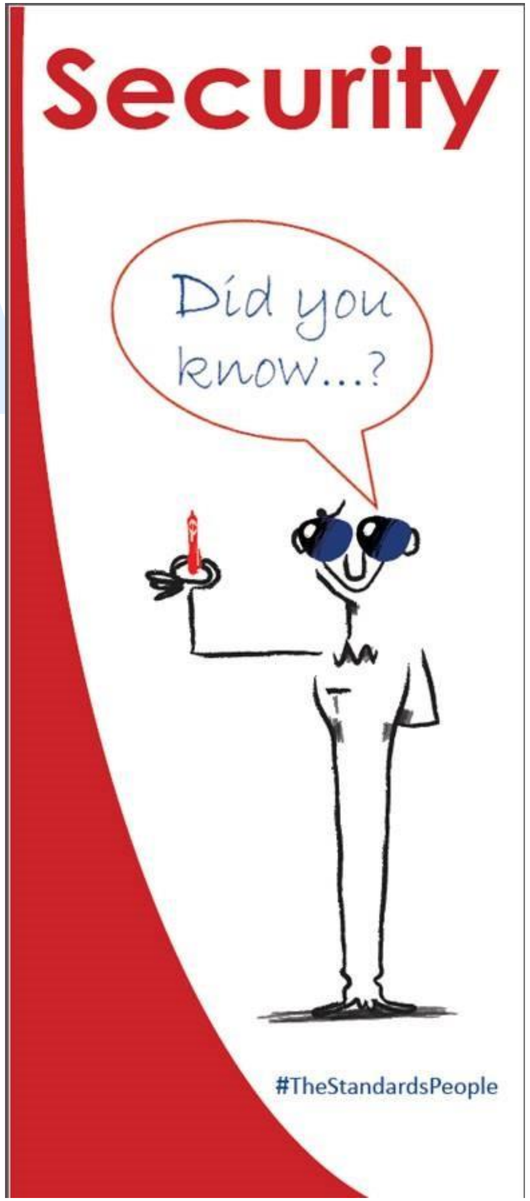
The Standards People

Standardization for cybersecurity

Presented by: **S. Compans**

For: **ILNAS workshop**

28 June 2019



Security @ ETSI

CROSS-DOMAIN CYBERSECURITY

- Ecosystem
- Protection of personal data & coms
- IoT security and privacy
- Critical infrastructures
- Enterprise and individual cybersecurity
- Forensics
- Information Security Indicators

SECURING TECHNOLOGIES & SYSTEMS

- Mobile / wireless systems (5G, TETRA, DECT, RRS,RFID...)
- IoT
- Network functions virtualization
- Intelligent Transports
- Broadcasting
- Artificial Intelligence

SECURITY TOOLS & TECHNIQUES

- Lawful interception & retained data
- Digital signatures & trust services
- Permissioned distributed ledgers
- Smart cards / secure elements
- Security algorithms
- Quantum key distribution
- Quantum safe cryptography

TC CYBER

What is TC CYBER?

- TC CYBER is ETSI’s Centre of Excellence for Cyber Security
- Created in 2014, TC CYBER works on a range problems – from privacy, to IoT, to protecting personal data and quantum-safe cryptography
- Works on both industry security challenges and EU security mandates to address global cyber security problems
- TC CYBER has fortnightly working calls and meets face-to-face four times per year.

Ongoing work in TC CYBER

Cybersecurity ecosystem

Protection of personal data and communication

IoT Security and Privacy

Cybersecurity for Critical Infrastructures

Enterprise/organization and individual cybersecurity

Forensic activities

Cybersecurity tools

Direct support to EU legislation

Quantum-Safe Cryptography

1. Cyber security eco-system

Informing TC CYBER’s global view of cyber security.

