Security Conference

EN 303 645 Ecosystem Update

Presented by: Dr. Samim Ahmadi

17/10/2023

Introduction to ETSI EN 303 645 / ETSI TS 103 645

6/2018: Begin TS 103 645 development

2/2019: Begin EN 303 645 development

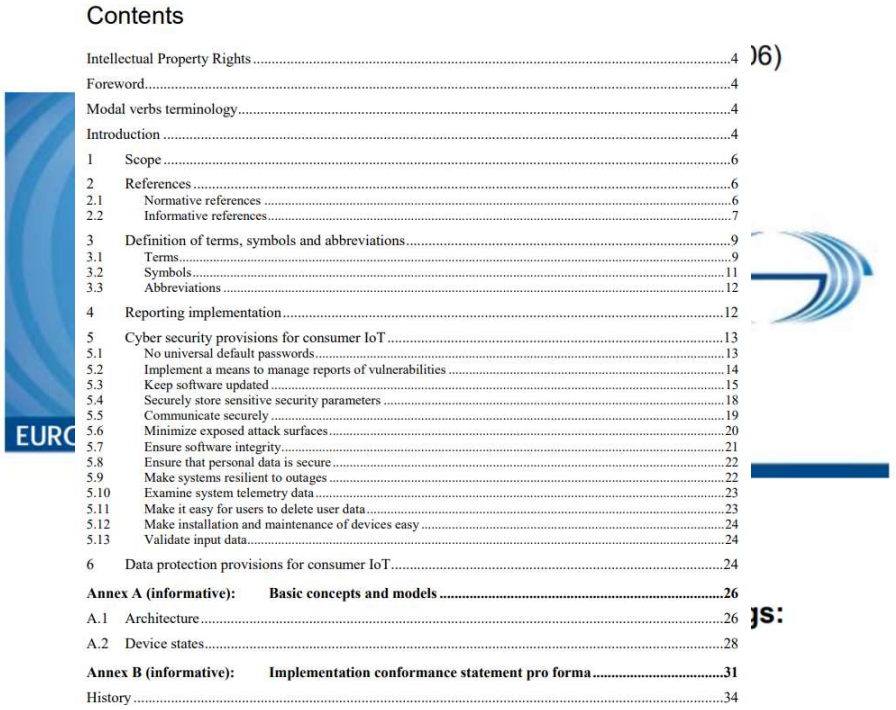
Collaboration with CEN/CENELEC JTC 13

Include core content of DIN SPEC 27072:2019

Europe-wide public enquiry and voting

6/2020: Adoption and publication

- 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
- Contains generically formulated security & data protection requirements to create the necessary flexibility and to cover all consumer IoT



