply

The standard

- EN 18031-series (published Aug. 2024; harmonized 30 Jan. 2025, with some restrictions)

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 3rd party
- Notified Body certificate is the preferred way for many to demonstrate compliance

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?

- Self assessment may be used when documenting compliance to the relevant harmonized EN 18031 standard(s)

- A Notified Body is required if any of the restrictions are used, or using non-harmonized standard(s)

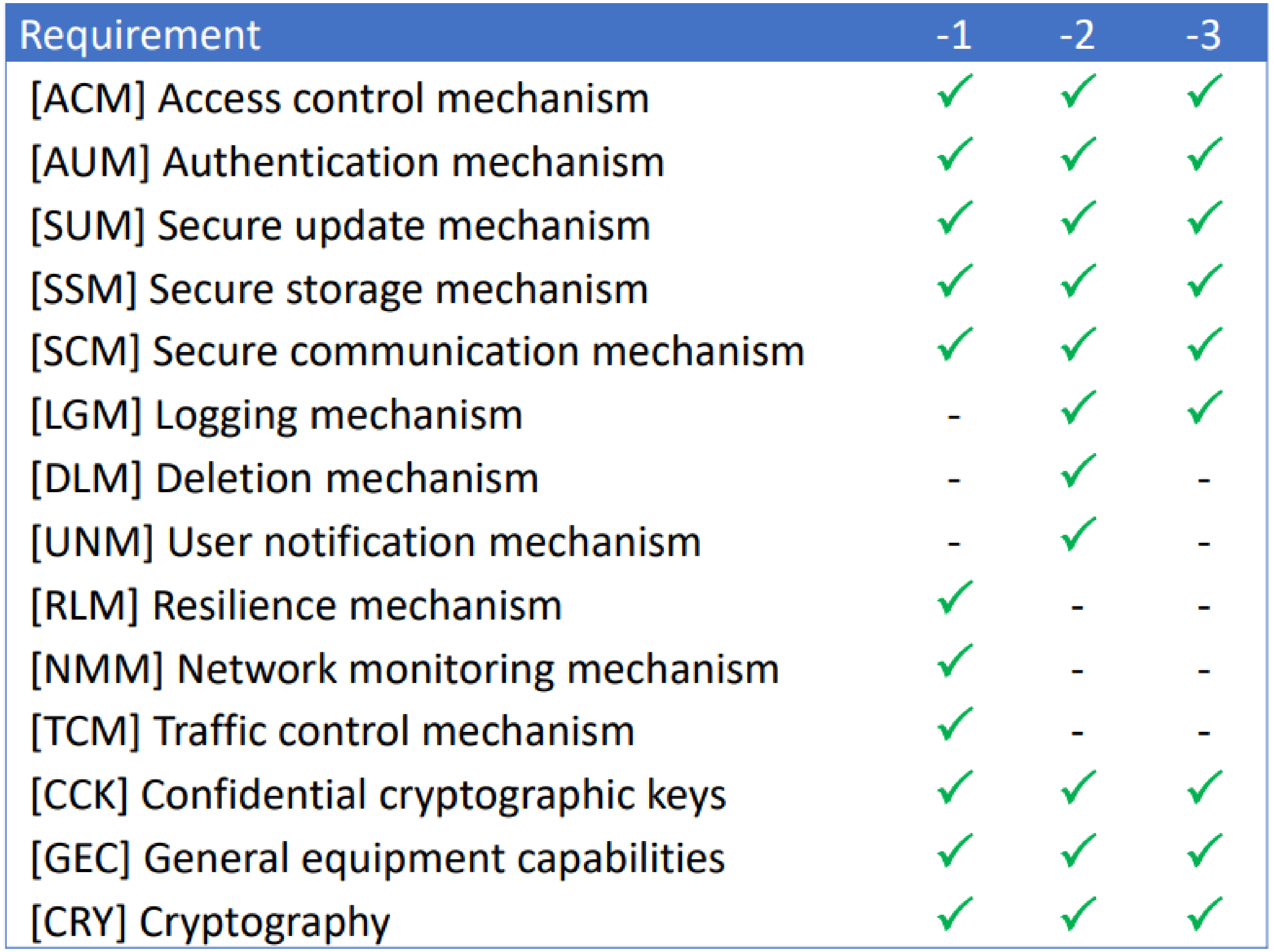
- Notified body certificate may also be issued covering Cybersecurity only (but not covering the restrictions only)

EN 18031 - the content

- An EN 18031 evaluation is about **protecting Asset's** and using **secure Mechanism** according to the different requirements.

- **Assets**
  What is to be protected?
  (Password, keys, user data, confidential info, …)
  - Network Asset
  - Security assets
  - Privacy Asset
  - Financial Asset

- **Mechanisms**
  How are assets protected?
  (Encryption, authentication, secure boot and recovery, …)



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	✓	✓	✓

A cybersecurity evaluation process

- Not like testing for Safety, EMC, Radio …
- High involvement with the manufacturer

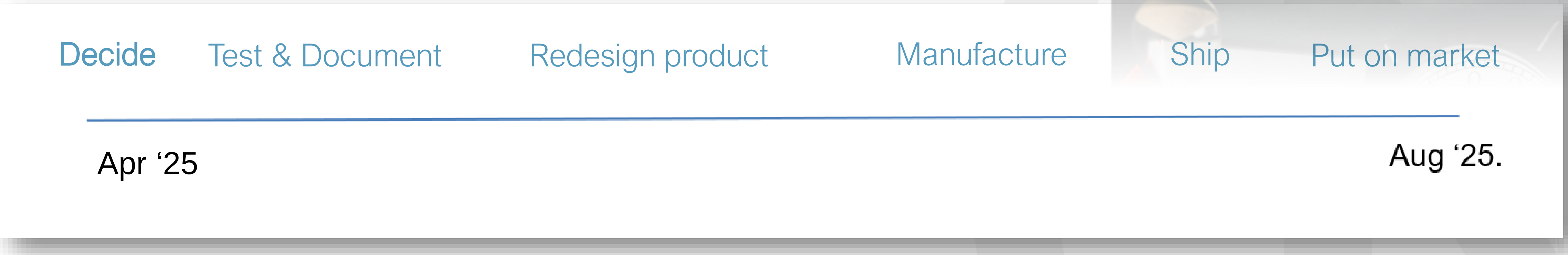
2 steps described by EN 18031

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

Nemko process

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

The (whole) timeline



Decide Test & Document Redesign product Manufacture Ship Put on market

Apr ‘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)

CRA Products Categories

The majority of products

Products with digital elements - Self assessment (Harmonized standard advisable)

Important products, Class I - Self assessment if use of Harmonized standard otherwise NB

- Browsers and OS
- Routers, modems
- Smart locks, cameras
- Wearbles for health or children

Important products, Class II - Notified body

- Firewalls
- Intrusion detection / prevention systems
- Tamper-resistant µ-processors/controllers

Critical product - Notified body

- Smart meter gateways
- Smart Cards

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!

Stay secure!

Book a free video meeting