UK SPF and techUK: RE-D, Changes Are Coming
RED Overview, Impacts, Standardisation & Certification

Alex Leadbeater CEng MIET, BT SECURITY
Head of Global Obligations Futures & Standards
(Chair of ETSI TC CYBER)
27th Oct 2021

Agenda

ETSI & ESOs

Raising the Bar - EU Cyber Security Standardisation Landscape

RED Overview and Standardisation

Risk Assessments, Testability, and Legal Certainty

Not just RED to worry about

What is ETSI?

- ETSI is a world-leading standards developing organization for Information and Communication Technologies (ICT).

- Founded initially to serve European needs, ETSI has become highly-respected as a Global producer of technical standards for worldwide use
  - E.g GSM and Partner in 3GPP responsible for 5G

- TC CYBER is ETSI's Centre of Excellence and focal point for Cyber Security.
  - TC CYBER works on a range problems – from Privacy, to IoT, to protecting personal data and Quantum Cryptography.

  - Works on both industry security challenges and EU security mandates to address global cyber security problems.

  - ETSI member Industry, Academia and Government representation.

- ETSI is one of three European Standardisation Organisations (ESO) that can be tasked by European Commission (EC) to develop standards in response to EU legislation.
  - ETSI, CEN, CENELEC

Cybersecurity work in ETSI/3GPP/OneM2M

CROSS-DOMAIN CYBERSECURITY

- Ecosystem
- Protection of personal data & coms
- IoT security and privacy
- Critical infrastructures
- Enterprise and individual cybersecurity
- Forensics
- Information Security Indicators
- Encrypted Traffic Integration

