# ETSI standards on consumer IoT security: EN 303 645 and TS 103 701

Presented by: **Jasper Pandza**
Rapporteur EN 303 645

**Gisela Meister**
Rapporteur TS 103 701

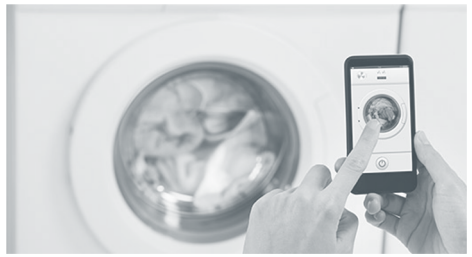
For: **ENISA Cybersecurity Certification Conference**

**18 December 2020**

# Connected consumer products

- Increasingly popular, but many are poorly secured
- Examples:
  - Just 13% of manufacturers allow vulnerability reporting (IoT Security Foundation, 17 March 2020)
  - Consumer associations and security researchers routinely identify serious issues
- Common challenges experienced by manufacturers:
  - “My organization is new to cyber security - where to begin?”
  - “There is a jungle of guidance out there, with no common baseline.”

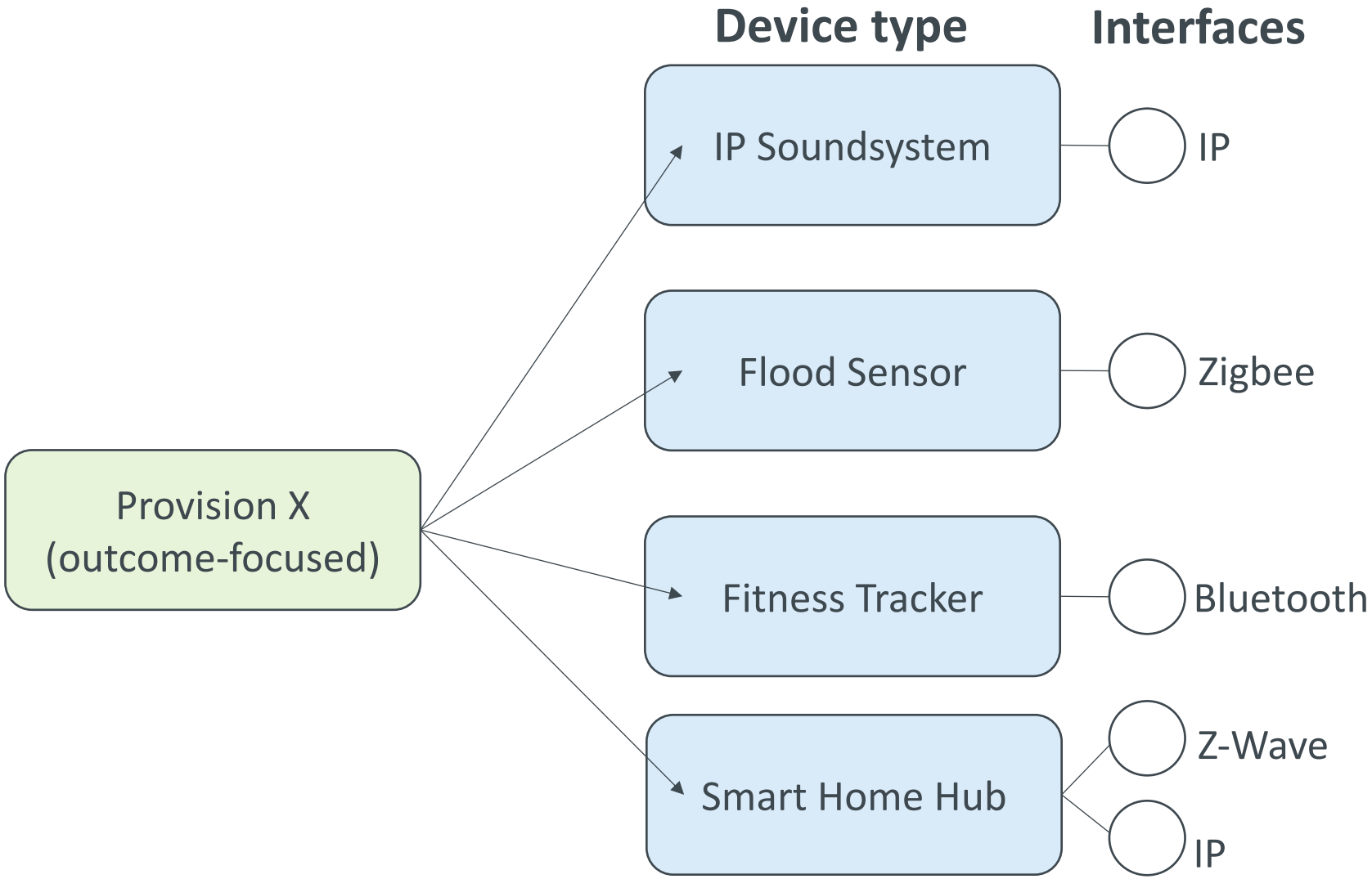




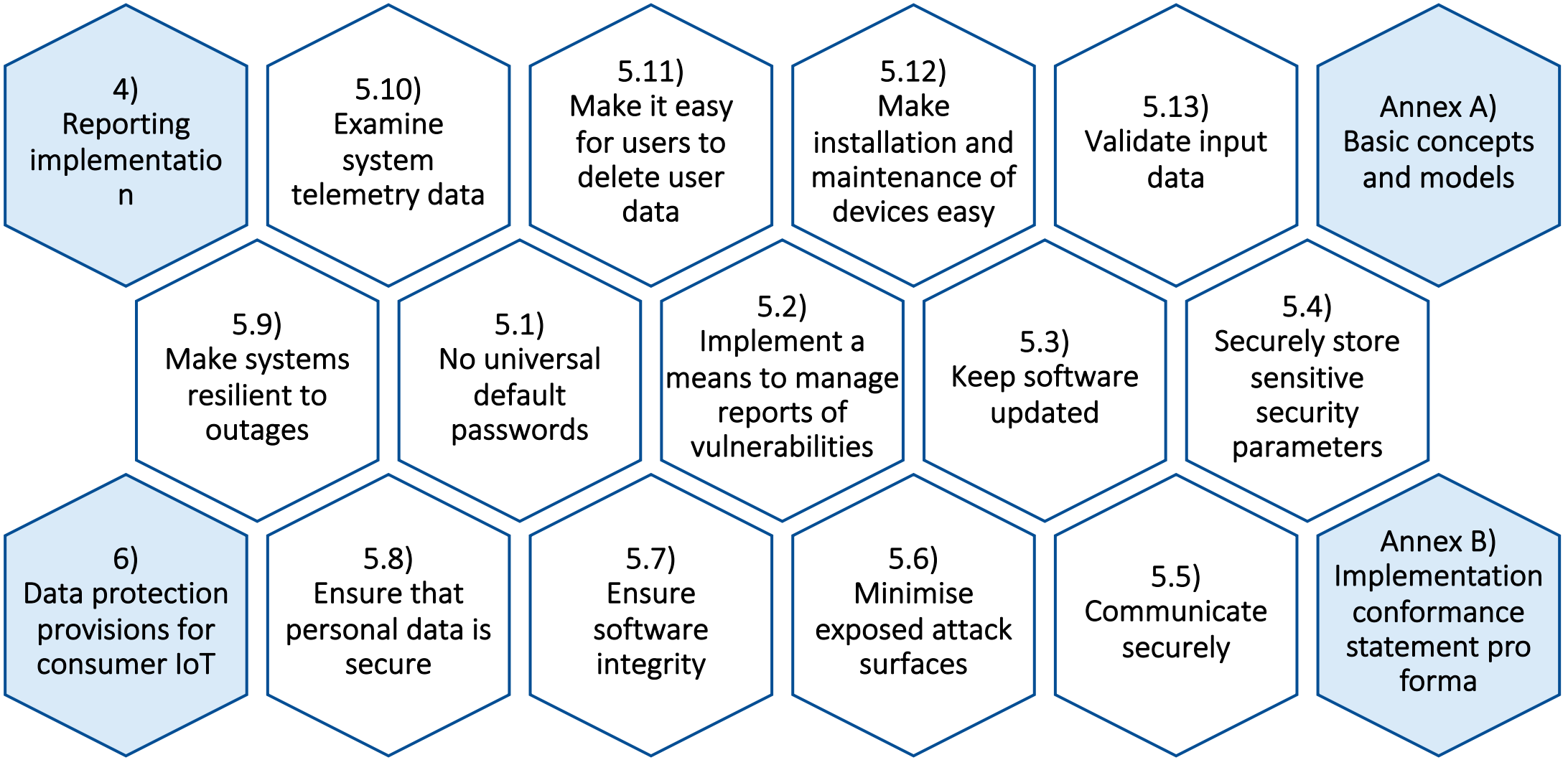

# Introducing EN 303 645: “Cyber Security for Consumer Internet of Things: Baseline Requirements”

- Establishes a common baseline across the European and wider global market, raising the security bar for all consumer IoT devices from near-zero to a good level.
