Panel 6: Vision of the Future

Rolling Plan Security Certification

Chair of ETSI TC CYBER & ISG Secure AI (SAI)
Alex Leadbeater CENG MIET, BT SECURITY
4th Feb 2021

Vision of the Future: Context of Security Regulation and Standards

What is the purpose of National, EU or Global Security Regulation?

- Protect National, European or Global Citizens from defined threat, which the regulation aims to mitigate?
    - We must not loose sight of the fundamental purpose of security regulation through certification.

What is the purpose of Security Standards?

- Define a common minimum baseline level to address defined Security Threats / Risks.
- Security bar <u>must be achievable</u>, while adding value (current product security vs “needed” security delta).

Security is a cost?

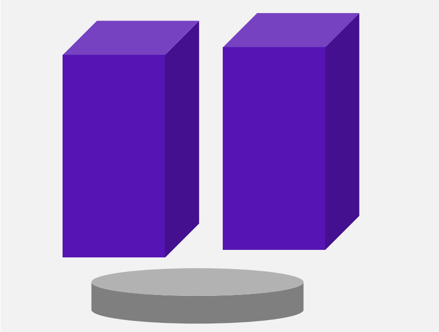
- Effective targeted Security Standards, Certification and Regulation reduce cost (e.g. financial or privacy).
- Security certification that does not mitigate intended threat / risk increases cost for little benefit.
- Multiple overlapping security mechanisms, requirements and certification obligations are inefficient.
    - End user, manufacturer or service provider rarely benefit.
    - Market agility and innovation reduced.

Overly prescriptive Regulation and Standards?

- Reduce end product market competition and security innovation?
- Barrier to market entry.
- Inflexible regulation and standards are vulnerable to market or security threat landscape change.

<u>Ultimately if the end service / product user does not receive the intended security or privacy benefit, then both regulation and security certification have failed.</u>

Vision of the Future: Rolling Plan Prioritisation



Many Square Pegs, One Round Hole?

Current Priorities: AI, Consumer IoT, Industrial Automated Control Systems – Right Priorities?

- Rolling plan spans a wide range of technologies.
- End user vs Critical National Infrastructure vs Industrial security importance.

Purpose of Certification: End Product vs Underlying Technology Certification.

- Rolling plan contains examples of "end user" products and general enabling technologies.
- Specific implementation security certification?
- **Substrate agnostic security certification**?
    - e.g. ETSI ISG SAI
- Horizontal vs Vertical certification – Need a consistent approach across the rolling plan.

Self certification vs notified body certification

- Layered testing or proportionate certification balancing specific technology or use case risks.

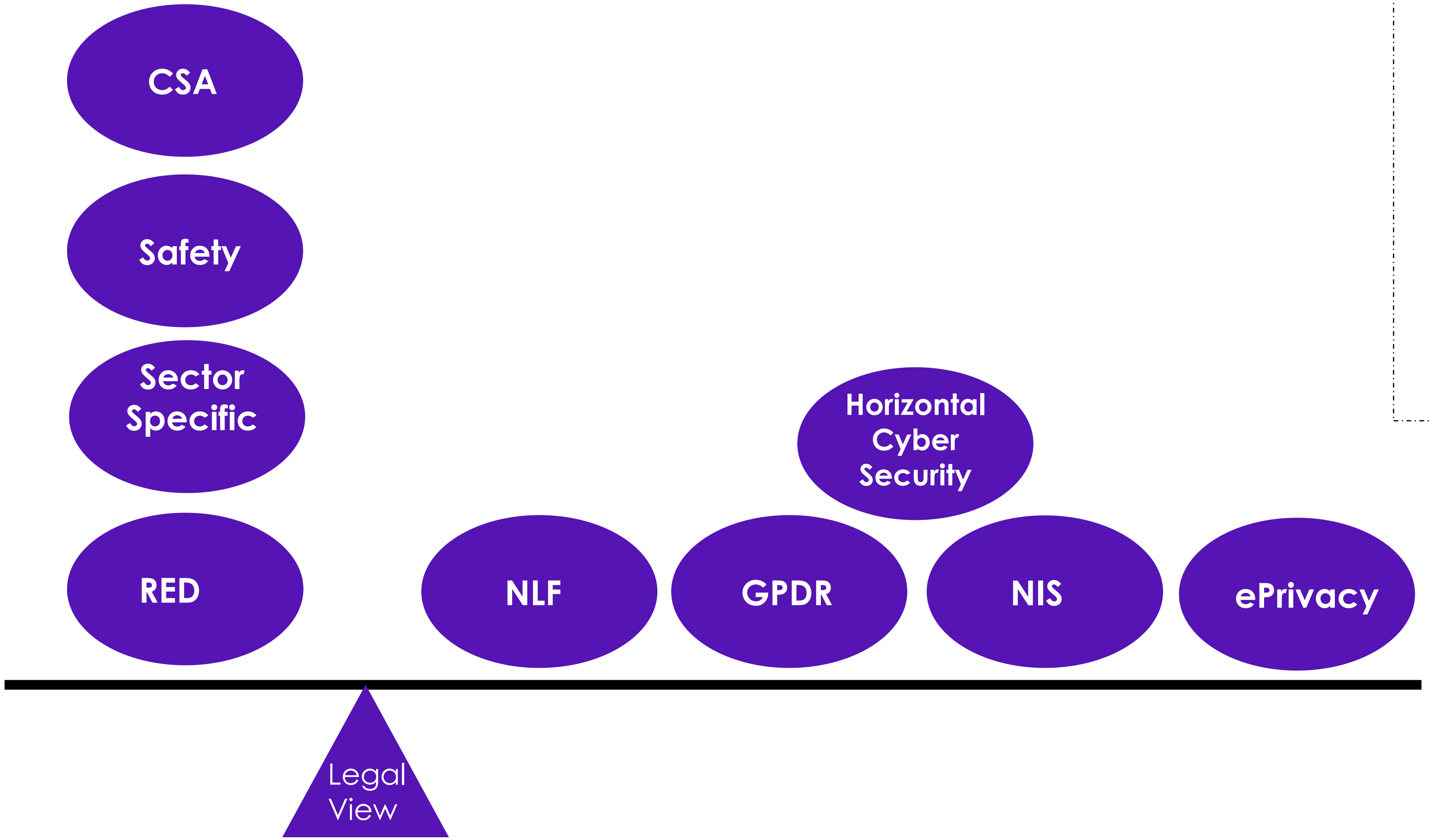
Agility and timeliness of Certification Standards

