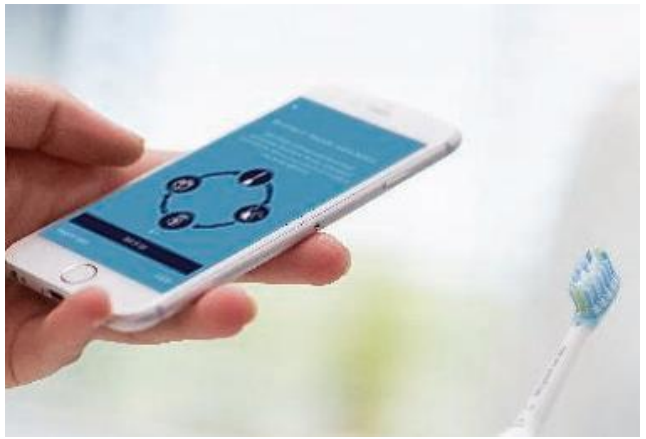
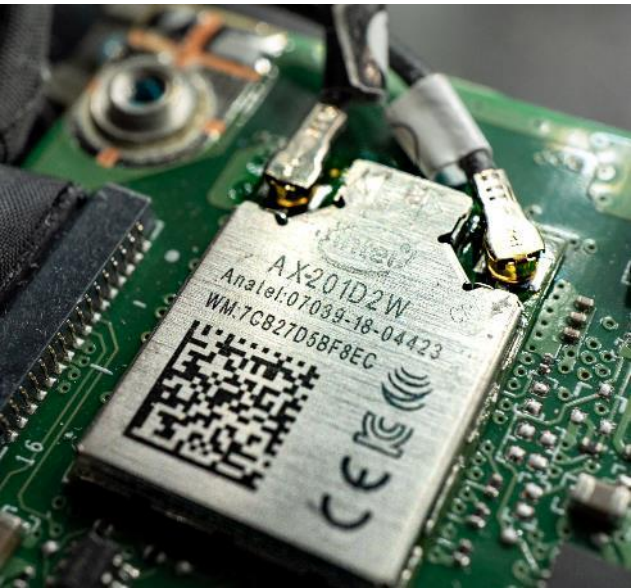
RED Delegated Act (2022/30) Standardization Request (M585) Working Draft Introduction

CEN/CENELEC JTC 13/WG 8

2023-02-07

7th ENISA-ESOs Cybersecurity Standardisation Conference 2023





RED Delegated Regulation (2022/30) activates RED requirements 3.3.d/e/f

- 3.3.d “radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service”
- 3.3.e “radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected”
- 3.3.f “radio equipment supports certain features ensuring protection from fraud”

The delegated regulation which was published on the 12th of January 2022, states in recital (1):

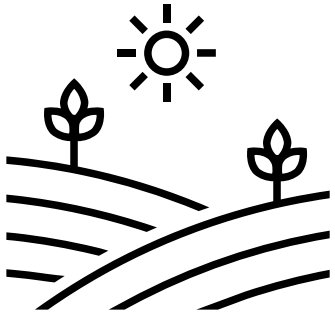
“Protection of the network or its functioning from harm, protection of personal data and privacy of the user and of the subscriber and protection from fraud are elements that support protection against cybersecurity risks”.

CEN/CENELEC JTC 13/WG 8 “Special Working Group RED Standardization Request”

- JTC 13/WG8 was established on July 7, 2022, to address the RED Standardization Request.
- JTC 13/WG8 is on a very tough meeting schedule with many online and hybrid meetings.
- WG8 currently has 167 committee members representing:
  - 18 National bodies
  - CENELEC TC’s
  - Liaisons:
    - ANEC
    - APPLIA
    - ESMIG
    - ETSI
    - EURALARM
    - EUROSMART
- Convenor: Ben Kokx
- Secretariat: NEN