- Every major, at scale, attack involving consumer IoT seen to date is covered.
  - E.g. Mirai, and more recent botnets (Satori, Okiru, OMG, Wicked, Miori)
- Comprehensively covers security and privacy best practice
  - Technical and organisational measures
- Contains outcome-focused provisions: to future-proof, create the necessary flexibility and cover *all* consumer IoT
- Pragmatic approach that is accessible to SMEs

# Challenge: implementation can vary according to product and use case



# Content of EN 303 645



# How to implement EN 303 645

## Review concepts:

- Review informative Annex A on device / network architectures and device states
- Review defined terms

## Implement provisions:

- Must implement all 33 requirements
- Should really make best attempt to implement all 35 recommendations
- Must record rationale if a recommendation is not implemented
- Refer to TR 103 621 (Q2 2021) for further guidance

## Conformance statement

- Complete Annex B: implementation conformance pro forma

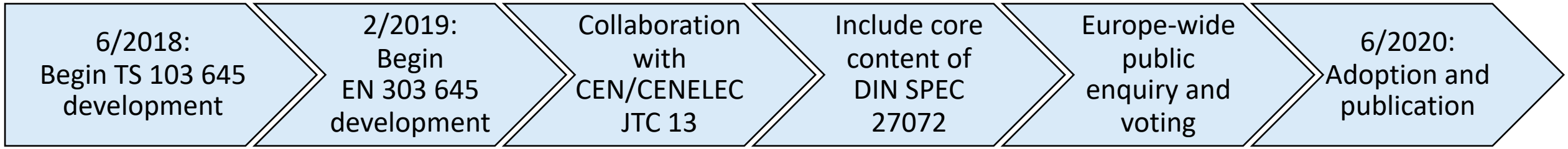
## Assessment

- Prepare for assessment (in-house or external) using TS 103 701 (Q1 2021)

# Status of ETSI TS 103 701
# “Cybersecurity assessment for consumer IoT products“

- In development, intermediate version to be published at the end of 2020. Fully adopted version planned to be published 1. Quarter 2021
- Objectives:
  - generic specification for the conformance assessment against EN 303 645
- Contains:
  - “Implementation Conformance Statement” (ICS, Annex B in EN 303 645)
  - “Implementation eXtra Information for Testing” (IXIT, defined in TS 103 701)
  - a catalogue of generic test cases mapped from all provisions of EN 303 645
- Target Group:
  - Supplier Organizations (SO) as manufacturers, in-house testing departments, independent assessment labs

# EN 303 645 development




- TC CYBER worked jointly with CEN/CENELEC JTC 13 members who made substantial contributions
- Includes core content of DIN SPEC 27072, following DE-UK technical study
- Contributors include:

# Significant uptake: selection of product assurance services

Singapore's national Cybersecurity Labelling Scheme builds on EN 303 645.

Finland's national consumer IoT certification scheme builds on EN 303 645.

