The Standards People

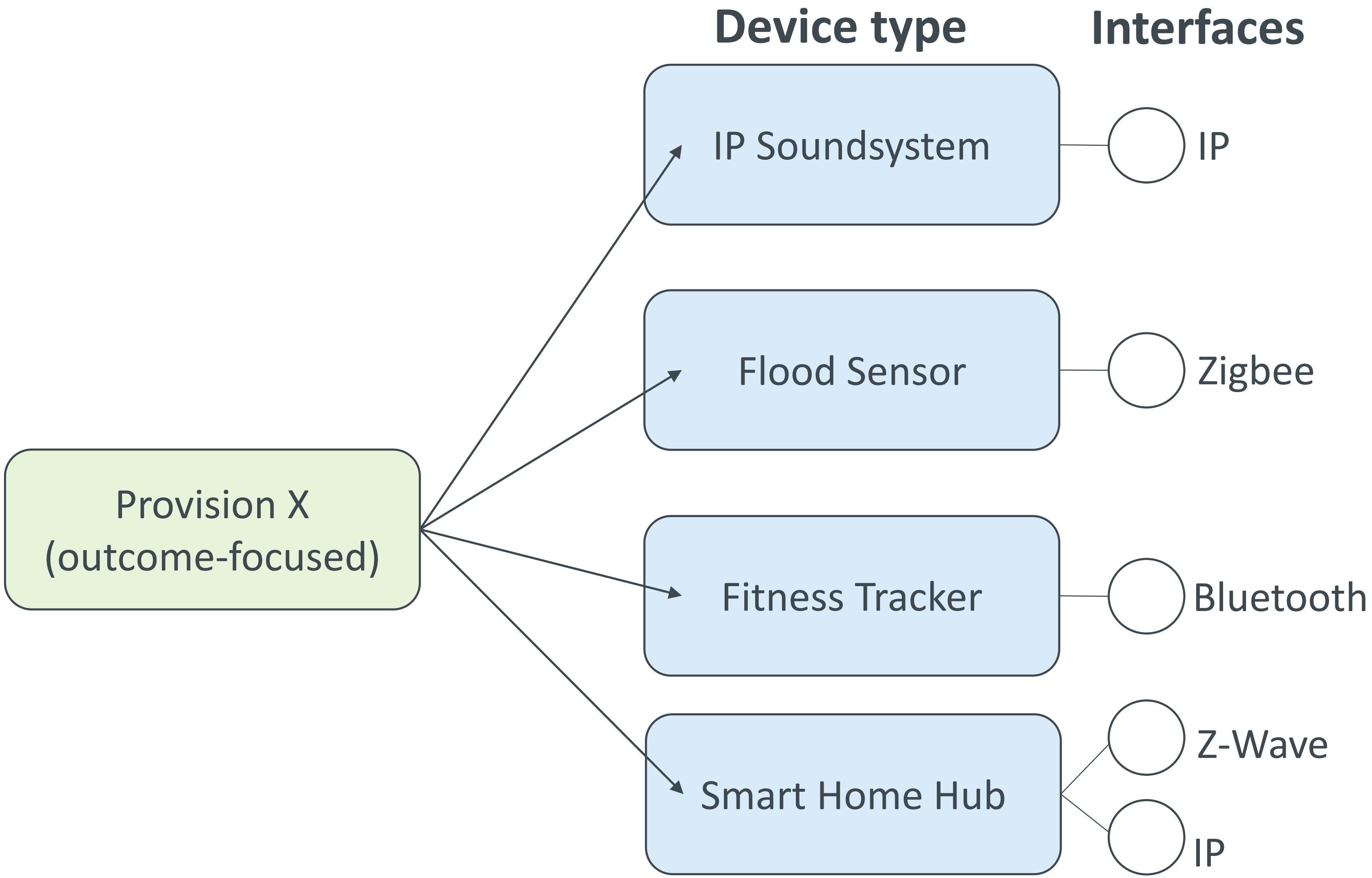
ETSI Draft Standard on Cybersecurity Assessment for consumer IoT security – Impact on future IoT Schemes