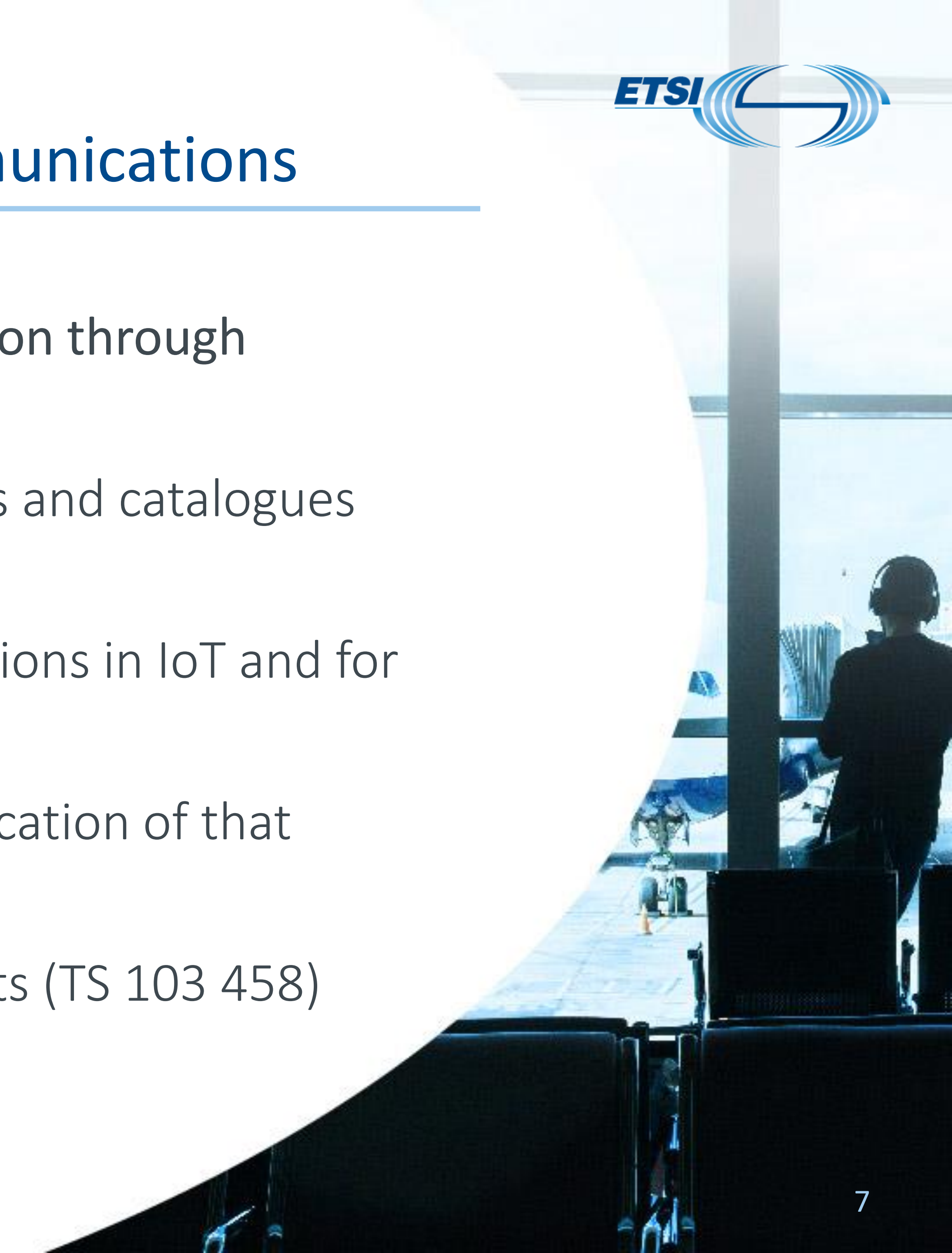
Specifications include:

- Technical Report 103 306 Global Cyber Security Ecosystem
- Technical Specification CYBER-0022 (TS 102 165 series) Methods and Protocols for Security

2. Protection of personal data and communications

ETSI provides technical support to privacy legislation through standards. In particular:

- A technical guide to privacy, which addresses and catalogues relevant standards globally (TR 103 370)
- Identity and identity management – applications in IoT and for pseudonymity (TS 103 486 ongoing work)
- Mechanisms for privacy assurance and verification of that assurance (TS 103 485 ongoing work)
- Attribute-Based Encryption ABE requirements (TS 103 458)



