The Standards People

Security Conference

Cybersecurity Standardization in ETSI

18 October 2023

Bringing people together at ETSI …

- ETSI is an Independent, non-profit organization
- More than 900 member organizations worldwide
- Drawn from over 60 countries and on five continents
- 30+ years track record of technical excellence in the ICT sector
- Strong community of experts and innovators
- Diverse community: SMEs, micro-enterprises, large companies, research entities, academia, government and public bodies, societal stakeholders
- Large and small member organizations

… in TC CYBER…

Technical Committee on Cybersecurity (TC CYBER)

- ETSI's Centre of Excellence for Cyber Security created in 2014
- Works on a range of problems – from device security to privacy, to network security, to cybersecurity tools and guides, with a Working Group on quantum-safe cryptography
- Works on both industry security challenges and security policies and legislation to address global cyber security problems

… and in many other groups…

3GPP SA3	Security of mobile networks
ISG NFV	Securing network function virtualization
TC ITS	Intelligent Transport Systems
ISG ETI	Encrypted Traffic Integration
TC SAI	Securing Artificial Intelligence
TC ESI	Digital signatures and trust services
TC SET	Smart cards and secure elements
ISG QKD	Quantum key distribution
TC LI	Lawful interception and retained data
ISG PDL	Permissioned Distributed Ledgers
ISG MEC	Muti-access Edge Computing

Cybersecurity Standardisation in ETSI

CROSS-DOMAIN CYBERSECURITY (TC CYBER)

- Cybersecurity ecosystem
- Protection of personal data & communications
- Consumer IoT security and privacy
- Security of critical infrastructures
- Enterprise and individual cybersecurity
- Forensics
- Cybersecurity tools and guides

SECURING TECHNOLOGIES & SYSTEMS

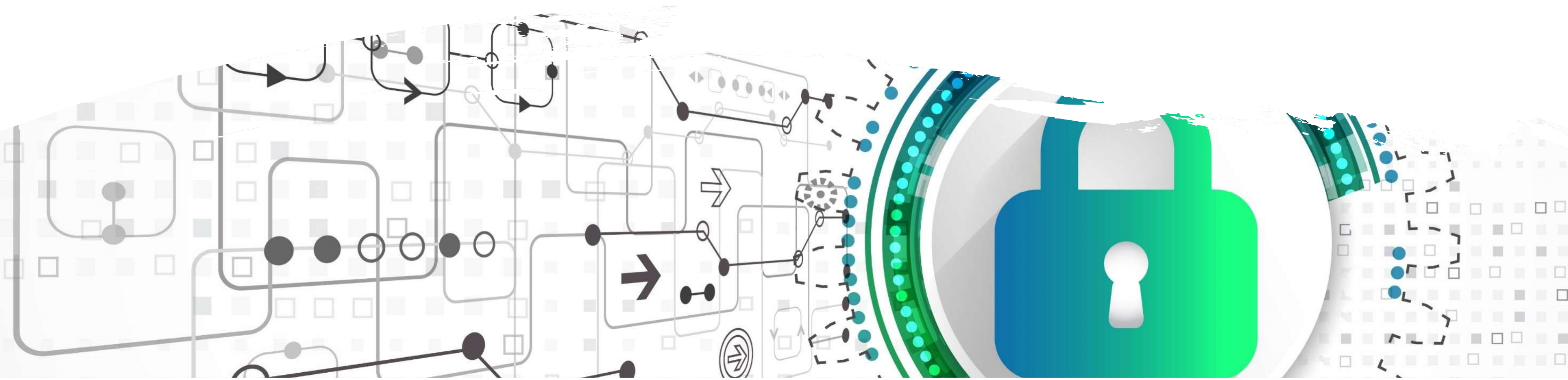
- Mobile / wireless systems (5G, TETRA, DECT, RRS, RFID…)
- Network functions virtualization
- Intelligent Transports Systems
- Broadcasting
- Artificial Intelligence
- IoT (oneM2M)

EVOLVING 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
- Encrypted Traffic Integration