Presented by: **Gisela Meister, Eurosmart**
Rapporteur TS 103 701

For: **ENISA Cybersecurity Standardization Conference Panel 4: Future schemes: Consumer IoT**

3 February 2021

Challenge: Implementation can vary according to product and use case



Device type

Interfaces

Provision X
(outcome-focused)

IP Soundsystem

IP

Flood Sensor

Zigbee

Fitness Tracker

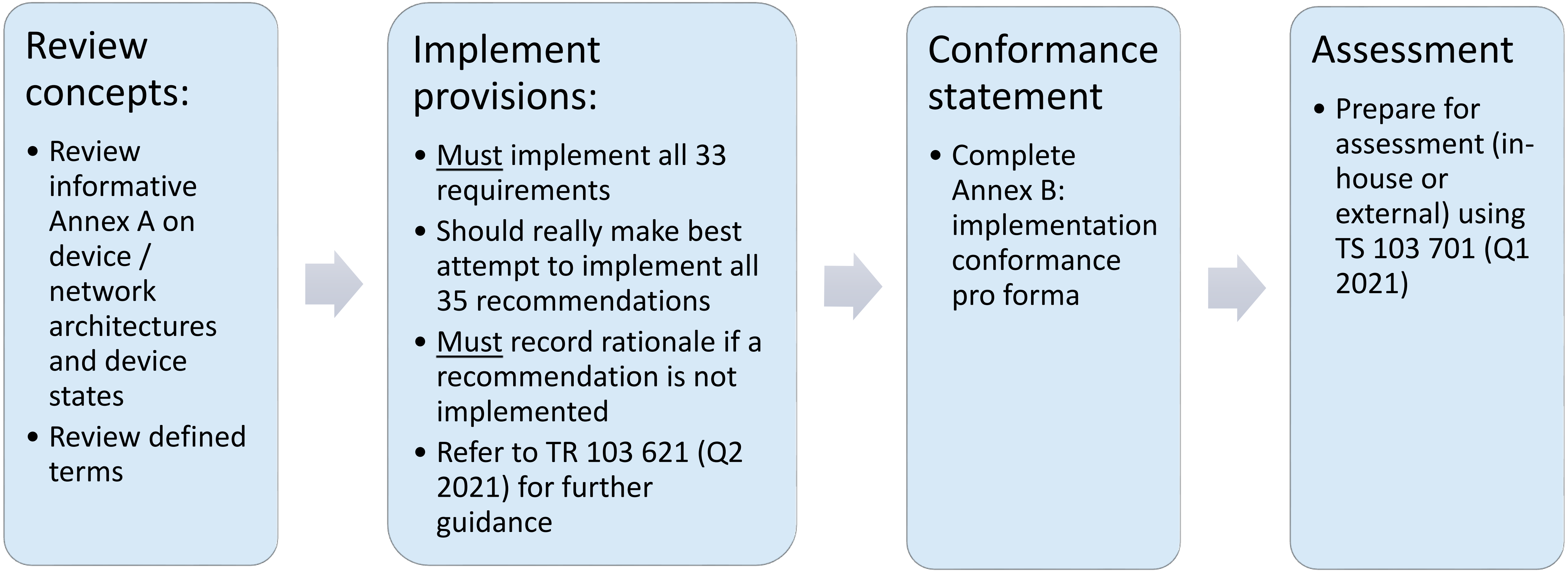
Bluetooth

Smart Home Hub

Z-Wave

IP

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