3. IoT security and privacy

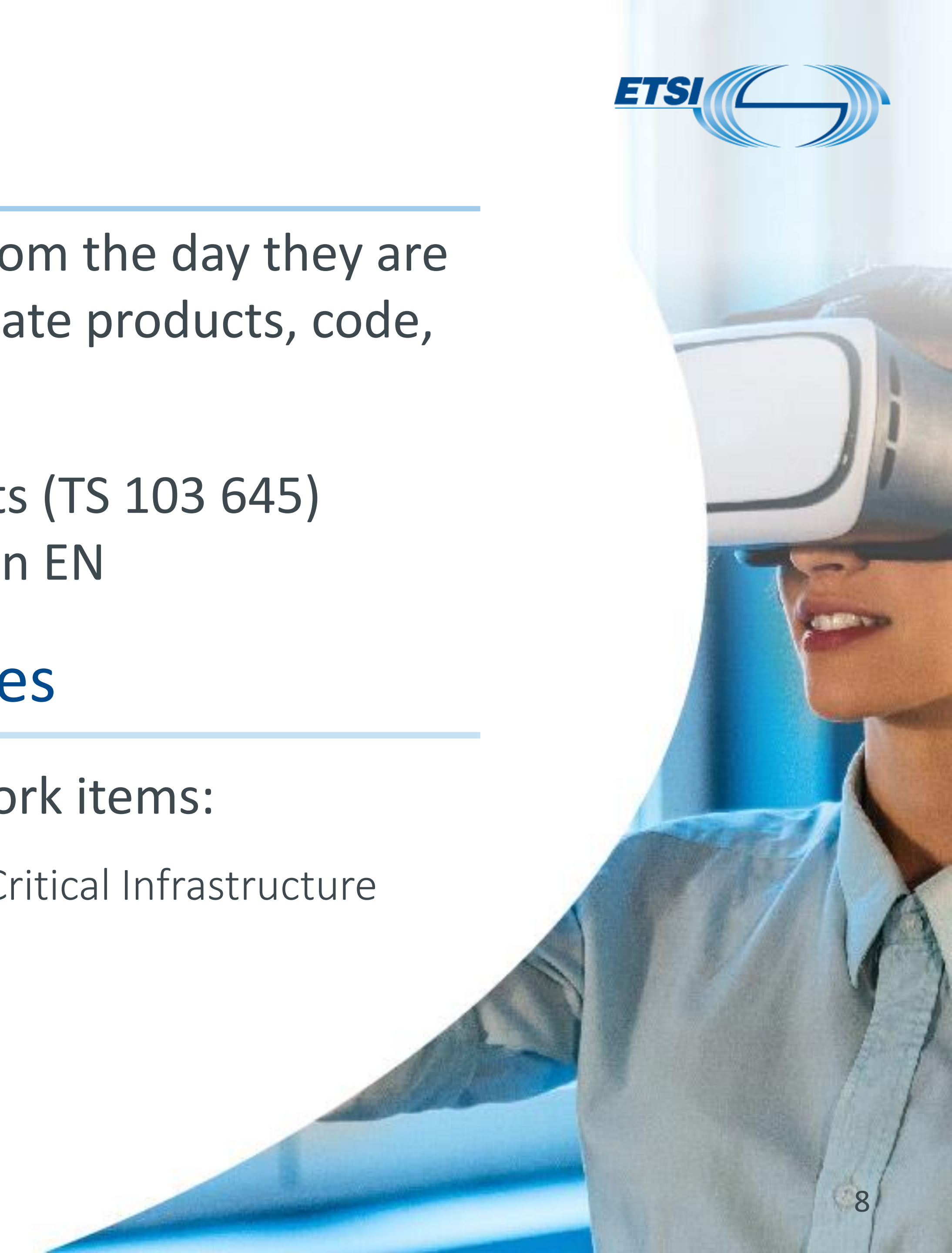
Many IoT devices, systems, services are insecure from the day they are designed. “Secure by design” means starting to create products, code, and software with security in mind from the start.

TC CYBER published a minimum set of requirements (TS 103 645) aimed at the consumer IoT market. Now working on EN

4. Cyber security for critical infrastructures

Protecting critical infrastructure, through recent work items:

- ✓ TR 103 303 Protection measures for ICT in the context of Critical Infrastructure
- ✓ WI-024 Metrics for Identification of CI
- ✓ WI-037 Guidelines for increasing smart meter security



