The relation between the Radio Equipment Directive and cybersecurity legislation

Presented by: **Neviana Nikoloski – Phonak, ETSI GA Chair**

For: **ENISA Cybersecurity Standardization Conference, panel 1: Radio Equipment Directive – implementing measures**

02.02.2021

On the role of the RED for cybersecurity

- Key question for standardizers is the role of RED articles 3(3)(d/e/f) in view of other legislative instrument
  - RED is scoped to the radio equipment
  - RED is ex-ante
  - Harmonised Standards under the NLF now require “legal certainty”
- ETSI presentation on panel 2 will show the limitations through the lens of security testing
  - Legal certainty under the RED is mainly limited to functional testing, which itself limits what can be achieved for security through the RED
  - RED cannot fully address security due to lack of lifecycle coverage and contextual knowledge on deployment for risk assessment

On the role of the RED

- Anticipation is key: what could the legislative landscape look like in the next 5+ years?

- Interrelations between legislative instruments require careful considerations to avoid (or handle) overlaps, avoid or resolve potential contradictions (contradicting requirements), and avoid duplication of testing and conformity assessment efforts
  - Including at the level of standards

Answers to these questions will drive standardisers' work

- What is achievable under each legislative instrument and how will this be coordinated?
  - how to ensure that manufacturers can navigate the legislative and standards corpus?
- Can the number of HEN be kept to a minimum?
  - clear-cut risk criteria (risk classes) could be sought on security, data protection, privacy protection in order to design generic HEN that would address the risk classes
    - For specific intended uses, a dedicated HEN could be envisioned
  - uncertain path, no appropriate risk classes identified so far
  - ideally, a Delegated Act should scope device categories such that the number of HEN is limited while proportionality is preserved
- Which kind of fraud may be considered under the RED?
- What role will RED 3(3)(d/e/f) and the related HENs play in this future landscape?
  - composition (see next slide)

Options for composition

Option	Remarks
A certificate given to a radio equipment under the CSA grants conformity to RED 3(3)(d/e/f) 🔴	• Security testing is out of the RED, conformity assessment amounts to verifying compliance of security properties provided by the certificate report against requirements of HEN • Is this acceptable from RED point of view? • Very significant testing effort is introduced to pass RED compliance • The Notified Body must have both RED and security expertise • Interactions with RED Article 4 may also increase testing effort • This solution requires alignment of RED classes with relevant CSA schemes (e.g. sectorial), which may lead to substantial fragmentation of RED classes, plus aligned timelines
Compliance of a component to a scheme under the CSA can be used to prove security properties of a radio equipment under RED 3(3)(d/e/f) Rest is functional testing under the RED 🟡	• The certificate can prove part of the security properties of the radio equipment under the RED, including their strength – similar to the handling of safety requirements • Other security properties of the radio equipment are evaluated on a functional level • Can scale for key components in the supply chain, such as secure elements • Risk that HEN require manufacturers to have certified components, for which no certification scheme exists – manufacturers must then embark on uncharted certification • Risk that the certificate is not valid for the usage context of the radio equipment • This solution would constrain the implementation of Radio Equipments to pre-established solutions, thus hindering innovation and introducing bias in the supply market
Conformity under RED 3(3)(d/e/f) grants compliance of a radio equipment under the CSA, the GDPR, or other legislative instrument 🔴	• The RED focuses on functional testing and the certification scheme accepts the result as-is • Can work as long as the legislative instrument accepts functional testing only, and no assessment of security assurance – thus CSA seems out of scope
Conformity under RED 3(3)(d/e/f) is reusable to prove compliance to a certification scheme under the CSA 🟢	• The RED can focus on functional testing of a limited set of security requirements and the certification scheme can address all other security requirements and security assurance • RED article 4 can be coordinated with certificate renewal rules • This solution requires alignment of RED classes with relevant CSA schemes (e.g. sectorial), which may lead to substantial fragmentation in RED requirements across classes

Legend: 🟢 feasible 🟡 feasible with care 🔴 strong reservations

Thank you!