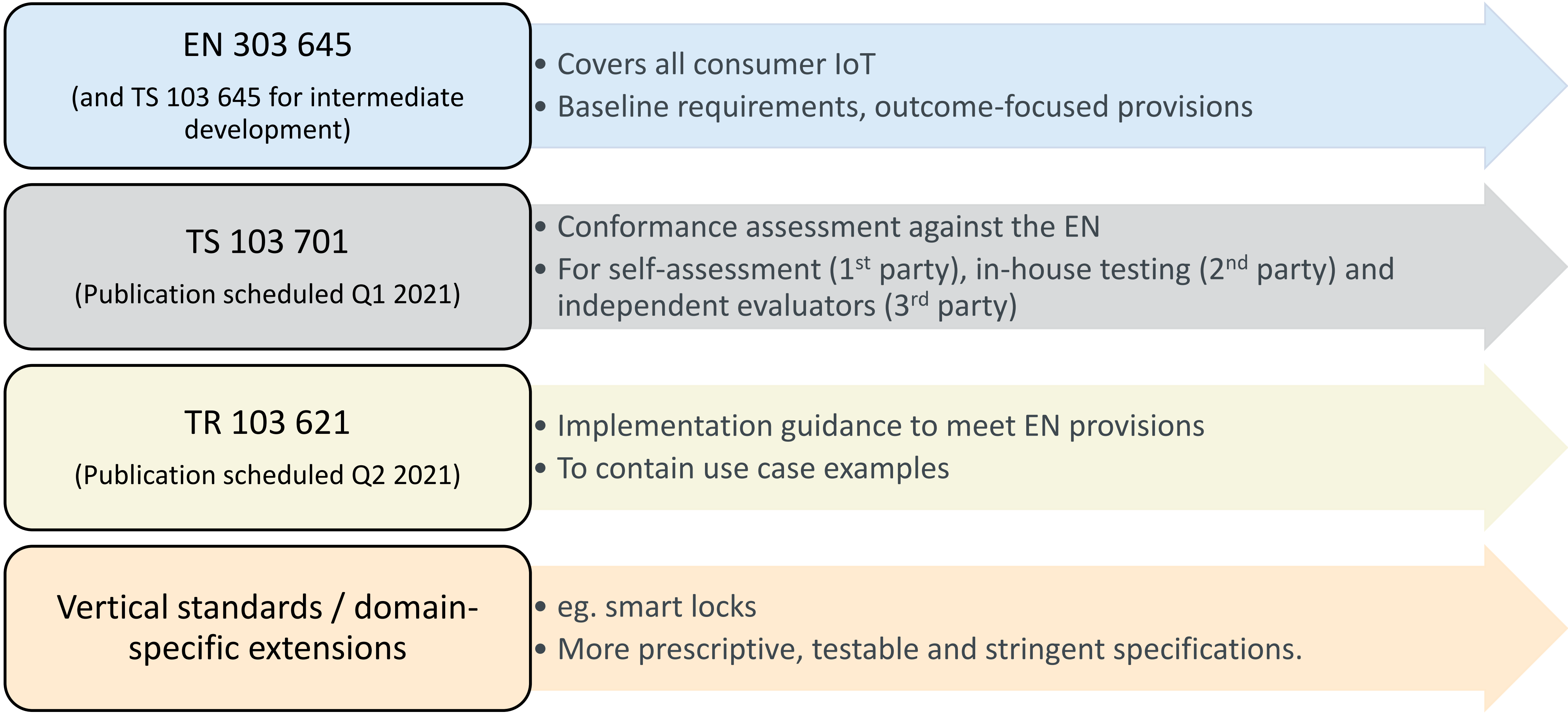
Conformance statement

- Complete Annex B: implementation conformance pro forma

Assessment

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

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

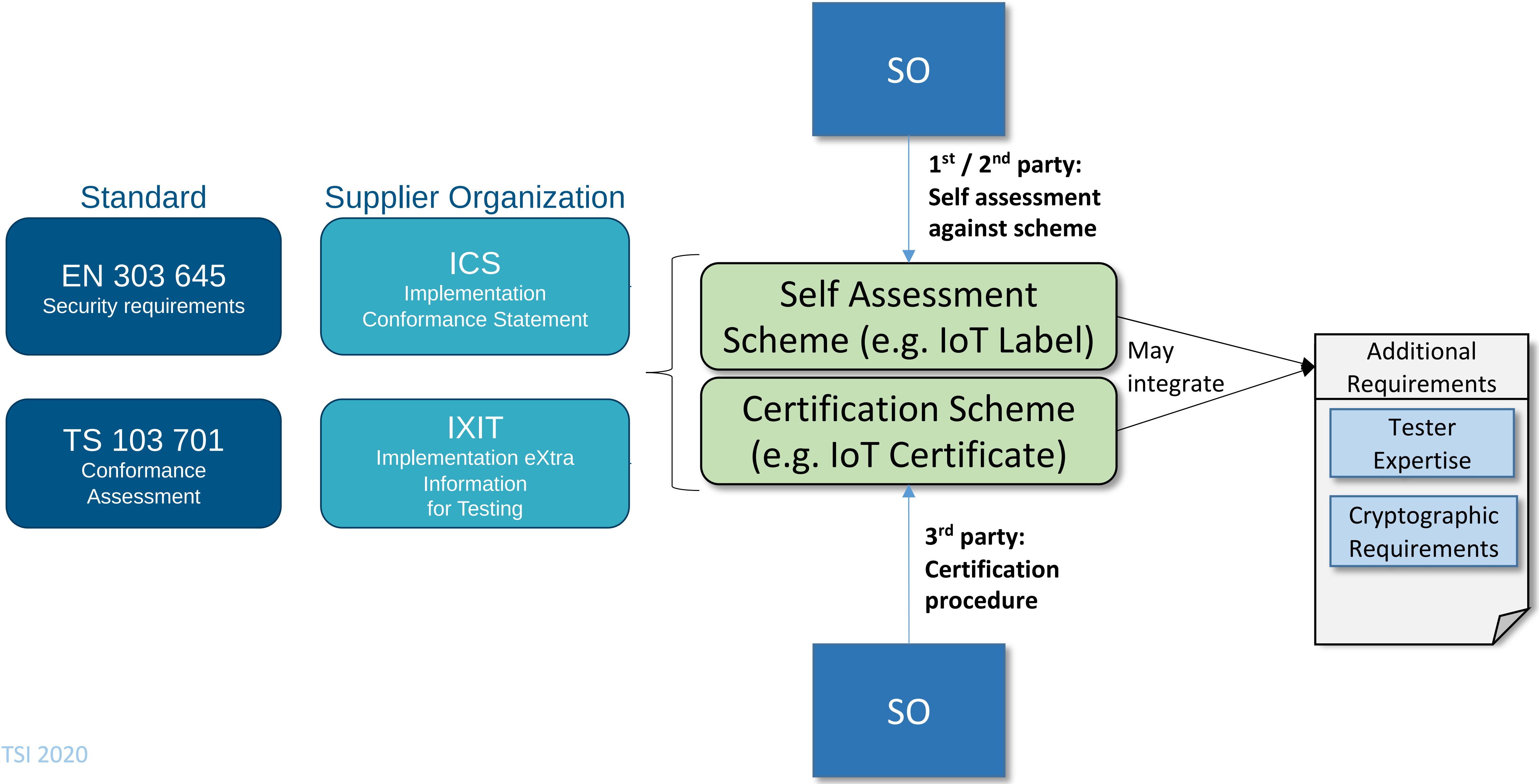
Vertical standards / domain-specific extensions

- eg. smart locks
- More prescriptive, testable and stringent specifications.

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

- In development, intermediate version V.0.0.5 has been made publicly available at 20.12.2020. Final draft for approval ready end of April.
- 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

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



Standard

Supplier Organization

EN 303 645
Security requirements

ICS
Implementation
Conformance Statement

TS 103 701
Conformance
Assessment

IXIT
Implementation eXtra
Information
for Testing

SO

1st / 2nd party:
Self assessment
against scheme

Self Assessment Scheme (e.g. IoT Label)

Certification Scheme (e.g. IoT Certificate)