Contents

Update of ETSI TS 103 645

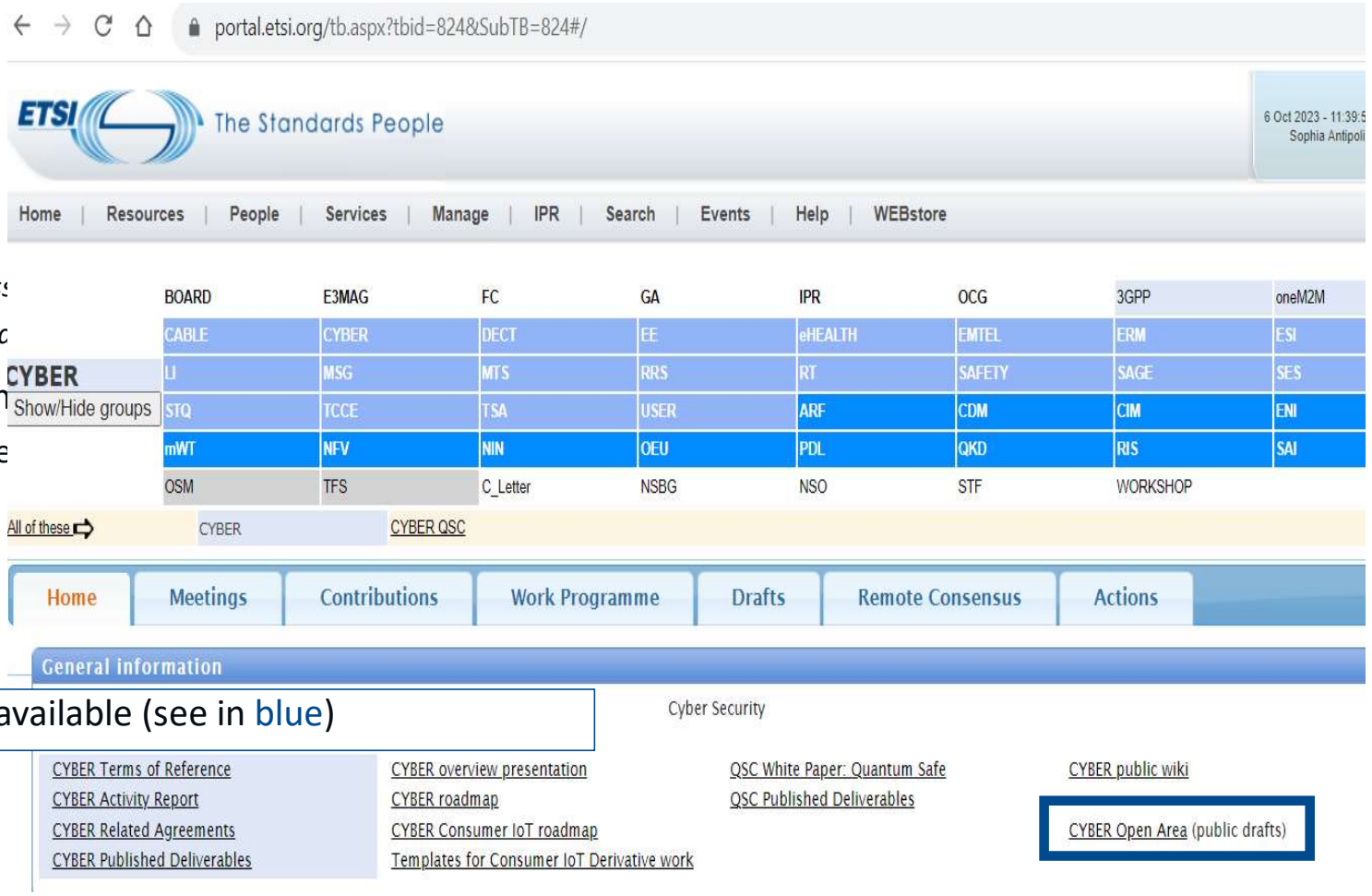
Clause 5 on security provisions:

- No major technical changes
- Clarifications / precisions added
  - Clarifications: E.g. *service* vs *ass*
  - Precision: E.g. term *constrained*

Clause 6 on data protection provision

- Technical changes appear to mee

➔Current interim draft is publicly available (see in blue)

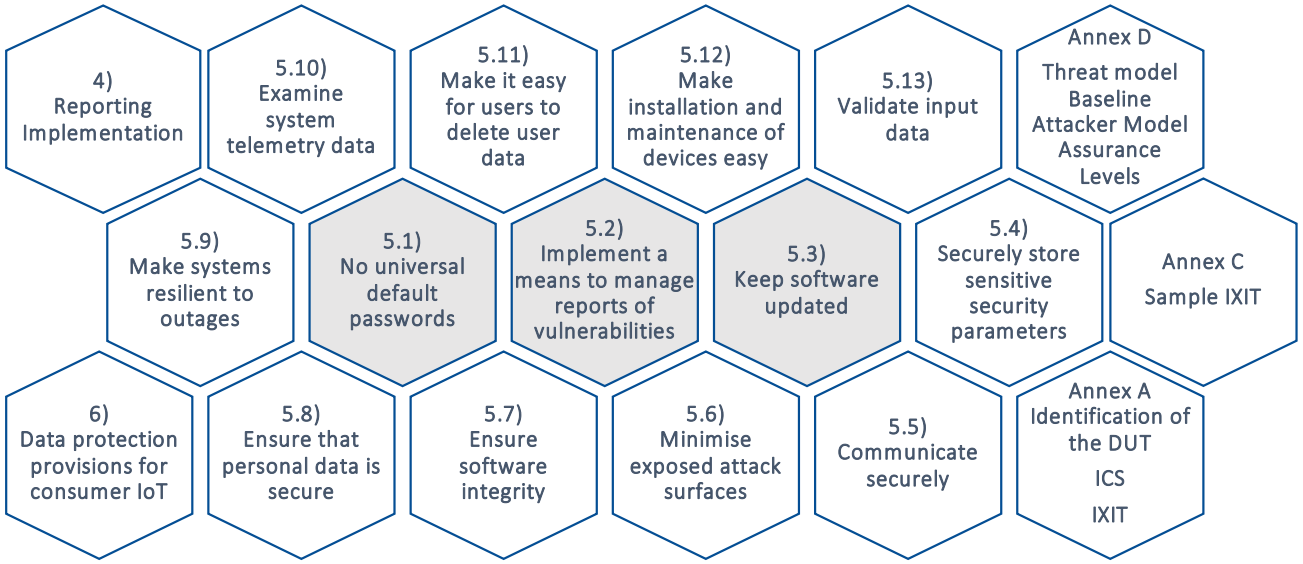


ETSI TS 103 701
Assessment criteria for ETSI EN 303 645

ETSI TS 103 701 provides examples and templates for the required

- Implementation Conformance Statement (ICS)
- Implementation eXtra Information for Testing (IXIT)

