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.
Update of ETSI TS 103 645

Clause 5 on security provisions:
- No major technical changes
- Clarifications / precisions added
  - Clarifications: E.g. service vs as:
  - Precision: E.g. term constrained

Clause 6 on data protection provisions:
- Technical changes appear to meet...
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
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.
ETS 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.
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
Overview of ETSI’s CIoT security documents including **verticals**

- **ETSI TS 103 701**
  - Assessment of ETSI EN 303 645 Requirements

- **ETSI EN 303 645 / TS 103 645**
  - Baseline Consumer IoT Security Requirements

- **ETSI TR 103 621**
  - Implementation examples of ETSI EN 303 645 Requirements

**Verticals**

- **ETSI TS 103 928**
  - Home Gateway Security Requirements

- **ETSI TS 103 848**
  - Home Gateway Security Requirements

- **ETSI TS 103 815**
  - Under development
    - Smart Door Lock Security Requirements

- **ETSI TS 103 927**
  - Under development
    - Smart Speaker Security Requirements
Thank you for your attention
Any further questions?

Contact me:
samim.ahmadi@accenture.com