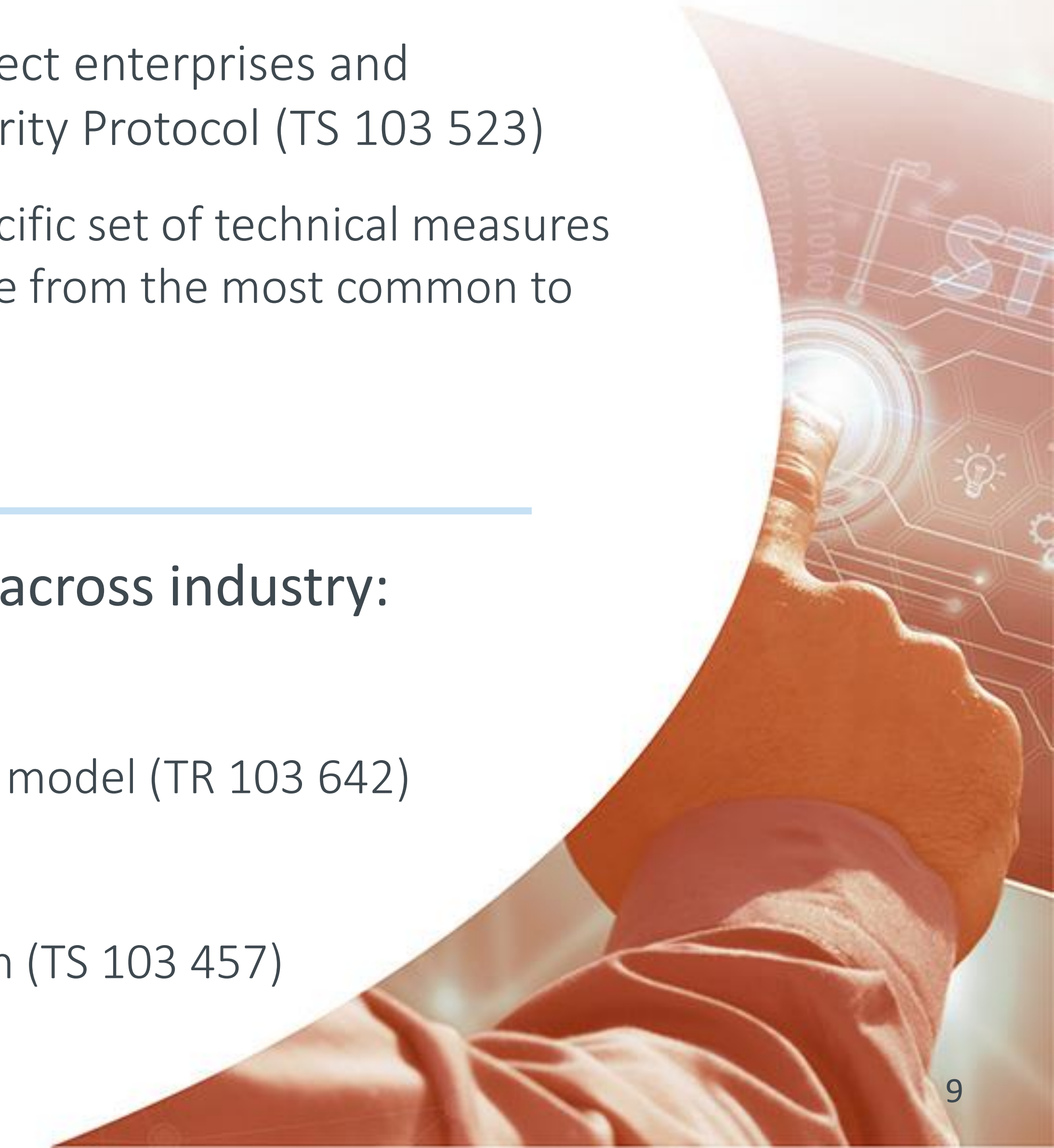
5. Enterprise and individual security

- Several standards developed or in development to protect enterprises and individuals from a range of attacks, the Middlebox Security Protocol (TS 103 523)
- Critical Security Controls (TR 103 305): Effective and specific set of technical measures available to detect, prevent, respond, and mitigate damage from the most common to the most advanced of those attacks

6. Cyber security tools

Cyber Security Tools – general techniques for use across industry:

- Threat Information Sharing (TR 103 331)
- Security techniques for protecting software in a white box model (TR 103 642)
- Attribute-Based Encryption (TS 103 458 & TS 103 532)
- Interface to offload sensitive functions to a trusted domain (TS 103 457)