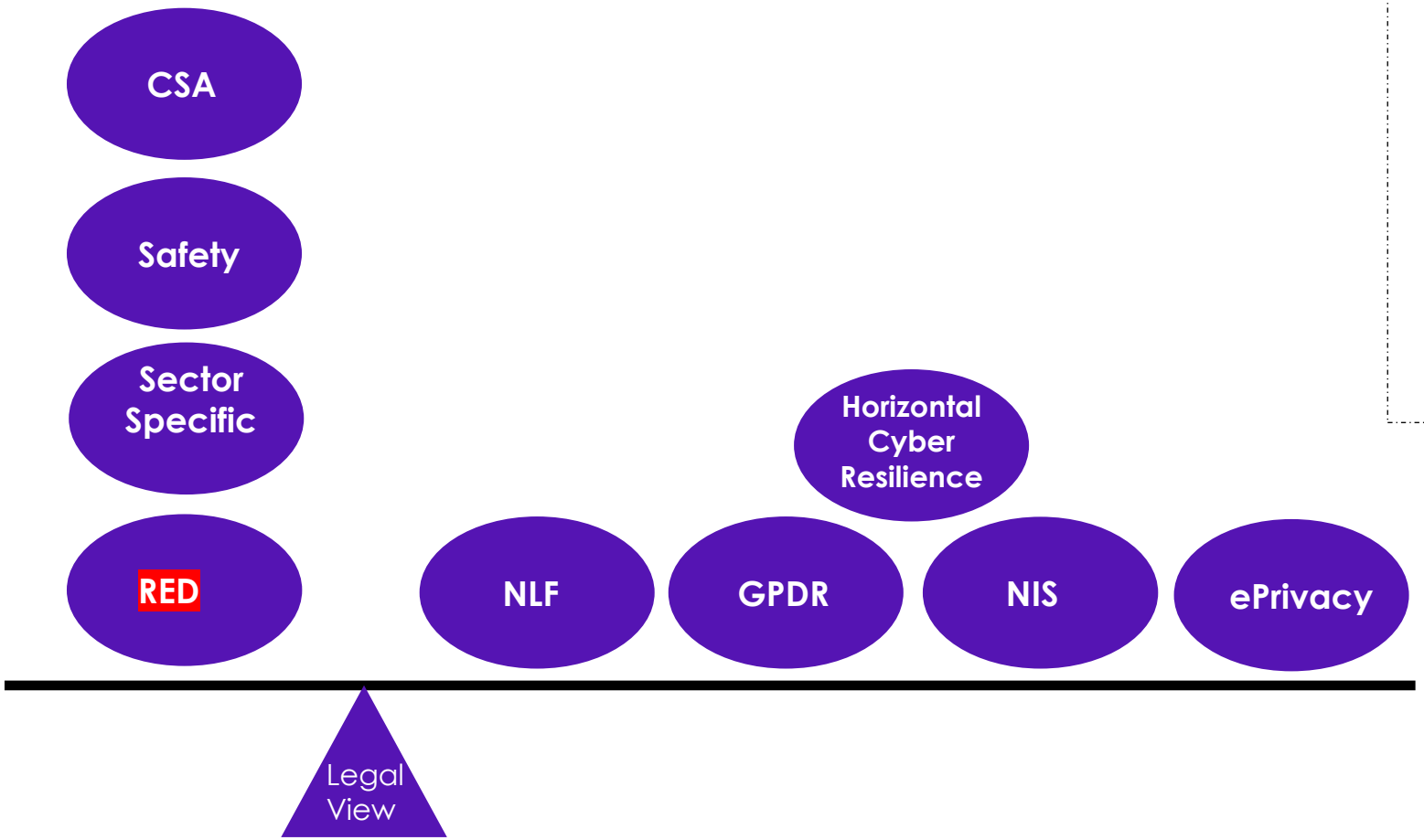
SECURING TECHNOLOGIES & SYSTEMS

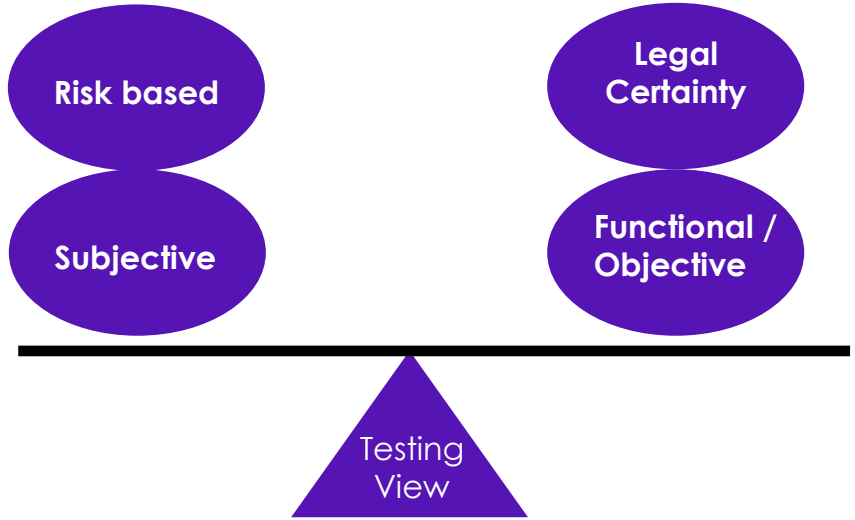
- Mobile / wireless systems (5G, TETRA, DECT, RRS,RFID...)
- IoT
- Network functions virtualization
- Intelligent Transports
- Broadcasting
- Artificial Intelligence
- Privacy-preserving pandemic protection

SECURITY TOOLS & TECHNIQUES

- Lawful interception & retained data
- Digital signatures & trust services
- Permissioned distributed ledgers
- Smart cards / secure elements
- Security algorithms
- Quantum key distribution
- Quantum safe cryptography

EU Legislation & Certification Landscape





RED Cyber Security Requirements – Articles (3)(3), d,e,f

DIRECTIVE 2014/53/EU -on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC

(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;

Requirements apply to Radio Equipment being placed on the market.

Requirements may apply where both "intended use" of radio equipment allows connection to the internet and where the functionality allows it to be connected in such a way (either indirectly or directly).

- Applies to all equipment containing radio capabilities.
- Limited exemptions – e.g. medical devices.

It is not the ESO(s) role to assess whether a product is in scope of RED. This is an EC and market surveillance authority role.