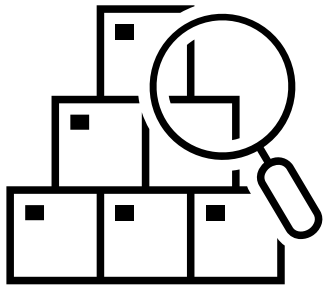
RED Delegated Regulation hENs			
Stage Code	**Stage**	**Target date**	**Duration**
10.99	Decision on WI Proposal	2022-10-14	
			+ 16 weeks
20.60	Circulation of 1st WD	2023-02-03	
			+ 8 weeks
30.99	Acceptance of ENQ draft	2023-03-31	
			+ 3 weeks
40.20	Submission to Enquiry	2023-04-21	
			+ 12 weeks
40.60	Closure of Enquiry	2023-07-14	
			+ 8 weeks
45.99	Acceptance of FV draft	2023-09-08	
			+ 3 weeks
50.20	Submission to Formal Vote	2023-09-29	
			+ 8 weeks
50.60	Closure of Formal Vote	2023-11-24	
			+ 2 weeks
60.55	DOR/Ratification	2023-12-08	
			+ 2 weeks
60.60	DAV/Definitive text available	2023-12-22	

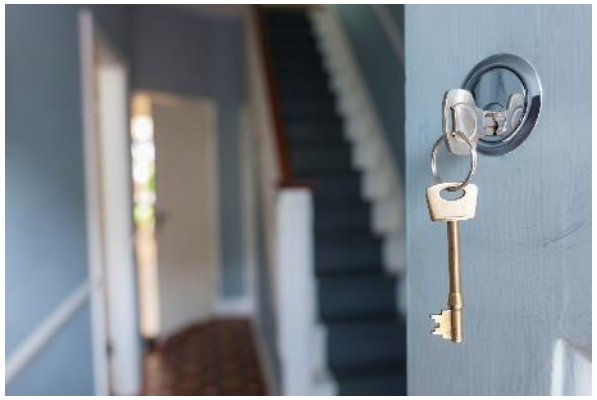
This horizontal scope includes a huge variety of equipment for vary different use environments…



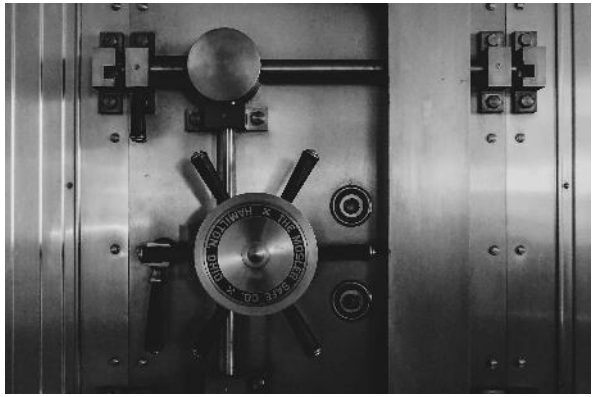
- Computers, cell phones, tablets, Single Board Computers, etc.
- Motor vehicles
- Civil aviation
- Road toll systems
- Childcare equipment
- Payment terminals (+ ATMs)
- Industrial equipment
- Agricultural equipment
- City automation
- Public transportation tracking systems
- Telecom infrastructure equipment
- Wireless networking equipment
  - Public infrastructure
  - Enterprise networks
  - Home routers
- Consumer IoT
  - Audio/video equipment
  - Home appliances
  - Home automation
  - Fitness equipment
  - Wearables
- Toys
- Any software product bundled with a (mini-)PC or other hardware (e.g., android tablet or Raspberry-Pi)!
- **And everything else using radio…** *except medical devices*

Requirement to “Protect the valuables in your house” has many appropriate solutions