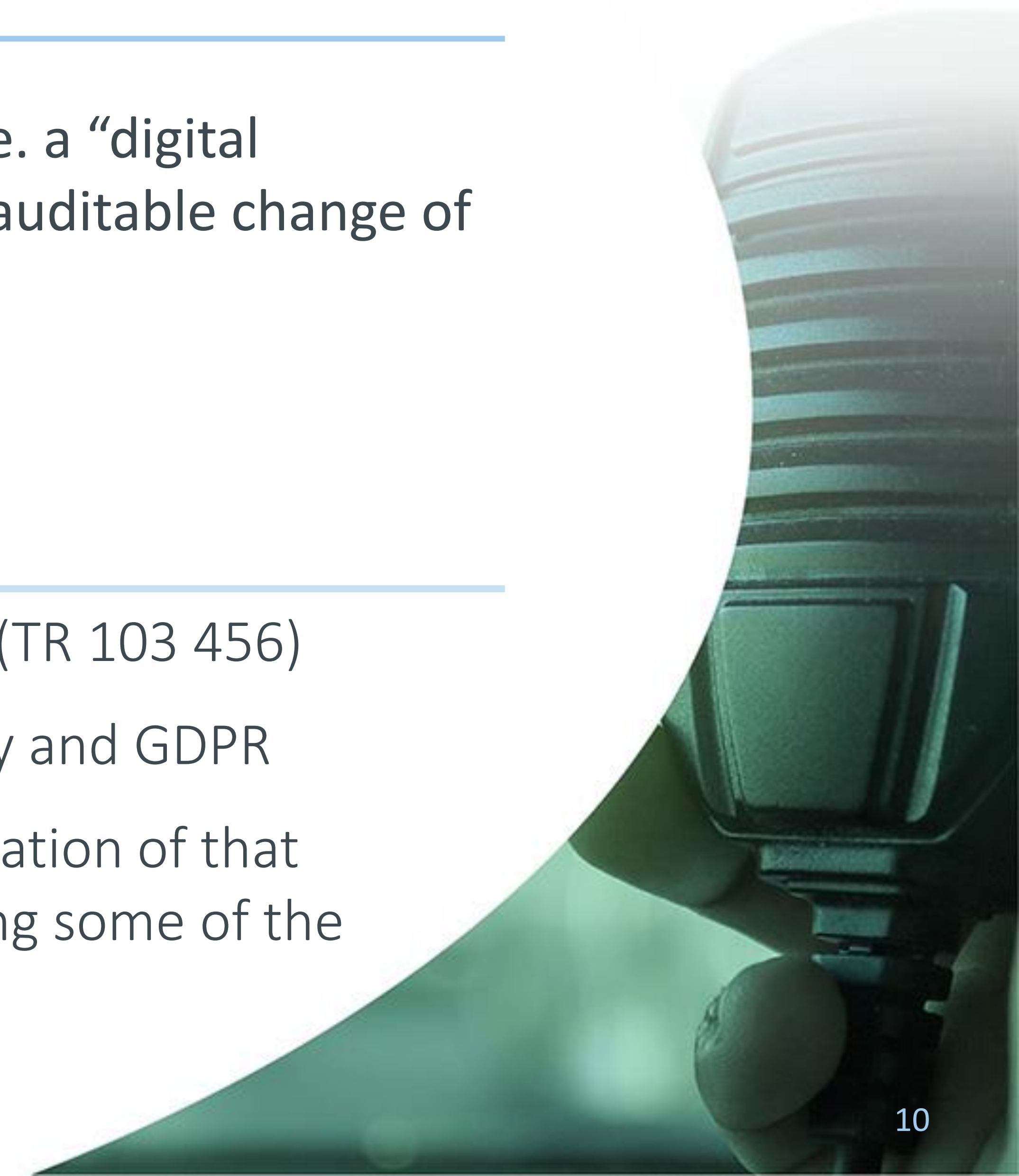


7. Forensic activities

Assuring of Digital Material for legal proceedings, i.e. a “digital evidence bag” covering cryptographic protections, auditable change of data - TS 103 643 Assuring Digital Material

8. Technical support to EU Legislation

- Guidance on implementing the NIS Directive (TR 103 456)
- TR 103 370 Guidance on standards for privacy and GDPR
- Mechanisms for privacy assurance and verification of that assurance (TS 103 485) can be used in meeting some of the obligations of GDPR



9. Quantum-Safe Cryptography working group

- Specialises in providing practical advice to industry on issues such as risk assessment, migration timelines, architecture and integration issues.
- Does not specify algorithms or key distribution techniques.
- Realistic quantum-safe options for important real-world applications such as code signing, transport security and VPNs should be endorsed by NIST and ETSI over the next few years.
- Launched in 2015, QSC became a TC CYBER working group in 2017
- Latest and ongoing work
  - Quantum-safe VPN TR
  - Hybrid key exchange TS

Why TC Cyber? How can I get involved with TC CYBER?