RED Cyber Security Requirements – (3)(3) DEF – Delegated Act

Sets out scope, requirements and activation timescales for compliance with RED articles (3)(3) D,E,F.

Undergoing final approval stages – No further changes expected.

30 month compliance timescale –likely starting ~1st Jan 2022.

Compliance via use of ECJ cited EU Harmonised Standards (HENs) or via direct evaluation by a notified body.

HEN development window between Jan 2022 and between July 22 – Jan 23.

- Exact window will depend on degree of parallel or serial steps in approval processes after drafting.

Manufacturers will get ~9-10 months implementation period post HEN citing in ECJ.

- No guarantee EU will accept standards.

Covers;

- Radio devices
- Toy devices (including childcare devices – excluding medical).
- Wearable devices

Additional areas;

- 5G Equipment (currently under (e) only)
- Smart Meters
- Smartphone implementation of e-IDAS 2.0 – e-wallet.

ESO approach to RED Article (3)(3)DEF HENs

Risk Assessment based.

- Risk associated with intended use.
- TR being developed to capture methodology.

Focus on capabilities that a device can support under RED.

- Security primitives but not their usage as part of a service deployment.
- E.g. Ability to turn on or off a functionality.
  - E.g. Camera or Location reporting.
  - However, API use of the functionality as part of a service is out of scope.

Common approach across all product categories within scope of DA.

- Likely heavy re-use of requirements extracted from EN 303 645.

Primary aim: Improve baseline security for all products.

Prioritisation and Proportionality

Avoid being too prescriptive and limiting security / product innovation.

Proposed ESO list of HENs to address article (3) (3) DEF Delegated Act

Baseline List:-

1. Common Security Requirements for internet connected radio equipment, addressing 3(3)(d)
2. Common Security Requirements for radio equipment processing data, addressing 3(3)(e) (it will cover internet connected radio equipment, childcare radio equipment, toys radio equipment and wearable radio equipment).
3. Common Security Requirements for internet connected radio equipment processing virtual money/monetary value, addressing 3(3)(f)

Possible Extended List:- (Under discussion, not agreed and with open issues).

1. 5G Equipment
   - Limited to (3)(3)e, only.
2. Smart Meters
   - CSA High level equivalent aligned to highest member state requirements.
3. Smartphone eIDAS 2.0 e-wallet
   - Only e-IDAS 1.0 is active in EU law.

Standardisation open issues include:-

Delegated Act is now frozen with no changes accepted.

- 30 month industry compliance timescale very challenging.

Security by Design definition not contained in DA or SR.

Have “informal agreement” with EC that this is CSA recitals 12 & 13.

State of the Art definition not contained in DA or SR.

Have “informal agreement” with EC that this is “established industry practice not bleeding edge”.

DA requires logging of security events.

No clear responsibility for manufacturer or GDPR impacts.

eIDAS 2.0 is not enacted in EU law.

No issue in principle with eIDAS 2.0 in future.

Accessibility device exemption not explicitly included.

Needs to be similar to medical exemptions.

No clear definition of scope of “5G” in DA

Existing industry NESAS scheme and EU CSA (in future) more than cover this already.

Smart Meters

No single common smart meter architecture in EU and member state EALs vary.