TC CYBER

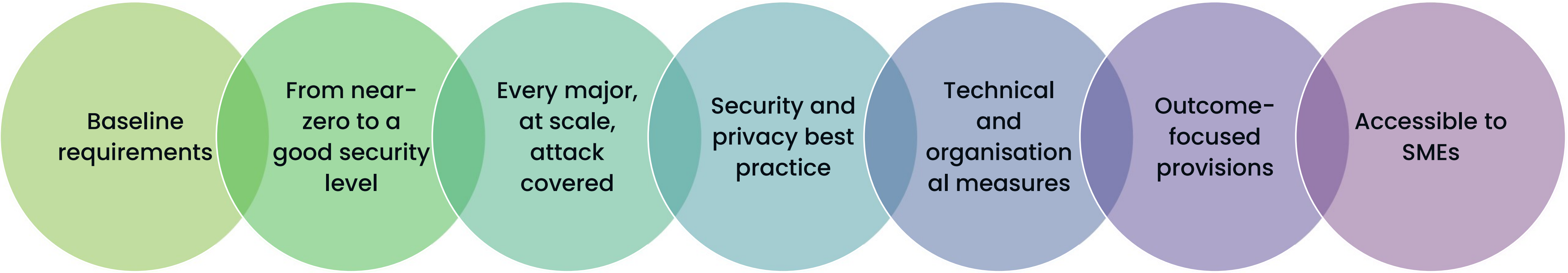
Cyber Security



TC CYBER Key areas of Work

- Cybersecurity ecosystem
- Protection of personal data and communication
- Cybersecurity for Critical Infrastructures
- Forensic activities
- Direct support to EU legislation
- Consumer IoT and Mobile Security and Privacy
- Network Security
- Enterprise/organization and individual cybersecurity
- Cybersecurity tools
- Quantum-Safe Cryptography

ETSI EN 303 645: “Cyber Security for Consumer Internet of Things: Baseline Requirements”



