Achievements of Cybersecurity Standardisation & Rolling Plan

Alex Leadbeater
Chairman TC Cyber
BT Group Plc

ETSI in a nutshell

- ICT standards organization, European roots, with global reach
- At the forefront of emerging technologies
  - NFV, IoT, smart cities, quantum safe cryptography, AI, edge computing…
- Global partnership projects: 3GPP and oneM2M
- Direct participation; consensus based
- Unique Centre for Testing and Interoperability (CTI)
- Renowned IPR policy

- ❖ Over 850 members of various sizes
  - ❖ From 65 countries & 5 continents
    - ❖ More than 45 000 free publications
    - ❖ More than 100 partnerships
    - ❖ Over 90 technical groups engaged in more than 4 000 meetings
    - ❖ More than 50 conferences and interop events per year
    - ❖ 25% of our members are SMEs

ETSI Cybersecurity Standards

ETSI develops security standards across full spectrum of Communications, Cloud, AI, IoT and Internet technology.

- Commercial Industry led.

- TC Cyber, ESI, ISG NFV, ISG ZSM, ISG ENI, ISG SAI, MEC.

- Security related partnerships e.g. 3GPP (5G), Smart M2M, GSMA

TS 103 645 Cyber Security for Consumer Internet of Things

- v1.1.1 Published Feb 2019

- First globally-applicable industry standard on consumer IoT security

- Global recognition and adoption

EN 303 645 Cyber Security for Consumer Internet of Things

- Under ENAP ballet ending Feb 2020.

- Developed in co-operation with CEN, CEN-ELEC & DIN

TS 303 701 Cybersecurity Assessment for Consumer IoT Products

ETSI CSA Roadmap Considerations

ETSI CSA related priorities include;

Consumer IoT

- Completion of EN 303 645 / TS 303 701

5G Networks (in partnership with 3GPP & GSMA)

- NESAS

eIDAS (ETSI Trust Service Standards) EN 319 403
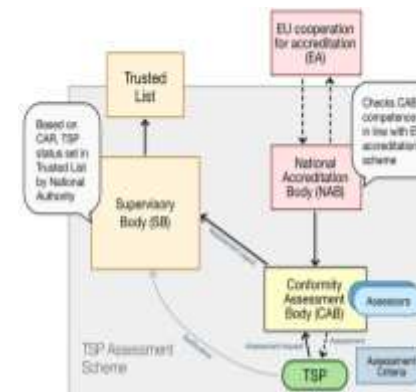
NFV

AI

QKD

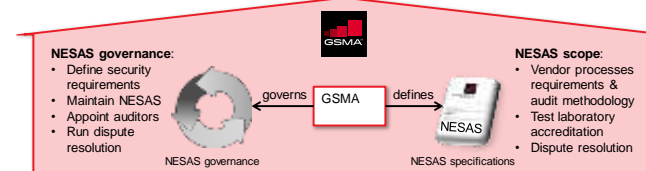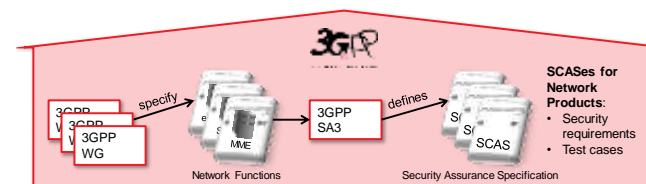CEN/CEN-ELEC JWG on Consumer IoT Security Aspects

Both traditional standards and open source projects (eg OSM)

Inter-relationship of RED

Industry developed schemes

ETSI Audit Scheme under eIDAS

Roles of GSMA and 3GPP in NESAS

ETSI Certification & Standards Considerations

Goal: Building consumer trust in EU products through standardisation and certification.

"Voluntary" certification standards: Need to build a culture of Security adds value and suppliers gain value by acting responsibly with user data.

Any certification scheme needs to add value and not be a box ticking exercise.

Whole lifecycle of the product needs to considered and possibility of use in different verticals.

Fit for purpose - Industry wide development of the schemes through ESOs essential.

Certification must not be a barrier to entry or EU innovation

Standards development must be open to all and freely available once published.

One size does not fit all.

Technology will always outpace standards & certification.

 - existing ESO EN & TS processes too slow to cover all scenarios?