EN 303 645

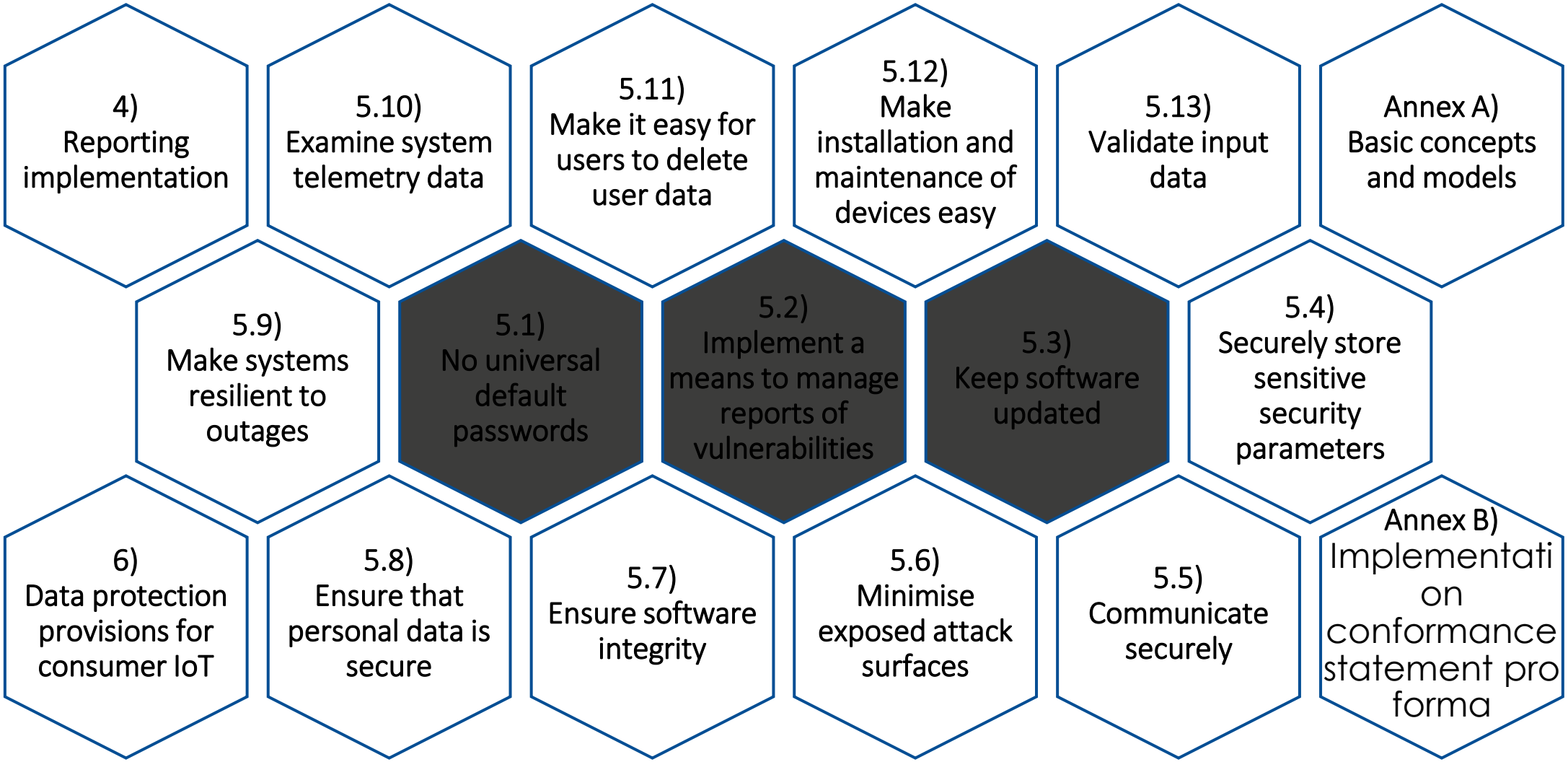
- EN 303 645: "Cyber Security for Consumer Internet of Things: Baseline Requirements"
  - Brings together technical and organizational measures that are widely considered good practice.

- Purpose:
  - Support all parties, especially manufacturers, in the development of consumer IoT
  - Establish a common baseline across the European and wider global market
  - Contribute to future certification schemes under the EU Cybersecurity Act