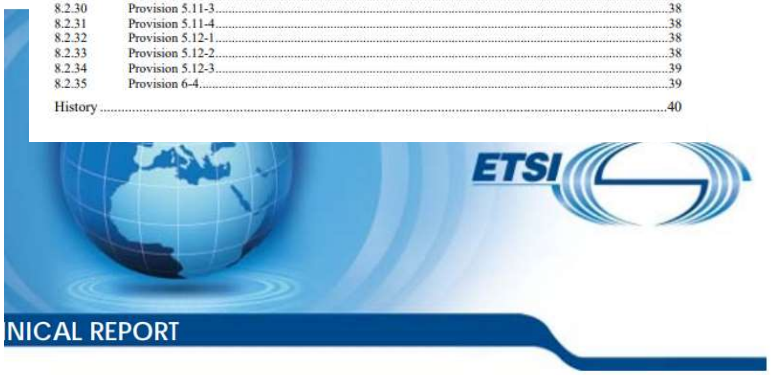
Catalogue of generic test cases mapped to all provisions of EN 303 645:



Changes to be expected depending on ETSI TS 103 645 update

ETSI TR 103 621

Contents



uide to Cyber Security for Consumer Internet of Things

ETSI TR 103 621
Example to meet a provision

6.9 Provision 5.3-1

"All software components in consumer IoT devices should be securely updateable". (ETSI EN 303 645 [i.1])

NOTE: Examples for this provision are also provided in ETSI EN 303 645 [i.1].

EXAMPLE 1: The secure update mechanism supports the device firmware and all third-party applications. The device firmware encompasses code running electronic components such as baseband processors, interface and networking chipsets, and sensors.

EXAMPLE 2: The device or hub accepts trusted updates that are signed by the manufacturer, which cover all device software components. The manufacturer is able to push updates to the device.

ETSI TR 103 621

Example allowing non-compliance with a „should“ provision / recommendation

8.2.3 Provision 5.3-1

"All software components in consumer IoT devices should be securely updateable". (ETSI EN 303 645 [i.1])

EXAMPLE: The software of a battery charge controller is not meant to be modified once it has been vetted for safety.

Last update on ETSI TR 103 621: V1.2.1

- Text was added to consider threats arising from the use of CIoT devices for domestic abuse
  - Some examples highlighted in blue
- Text was added to consider measures which could help to mitigate domestic abuse by using CIoT devices
  - Some examples are highlighted in green
- Current work on that topic within ETSI TC CYBER:
  - ETSI-Guide to Coercive Control (see SESSION D3-2)

Changes to be expected depending on ETSI TS 103 645 update

The examples in clauses 6 and 7 of the present document provide guidance on the implementation of cybersecurity mainly protecting users from unknown other users. However, consumer IoT devices can be misused, e.g. by intimate partners, which makes it even more difficult to find appropriate security measures.

The following list provides examples of related threats using consumer IoT devices:

- audio control (i.e. recording and/or replying);
- video control (i.e. recording and/or displaying);
- data control (i.e. collection, manipulation, unintended disclosure);
- access to shared accounts linked to the consumer IoT device and therefore providing the possibility for social stalking (e.g. social media);
- other remote control threats (e.g. heating control, door lock control).

The exploitation of the aforementioned threats might result in coercive control (e.g. isolation from friends and family, spying, deprivation of vital and basic means such as medical services and food, controlling finances, etc.).

In this regard, the following measures could help to mitigate domestic abuse by using consumer IoT devices [i.31]:

- introduction of legal policy to prosecute abusers and protect victims of domestic abuse in cases of digital coercive control;
- development of technology that at least provides evidence of activity in cases of domestic abuse, however, without violating data protection/privacy regulations;
- creation of awareness to improve prevention, and establish contact possibilities in cases of domestic abuse to support the victims by providing appropriate advice.

Privacy and data protection related legislation only cover a small part of the first of the aforementioned measures as requirements are set against personal data in terms of transparency in processing as well as purpose limitation, accuracy, integrity and confidentiality.