PSA Certified (backed by Arm) has been mapped to EN 303 645.

The Global Certification Forum offers accreditation to EN 303 645.

TÜV Süd offers testing against EN 303 645.

TÜV Rheinland offers certification against EN 303 645.

VDE offers testing against EN 303 645.

SESIP by Global Platform has been mapped to EN 303 645 and TS 103 701.

SGS IoT Testing and Conformity Assessment Program is partially based on EN 303 645.

DEKRA offers security evaluation based on TS 103 701 and against EN 303 645.

***And many more: UL, Eurosmart, KIWA, Secura, Nemko, ACCS, DTG, IASME…***

# ETSI consumer IoT security document set: overview

**EN 303 645**
(and TS 103 645 for intermediate development)

- Covers all consumer IoT
- Baseline requirements, outcome-focused provisions

**TS 103 701**
(Publication scheduled Q1 2021)

- Conformance assessment against the EN
- For self-assessment (1st party), in-house testing (2nd party) and independent evaluators (3rd party)

**TR 103 621**
(Publication scheduled Q2 2021)

- Implementation guidance to meet EN provisions
- To contain use case examples

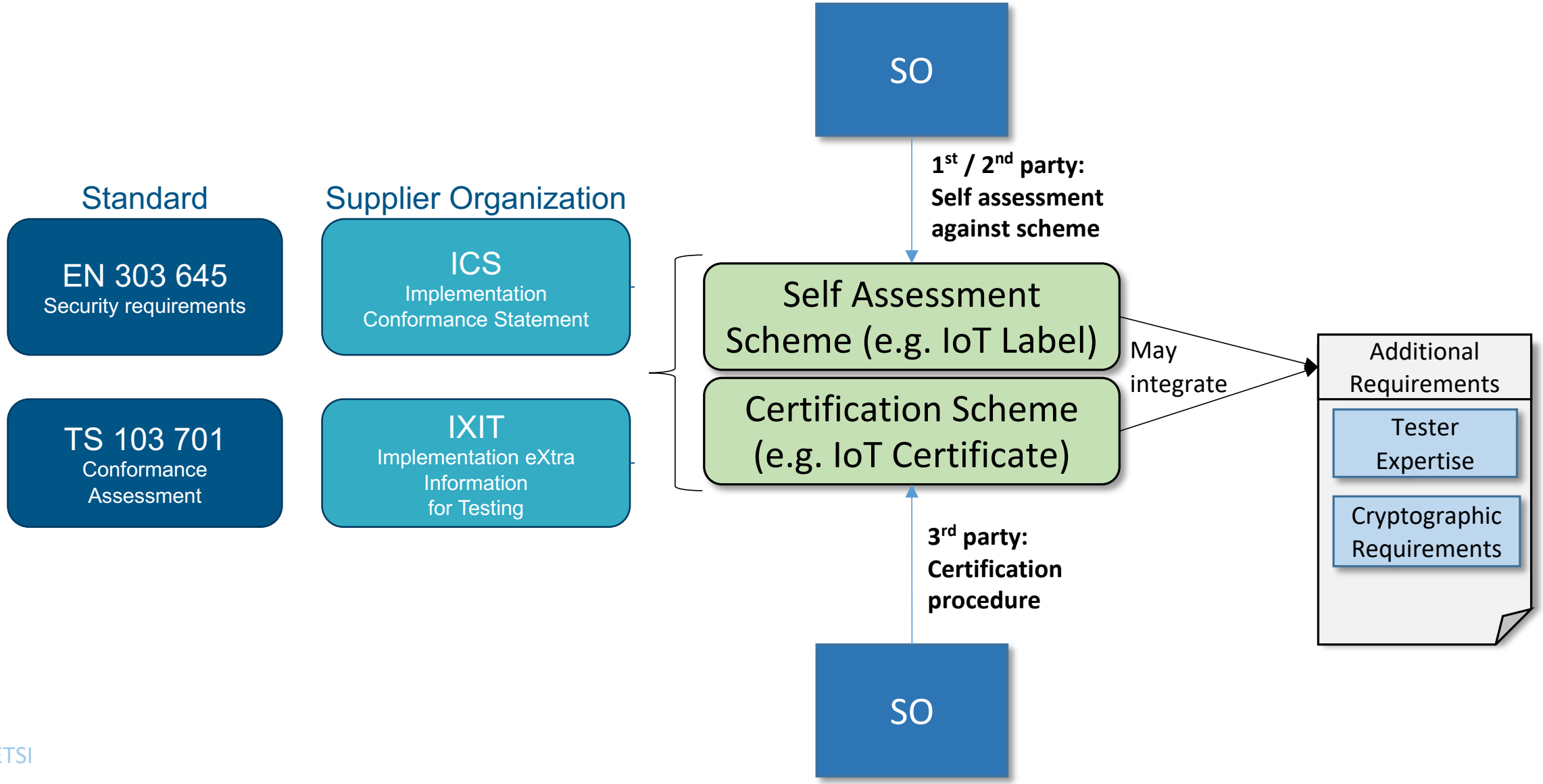
**Vertical standards / domain-specific extensions**

