EN 303 645:
The European Standard
on connected device security

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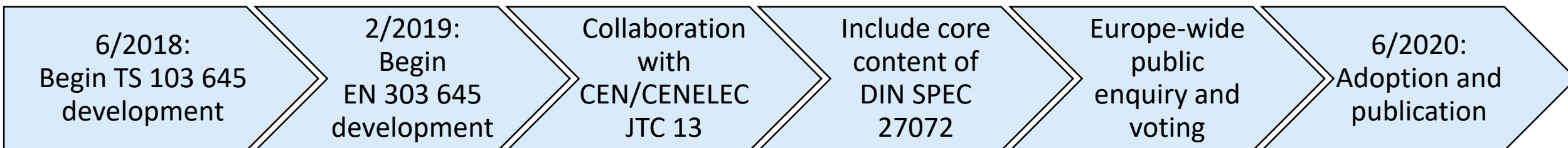Rapporteur EN 303 645

For: **Cybersecurity Standardization Conference 2021**

3 February 2021

© ETSI

Introducing EN 303 645

- 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

- Comprehensively covers security and privacy best practice

- Pragmatic approach that is accessible to SMEs

- Contains outcome-focused provisions: to future-proof, create the necessary flexibility and cover *all* consumer IoT

EN 303 645 development

| 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 | Europe-wide public enquiry and voting | 6/2020: Adoption and publication |

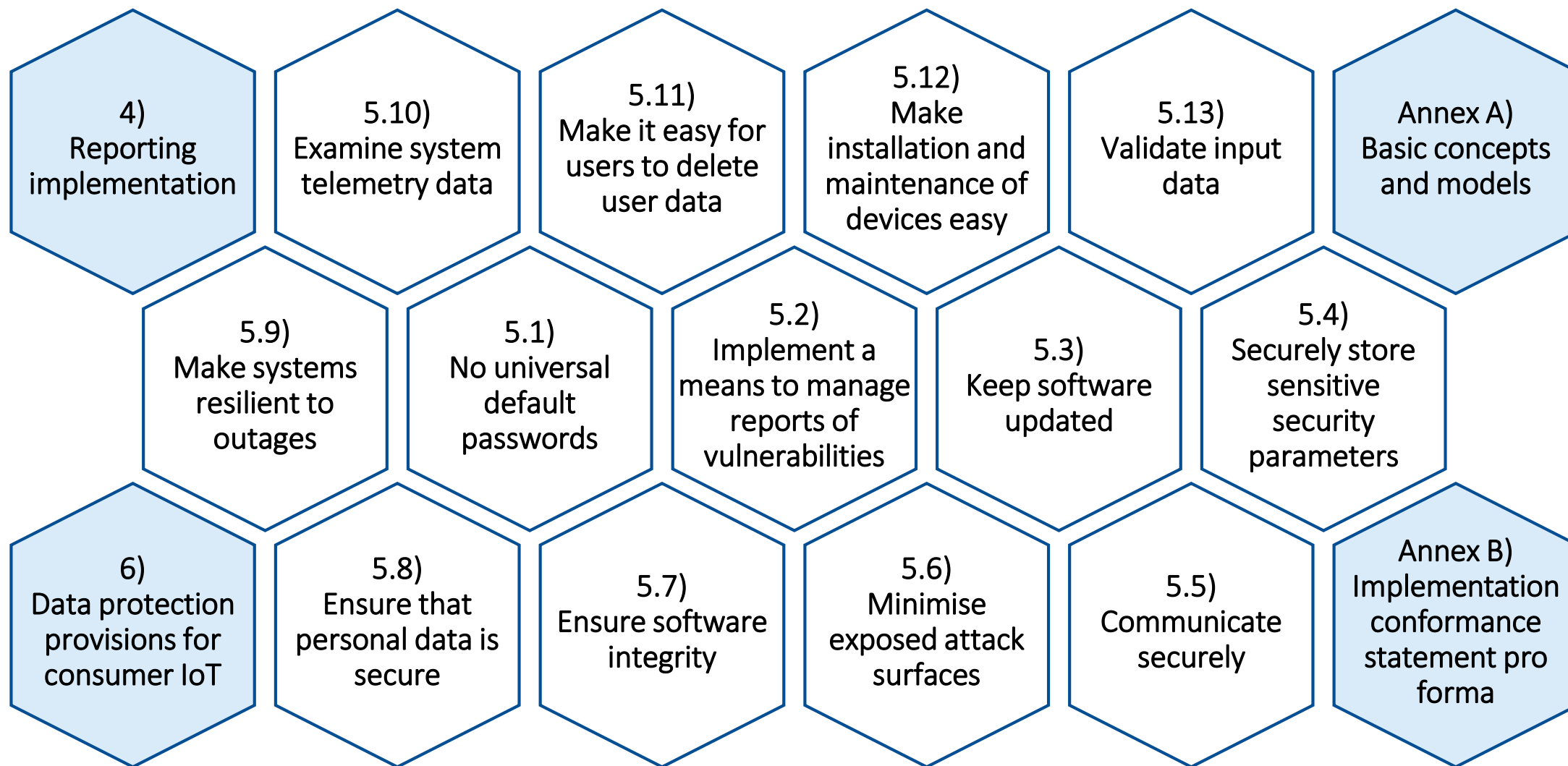- TC CYBER worked jointly with CEN/CENELEC JTC 13 members who made substantial contributions

- Includes core content of DIN SPEC 27072, following DE-UK technical study

- Contributors include:

Content of EN 303 645

4)
Reporting
implementation

5.10)
Examine system
telemetry data

5.11)
Make it easy for
users to delete
user data

5.12)
Make
installation and
maintenance of
devices easy

5.13)
Validate input
data

Annex A)
Basic concepts
and models

5.9)
Make systems
resilient to
outages

5.1)
No universal
default
passwords

5.2)
Implement a
means to manage
reports of
vulnerabilities

5.3)
Keep software
updated

5.4)
Securely store
sensitive
security
parameters

6)
Data protection
provisions for
consumer IoT

5.8)
Ensure that
personal data is
secure

5.7)
Ensure software
integrity

5.6)
Minimise
exposed attack
surfaces

5.5)
Communicate
securely

Annex B)
Implementation
conformance
statement pro
forma

How to implement EN 303 645

Review concepts:

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

Implement provisions:

- <u>Must</u> implement all 33 requirements
- Should really make best attempt to implement all 35 recommendations
- <u>Must</u> 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)

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.

ioXt is developing a new assurance profile for 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 fully includes 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…

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]."

- 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

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

  - Forthcoming requirements align with EN 303 645, covering default passwords, vulnerability disclosure and transparency on security update support periods.

Further information

- Overview of ETSI TC CYBER initiatives in consumer IoT security:
https://www.etsi.org/technologies/consumer-iot-security

- Work item of ETSI EN 303 645 with link to adopted version 2.1.1:
https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=57991

  - ETSI standards are available free of charge

- ETSI press release of 30 June 2020 to mark publication of EN
https://www.etsi.org/newsroom/press-releases/1789-2020-06-etsi-releases-world-leading-consumer-iot-security-standard