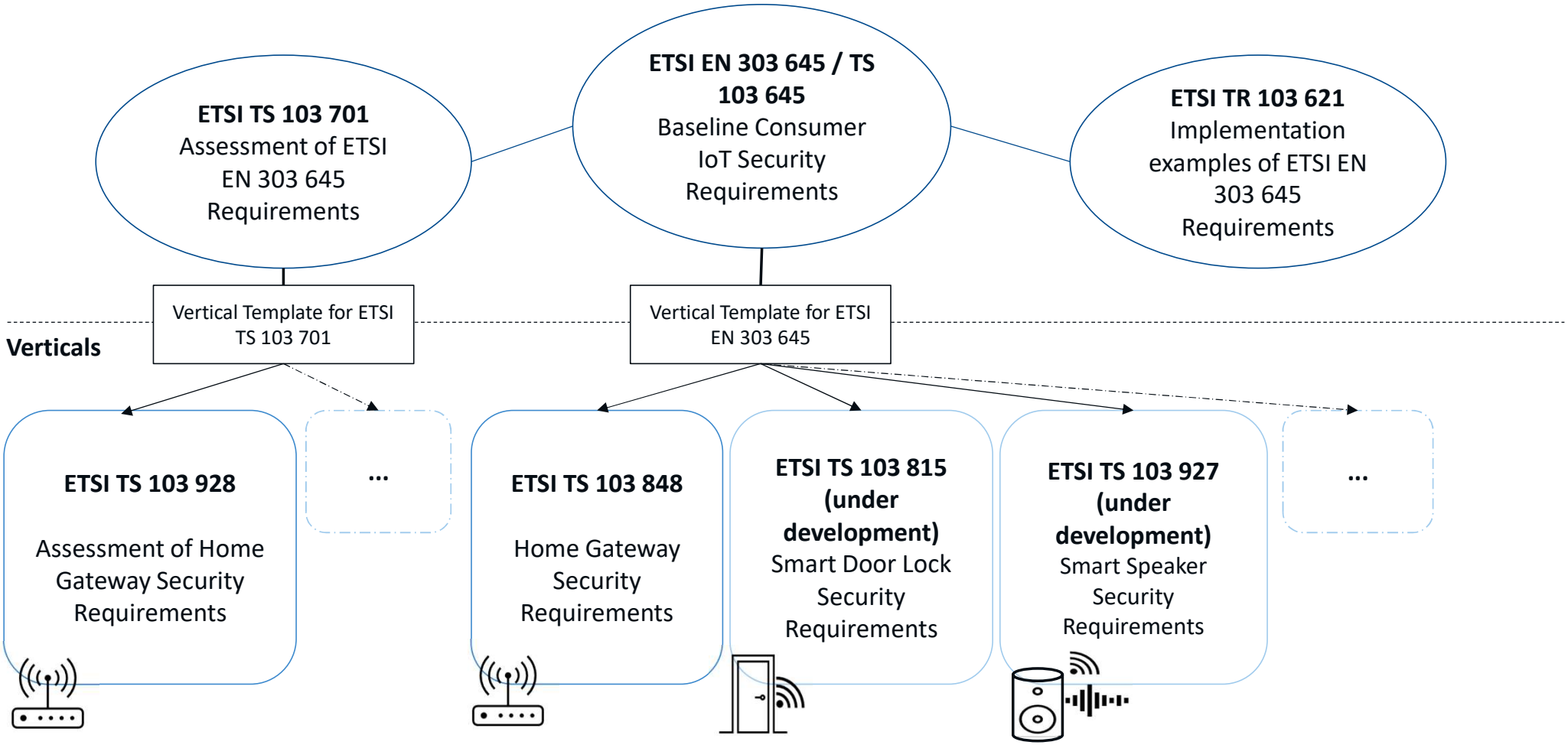
The second item referring to technology depends on the specific application scenario and can be considered during the development of corresponding solutions or verticals based on ETSI EN 303 645 [i.1] appropriate to the properties of the technology, risk, benefit and usage. Designing ways to prevent the misuse of the device intends to mitigate the risk of its misuse, but it is understood that it might not eliminate the risk entirely.

The item regarding awareness can be realized by training and by reaching out to all stakeholders of consumer IoT products, for instance by advertisements or by including the domestic abuse matter into guidelines as in the present document.

NOTE: The UK Code of Practice for Consumer IoT Security [i.32] provides statistics and references to the current state of the art regarding research in consumer IoT tech abuse. It also references to industry actors providing guidelines to prevent that technology is being used for domestic abuse.

6 Examples to meet cyber security provisions for consumer IoT

Overview of ETSI's CIoT security documents including **verticals**



Thank you for your attention

Follow us on:

Any further questions?

Contact me:

samim.ahmadi@accenture.com