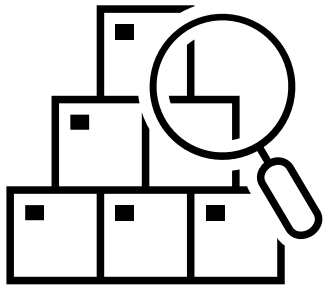




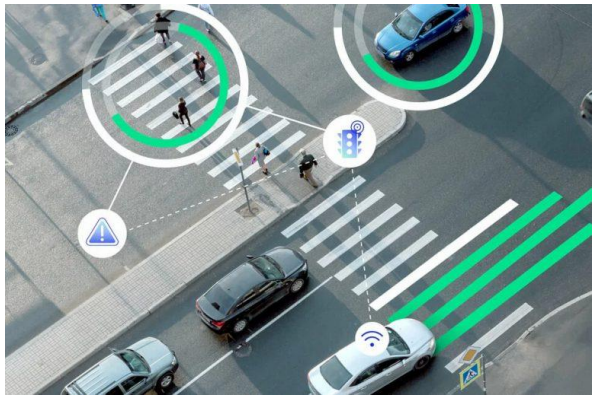
and combinations of…



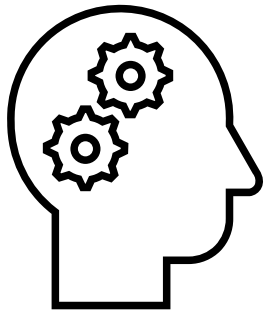
Also, the security protection levels that should be achieved are different across the various sectors



What is appropriate? (cost/benefit)



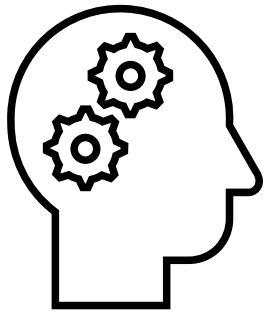
The main challenge – Horizontal approach



The main challenge to develop these standards is that the RED is a **horizontal legislation**.

As cybersecurity threats and risk landscape are continuously changing, we typically address security with **security-by-design** processes and a **defense in depth** approach for the **product** itself and the **operational environment** it is used in, but under the RED we are constrained to **requirements for the product**.

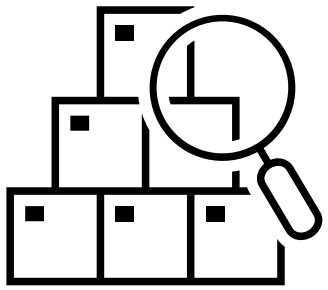
The main challenge – Horizontal approach



To recognize the specific needs and possible constraints, the security requirements must address **applicability and appropriateness** of the security control requirements which are **dependent** on the equipment's:

- *reasonably foreseeable and intended use;*
- *intended operational environment of use and;*
- *the risk to <d>: privileged data and network resources*
  <e>: personal, traffic and location data
  <f>: related to the transfer of (virtual) money

The main challenge – Horizontal approach



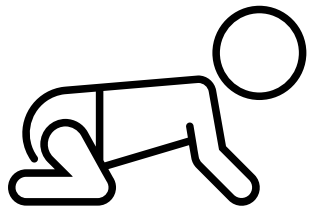
The workgroup is introducing so called '**mechanisms**' which are **specific security functionalities** that the equipment must address

Whether or not these mechanisms are both applicable and appropriately implemented needs to be assessed by documenting, analysing and risk assessing the implementation of each requirement with pass/fail criteria.

4.1.1.1 The equipment shall use appropriate access control mechanisms to manage entities access to privileged functions, privileged data and network resources, unless

- ***the "equipment's reasonably foreseeable and intended use" does not require access control for privileged functions, privileged data or network resources; or***
- ***the "intended operational environment of use" provides sufficient access control.***

What's next?



The working draft is out for a 3-week review period to get stakeholder input on the selected approach and understand if this approach can lead to an acceptable harmonized standard that will be cited in the OJEU:

- As a horizontal standard it provides more flexibility to the manufacturers than what some stakeholders would like to see
- This flexibility could be misused by **bad apples**, but **standards can't stop this**, only the **Market Surveillance Authorities** can
- Not citing the standards in the OJEU and the huge number of products in scope of the RED delegated regulation will have an impact on the ability to place products on the market

Thank you,

Ben Kokx,
Convenor CEN-CENELEC JTC13/WG8

ben.kokx@philips.com