May integrate

Additional Requirements

Tester Expertise

Cryptographic Requirements

3rd party:
Certification
procedure

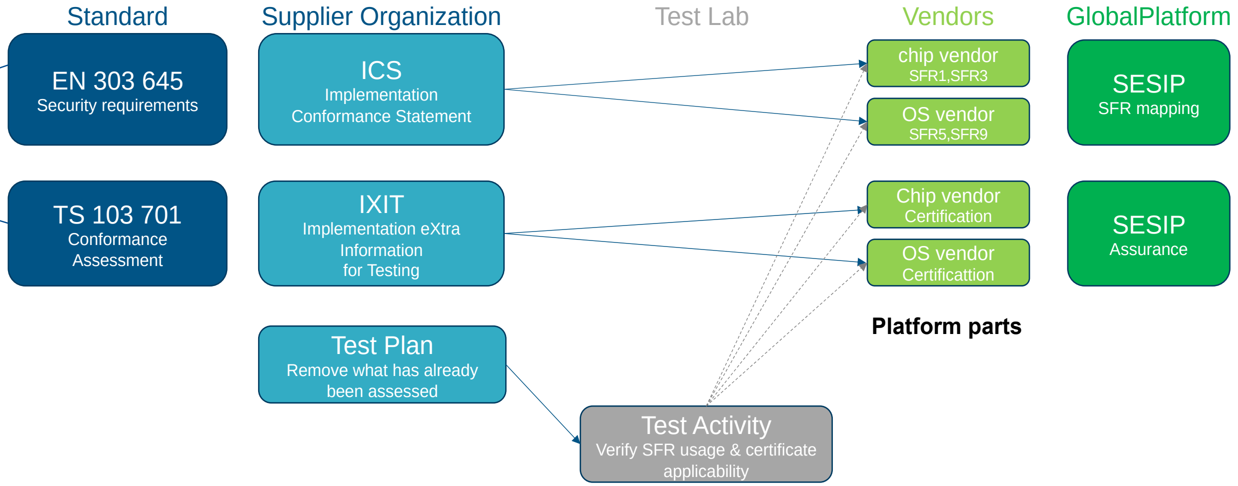
SO

Application Context
Self Assessment Schemes
German IT Security IoT Label

Application Context IoT Schemes Industry Mapping on Certification /Self Assessment Schemes as SESIP

Federal Office
for Information Security

- Based on a manufacturer declaration
- combined with a dynamic information component
- Market Surveillance by BSI



Standard

EN 303 645
Security requirements

TS 103 701
Conformance Assessment

Supplier Organization

ICS
Implementation Conformance Statement

IXIT
Implementation eXtra Information for Testing

Test Plan
Remove what has already been assessed

Test Lab

Test Activity
Verify SFR usage & certificate applicability

Vendors

chip vendor
SFR1,SFR3

OS vendor
SFR5,SFR9

Chip vendor
Certification

OS vendor
Certificattion

Platform parts

GlobalPlatform

SESIP
SFR mapping

SESIP
Assurance

Using SESIP Certified sub-components **reduces Testing Lab effort** on ‘conformity of design’ and ‘conformity of implementation’ and risk of non-conformity for the Supplier Organization

Extra slides

The German IT Security Label

- **Based on a manufacturer declaration** regarding compliance of his product to a standard (approved for the label), like
  - ✓ national technical guidelines, e.g. BSI TR Secure Broadband Router (BST TR-03148) or
  - ✓ international standards, e.g. ETSI Baseline Requirements on Cyber Security for Consumer IoT (ETSI EN 303 645)
  - ✓ to ensure verifiability and comparability an **approved standard requires an associated test specification**
- **The label is combined with a dynamic information component** (e.g. provided via a governmental website) that provides product information concerning:
  - ✓ **Transparency** means providing security relevant information about the products
  - ✓ **Patches** for closing security flaws
  - ✓ **Cryptography** to secure communication and storage
  - ✓ etc.
- **Market Surveillance** is foreseen
  - ✓ Random and ad hoc inspections will be performed
  - ✓ If manufacturers don‘t cooperate, patch or do nothing in general -> withdrawal of the label

Roadmap of TS 103701

Release v0.0.6

Mon, 1 February 2021

- Covers all mandatory provisions
  and all recommendations of EN 303 645

Release v0.0.7

Fri, 26 March 2021

- Including resolution of industry comments
  - Public review of v0.0.5
- Presentation Cyber#24

Release Final Draft for Approval v1.0

Mon, 26 April 2021