- E.g. smart locks
- More prescriptive, testable and stringent specifications.

# EN 303 645 in support of the Cybersecurity Act

- EU Council Conclusions on the cybersecurity of connected devices (2 December 2020):
  - "Notes the ETSI EN 303 645 cybersecurity standard for consumer IoT devices as an important step in [developing standards to support the CSA]."
  - Invites the establishment of a candidate cybersecurity certification scheme for connected devices and related services
- EN 303 645 and TS 103 701 are well placed to provide the foundation for "basic"-level consumer IoT assurance.
  - Broad, multi-stakeholder consensus
  - Pragmatic and accessible approach that achieves good security outcomes
  - Supported by evolving consumer IoT document set in ETSI TC CYBER

# Mapping of EN 303 645 / TS 103 701 on self-assessment schemes and future CSA IoT schemes



# EN 303 645 in support of market access legislation

- Radio Equipment Directive
  - EN 303 645 is not suitable to become a Harmonised Standard (HEN) under the RED. However, it can inform the development of such HEN, once commissioned.
- Proposed UK legislation on connected product security
  - Market access requirements align with EN 303 645 provisions, covering default passwords, vulnerability disclosure and transparency on security update support periods.

# Extra slides

| Document | Security level | Purpose | 2021 | 2022 | 2023 |
|---|---|---|---|---|---|
| **EN 303 645** | *Baseline requirements (raising the initial, near-zero bar, compatible with "basic level" assurance)* | Appropriate for all consumer IoT.<br>Outcome-focused provisions – the actual implementation depends on the use case.<br>Focus on what matters most. Addresses all major automated attacks on devices currently seen. | | | Q1: Begin ENAP on basis of TS 103 645. |
| **TS 103 645 (for intermediate EN development)** | | | Further develop clause 6: data protection | Review provisions with a view to making more mandatory.<br>Review applicability of key provisions to associated services. | |
| **TS 103 701** | | Motivate coherent, resource-efficient and meaningful approaches to assessing products against EN/TS x645.<br>For first, second and third party evaluators.<br>Exact implementation depends on the use case. | Q1: Publish v1 | | |
| **TR 103 621** | | Implementation guidance to help stakeholders meet EN provisions. Contains use cases. | Q2: Publish v1 | | |
| **Vertical: Smart locks (DTS/ CYBER-0058)** | | Requirements for cyber and mechanical security of consumer smart door locks.<br>Builds on EN 303 645 for cyber requirements. | Q3: Publish v1 | | |
| **No open work item at present** | | Harmonized Standard(s) for use with the RED.<br>Requirements set out in prescriptive provisions that are testable beyond doubt. | | | |
| **No open work item at present** | *More stringent ("substantial level") security requirements* | | | | |
| **No open work item at present** | *n/a* | TR to map the consumer IoT security document set to existing frameworks worldwide | | | |
| **No open work item at present** | *n/a* | TR introduction to cyber security to make this document set more accessible | | | |