How to get involved with TC CYBER

Find TC CYBER on ETSI's website: www.etsi.org

TC CYBER:

- www.etsi.org/technologies-clusters/technologies/cyber-security

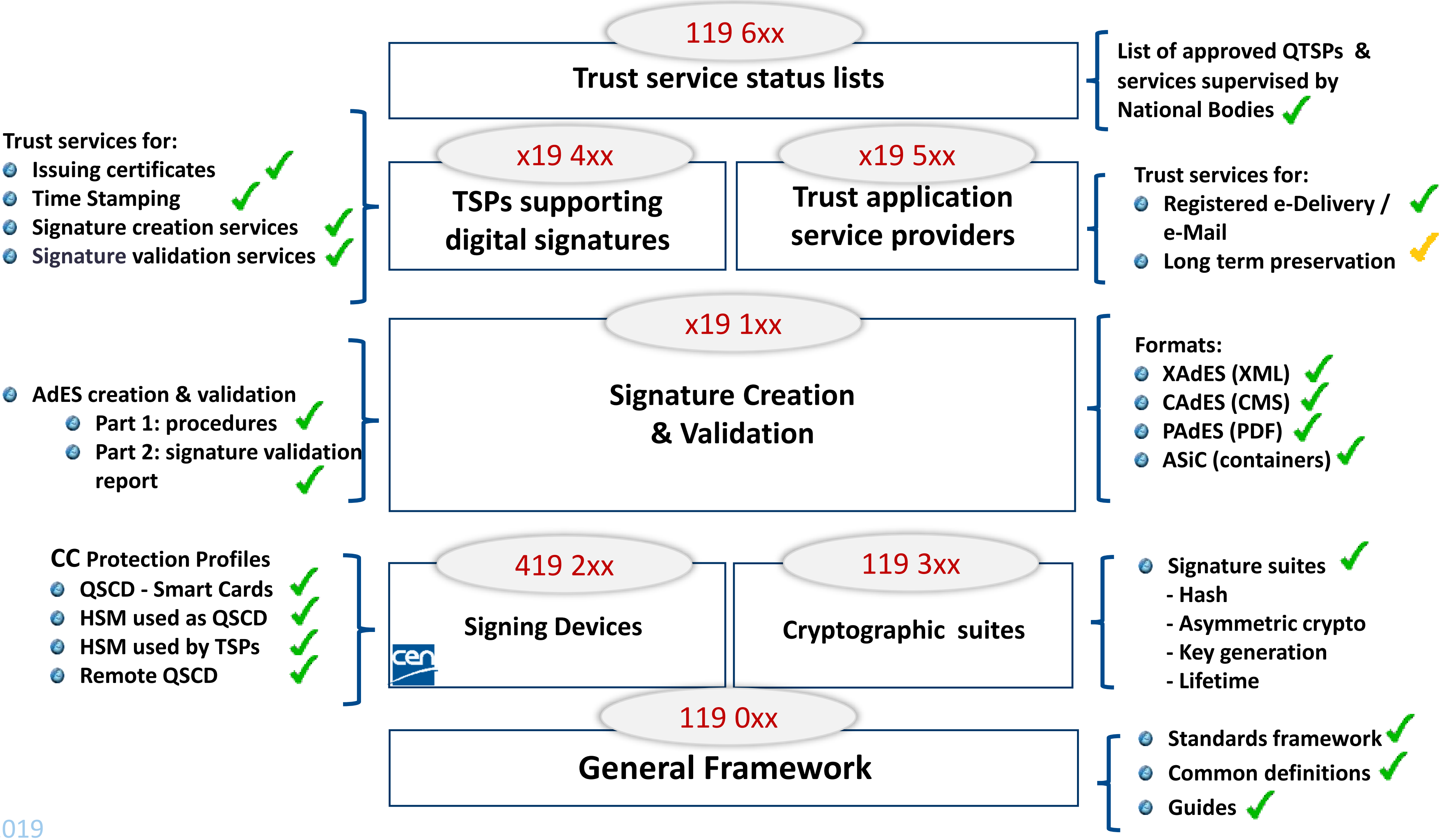
QSC:

- https://www.etsi.org/technologies-clusters/technologies/quantum-safe-cryptography

Next meetings:		
	QSC#13	9-10 June 2019
	CYBER#17	11-13 September 2019

TC ESI

eIDAS Standards Framework: Published Standards



119 6xx
Trust service status lists

List of approved QTSPs & services supervised by National Bodies ✓

Trust services for:
- Issuing certificates ✓
- Time Stamping ✓
- Signature creation services ✓
- Signature validation services ✓

x19 4xx
TSPs supporting digital signatures

x19 5xx
Trust application service providers

Trust services for:
- Registered e-Delivery / e-Mail ✓
- Long term preservation ✓

- AdES creation & validation
  - Part 1: procedures ✓
  - Part 2: signature validation report ✓

x19 1xx
Signature Creation & Validation

Formats:
- XAdES (XML) ✓
- CAdES (CMS) ✓
- PAdES (PDF) ✓
- ASiC (containers) ✓

CC Protection Profiles
- QSCD - Smart Cards ✓
- HSM used as QSCD ✓
- HSM used by TSPs ✓
- Remote QSCD ✓

419 2xx
Signing Devices

119 3xx
Cryptographic suites

- Signature suites ✓
  - Hash
  - Asymmetric crypto
  - Key generation
  - Lifetime

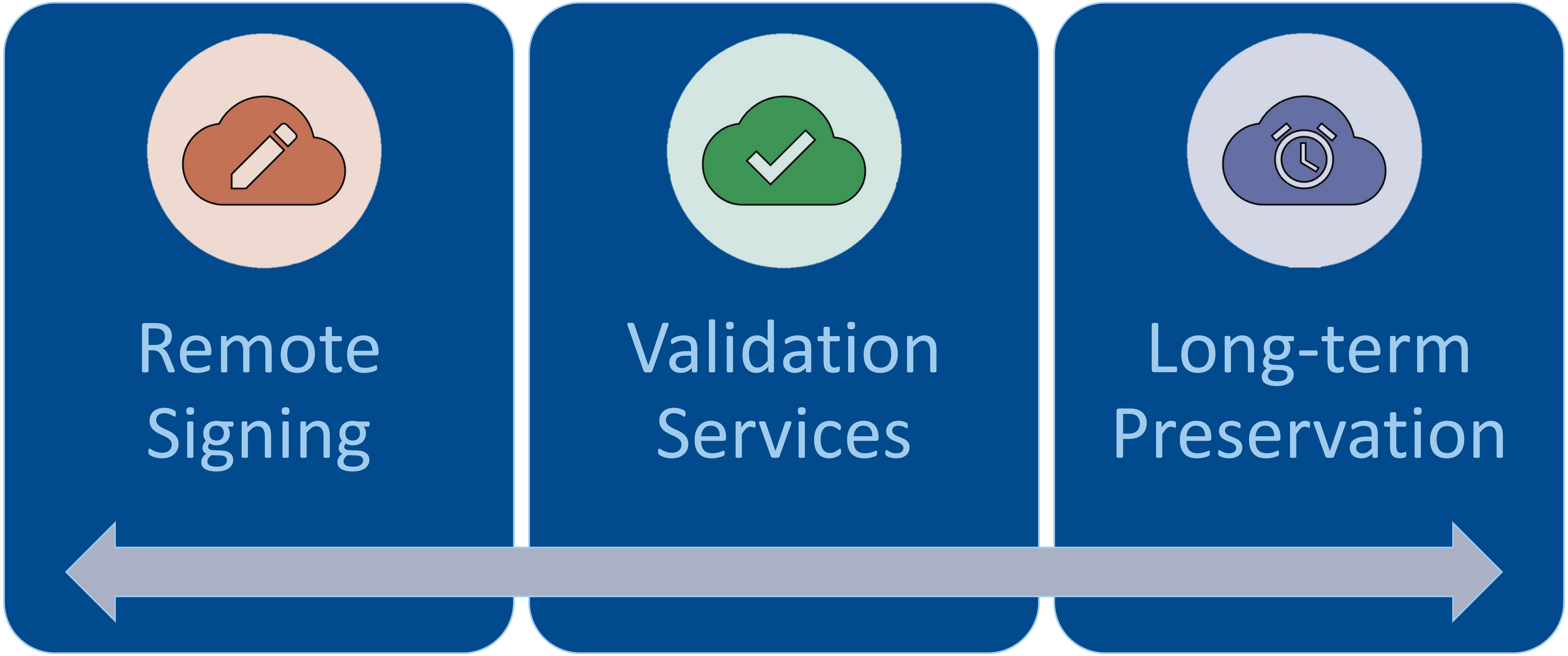
119 0xx
General Framework

- Standards framework ✓
- Common definitions ✓
- Guides ✓

Trust service issuing certificates

e-Signatures	• For use by natural persons
e-Seals	• For use by legal persons
Website authentication	• For websites