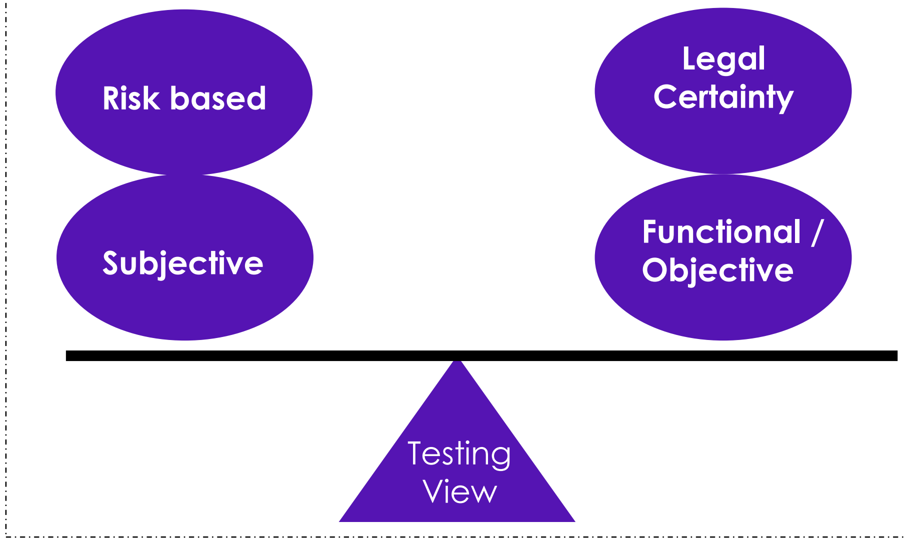
- Rolling Plan priorities may lag technology role out (e.g. 5G or AI).
- Eco-system and use cases evolve.
- Role of lightweight certification – Low cost or highly agile market use cases.

New vs Established Technologies

- Threat landscape and risk mitigation strategies may be different.
- When is the right time in a new technology development to certify?

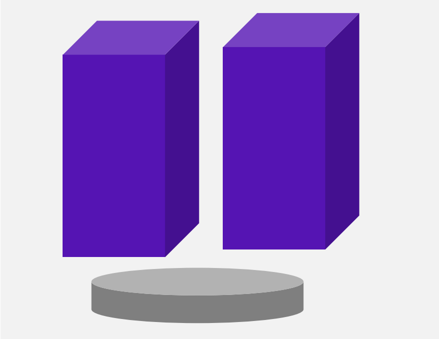
Vision of the Future: Certification Landscape





Rolling plan should avoid spawning further overlapping regulatory requirements and seek to minimise global market fragmentation except where absolutely necessary (e.g. to ensure European Privacy norms).

Vision of the Future: Role of Standards



More Square Pegs, More Round Holes?

New standardisation requests: The answer is not always more standards.

Can existing standards form the framework for future certification areas?

- e.g. reuse of CSA or RED (including component certification reuse)
- Suitability of existing threat model?

Vertical vs Horizontal Standards?

- Rolling Plan includes a diverse set of technologies.
- One size does not fit all, neither does one speed.
- Lower level of detail for specific verticals but is low level testable with legal certainty?.

Types of standards – Right types for the right purpose

- Harmonised ENs may give legal certainty but they are far from agile.
- Technical Specifications faster and can be updated but less legal certainty?

A degree of standards and ESOs competition is healthy?

- Still a significant tendency for standards bodies to "duplicate" areas of existing work.
- Co-ordination and collaboration OK at times, not as efficient as it could be.
  - e.g. 5G, NFV, AI Security, Wider IoT Security.

Standards must not be a barrier to market entry

- Participation in standards, cost of published standards, IPR in mandatary certification standards.

Vision of the Future: Wider Perspectives

Open Source

- Provides a ever larger horizontal component of ICT and Communications Technology.
- Too large and agile to test with EU CC or similar.

Secure by Design: Designer / Manufacturer Certification

- Product testing does not automatically lead to systematic design lifecycle improvements?
- Security certification of software design methodology improves all products
- Needs to be linked to EU led secure design university teaching?

ETSI is already the home of standardisation for many product and fundamental technologies in Rolling Plan

- 5G / 4G (largest 3GPP partner)
- Network Function Virtualisation
- SmartM2M / OneM2M
- Multi-Access Edge Computing (MEC)
- Intelligent Transport
- AI (Security, Network Automation, Sector specific)
- Cryptography – GSM, 3GPP, DECT, TETRA, Hiperlan

In depth security testing will always be subjective.

Any Certification approach must be complementary to exist functional and security technology standards.

Ultimately collaboration and co-ordination is a must.