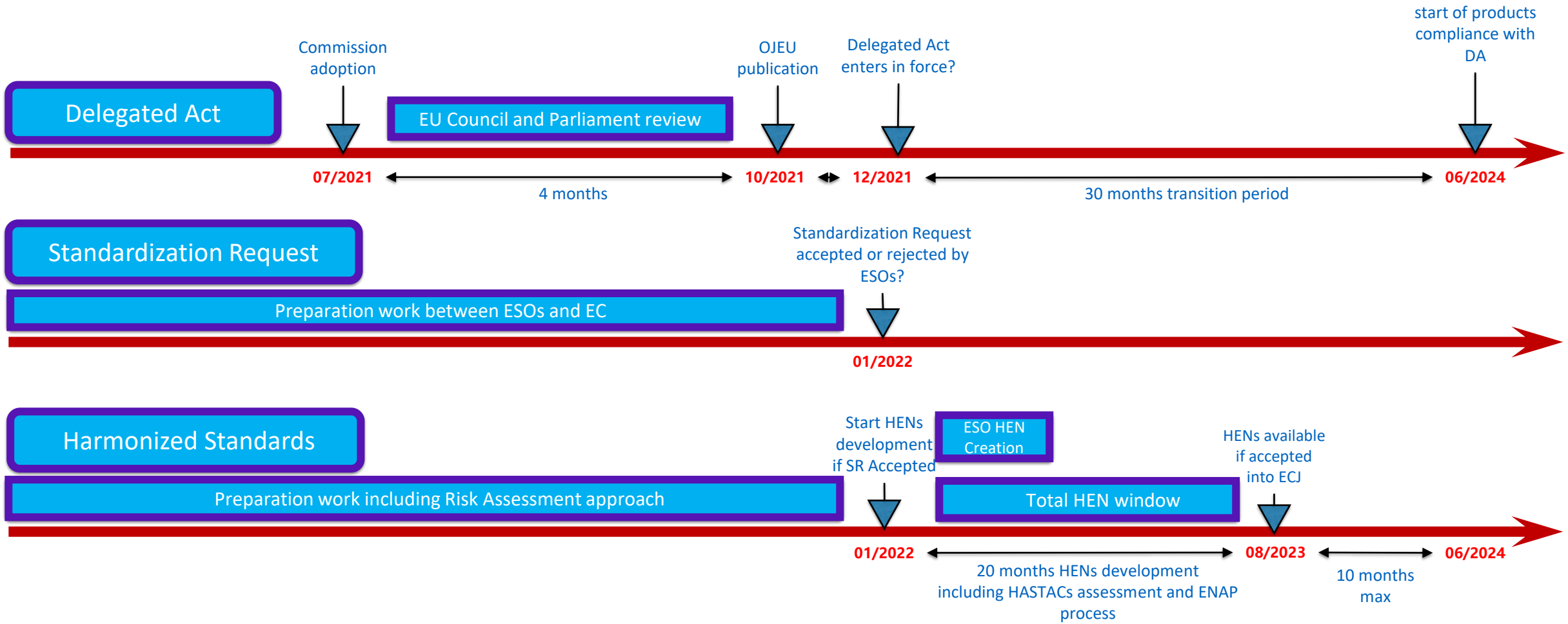
➢ To better protect consumers and other users of connected "smart" products.

➢ **Not specifically developed, proposed or formulated for RED but serves as an example of the sort of requirements that will be contained in the three generic d,e,f RED HEN(s).**

EN 303 645: Content



Estimated RED 3.3(d,e,f) roadmap



Get involved?

ETSI running a pan ETSI #SR group to handle discussion of RED article 3.3 d,e,f

- Convened by ETSI TC CYBER leadership
- https://portal.etsi.org/tb.aspx?tbid=824&SubTB=824,856#/
- CEN CENELEC members also welcome as part of ESO co-ordination in Cyber Security.
- Dedicated #SR email list
- Will be response for final ETSI board recommendations on whether to accept or reject SR.

Negotiations with EC on final issues nearly complete.

- Very limited scope to bring new issues after mid November.

ESO(s) undertaking parallel activities for CSA and AI Act.

Not just RED

EU Cyber Security Act (CSA) significantly overlaps with RED.

- Currently limited alignment and significant risk of double certification.

Recently announced Horizontal EU Cyber Resilience Act

- Significant scope for triple certification.

UK still looking to mandate provisions of EN 303 645 into UK law.

- ETSI expect to reuse EN 303 645 for RED so unlikely to be significant divergence.

EU draft Eco Design Regulation

- Currently includes provisions to mandate user ability to role back to earlier software versions
  - No specific security patch exemption.
  - Manufacturers will need to support multiple code branches.
  - Applies from firmware upwards through to OS & Applications.