Signature Enhanced Trust Services

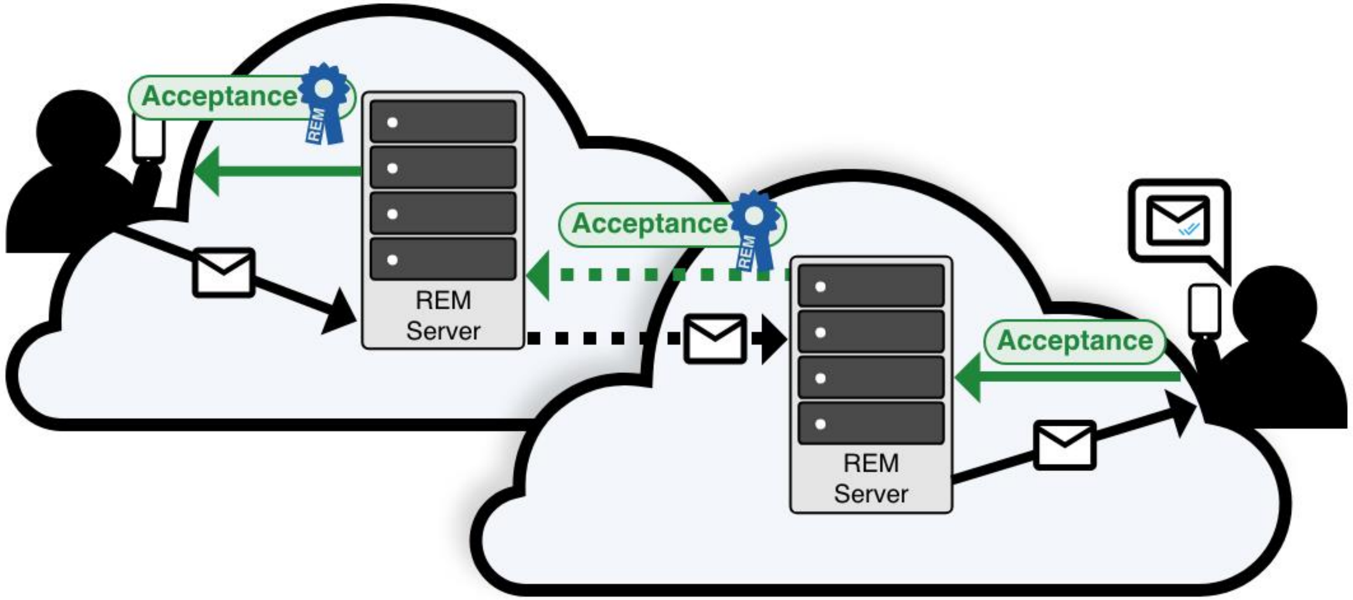


Remote Signing

Validation Services

Long-term Preservation

Electronic Registered Delivery (ERDS) and Registered Electronic Mail (REM)



Summary

CROSS-DOMAIN CYBERSECURITY

- **Ecosystem**
- **Protection of personal data & coms**
- **IoT security and privacy**
- **Critical infrastructures**
- **Enterprise and individual cybersecurity**
- **Forensics**
- Information Security Indicators

SECURING TECHNOLOGIES & SYSTEMS

- Mobile / wireless systems (5G, TETRA, DECT, RRS,RFID...)
- IoT
- Network functions virtualization
- Intelligent Transports
- Broadcasting
- Artificial Intelligence

Contact:
Sonia COMPANS
Technical Officer
sonia.compans@etsi.org

SECURITY TOOLS & TECHNIQUES

- Lawful interception & retained data
- **Digital signatures & trust services**
- Permissioned distributed ledgers
- Smart cards / secure elements
- Security algorithms
- Quantum key distribution
- **Quantum safe cryptography**

ETSI

The Standards People