Baseline requirements

From near-zero to a good security level

Every major, at scale, attack covered

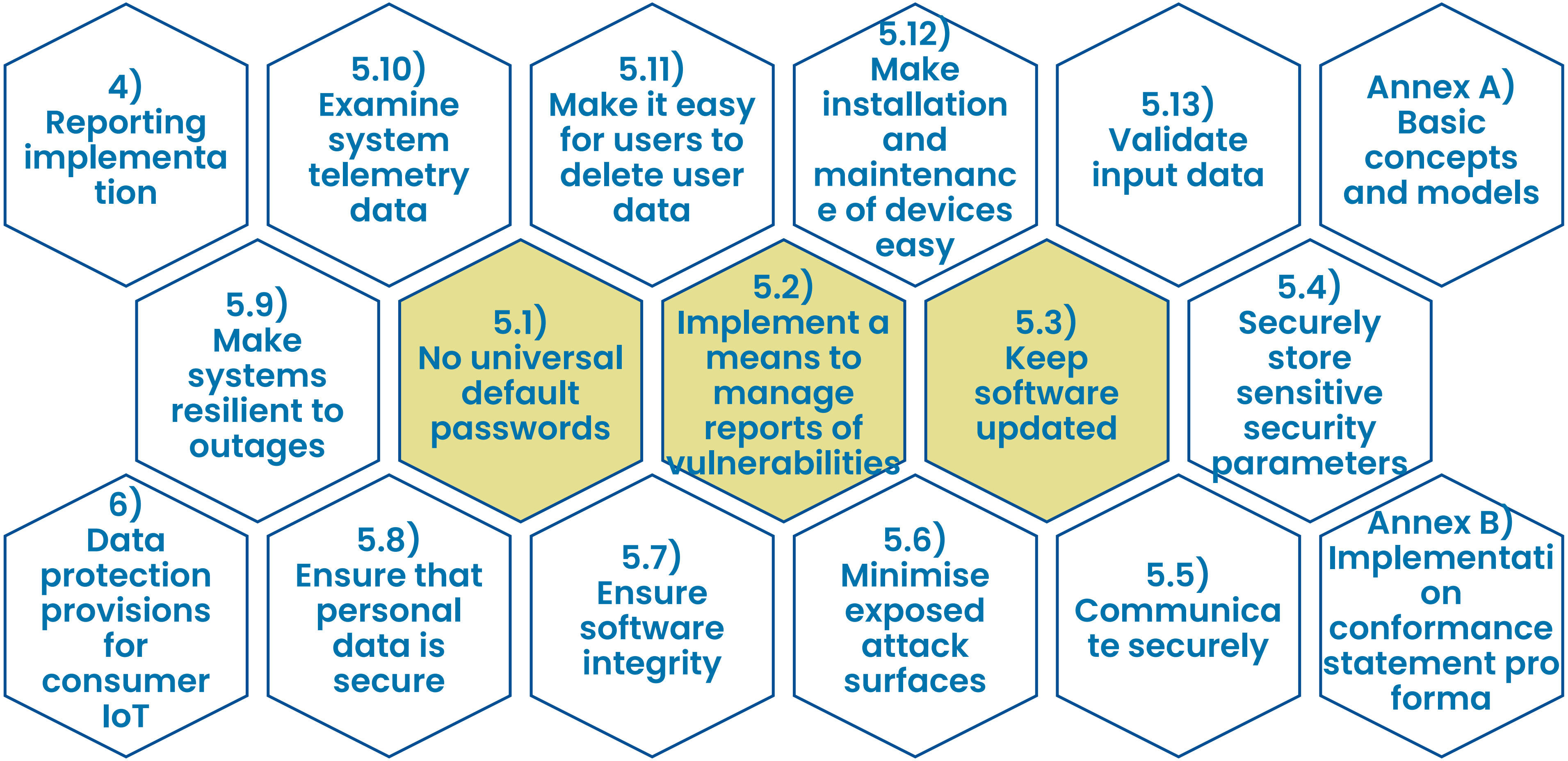
Security and privacy best practice

Technical and organisation al measures

Outcome-focused provisions

Accessible to SMEs

ETSI EN 303 645: Cyber Security for Consumer IoT



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 on conformance statement pro forma

Consumer Mobiler Device Protection Profile

- The CMDPP, developed in the TS 103 732 series, is a powerful tools to grant a common level of security in the consumer mobile devices.
- The CMDPP may become the reference for the mobile device cybersecurity baseline and used by other organisations.
- The CMDPP will be the first Protection Profile developed by ETSI certified against Common Criteria expanding the ETSI standards portfolio.

Protection of personal data and communications

ETSI is addressing the technical support to privacy legislation in the EU and beyond.

Technical guide to privacy addressing and cataloguing relevant standards globally ETSI TR 103 370 V1.1.1 (2019-01)

Attribute-Based Encryption ABE requirements ETSI TS 103 458 V1.1.1 (2018-06)

Mechanisms for privacy assurance and verification ETSI TS 103 485 V1.1.1 (2020-08)

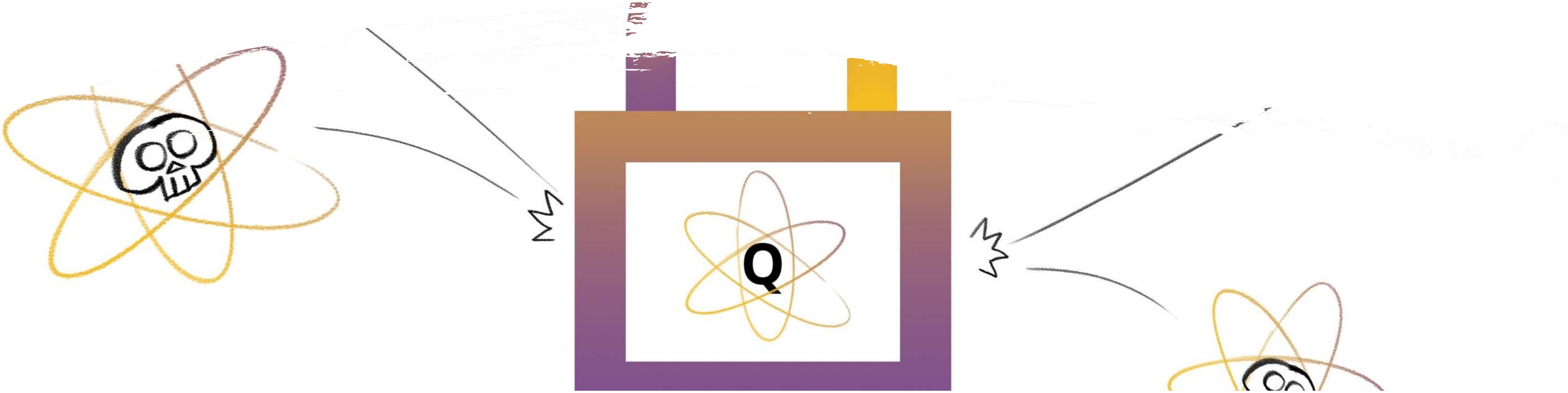
Ongoing work:

A Verifiable Credentials extension using Attribute-Based Encryption

Design practices against technology enabled coercive control

TC CYBER - WG QSC

Quantum-Safe Cryptography



Quantum-Safe Cryptography (QSC)

Launched in 2013 as a Workshop and as an Industry Specification group in 2015 to **study the potential impacts of Quantum Computing** in order to make recommendations on Quantum Safe Cryptography.

QSC became a working group of TC CYBER in 2017.

Specialises in providing **practical advice to industry** on issues such as risk assessment, migration timelines, architecture and integration issues.

Realistic quantum-safe options for important real-world applications such as VPNs, code signing, transport security…

(Does not specify algorithms or key distribution techniques)

Quantum-Safe Cryptography –
Publications

CYBER; Quantum-Safe Cryptography Migration for ITS and C-ITS, ETSI TR 103 949 V1.1.1 (2023-05)

CYBER; Quantum-Safe Key Exchanges, ETSI TR 103 507 V1.1.1 (2017-10)

Quantum-Safe Public Key Encryption and Key Encapsulation, ETSI TR 103 832 V1.1.2 (2021-09)

CYBER; Quantum-Safe Signatures, ETSI TR 103 616 V1.1.1 (2021-09)

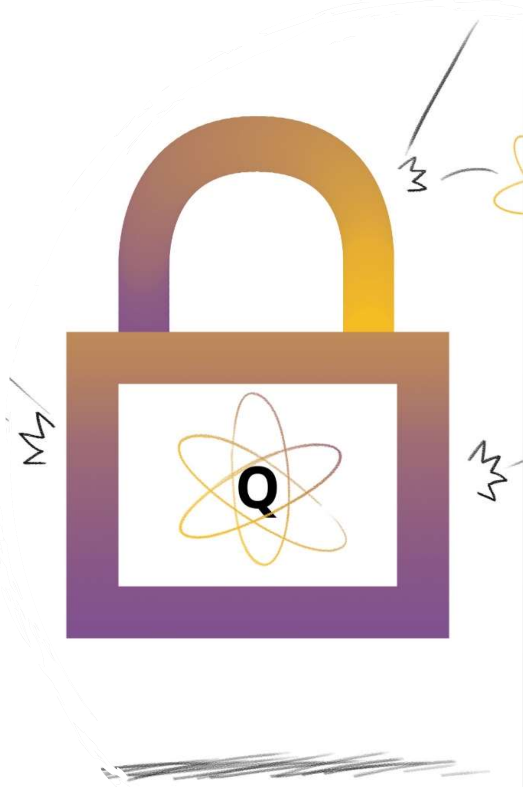
CYBER; Quantum-Safe Virtual Private Networks, ETSI TR 103 617 V1.1.1 (2018-09)

CYBER; Quantum-Safe Identity-Based Encryption, ETSI TR 103 618 V1.1.1 (2019-12)

CYBER; Migration strategies for Quantum Safe schemes, ETSI TR 103 619 V1.1.1 (2020-07)

State Management for stateful authentication mechanisms, ETSI TR 103 692 V1.1.1 (2021-11)

CYBER; Quantum-safe Hybrid Key Exchanges, ETSI TS 103 744 V1.1.1 (2020-12)



Quantum-Safe Cryptography – Ongoing Work

Current Work Items:

Deployment Considerations for Hybrid Schemes (TR)

Quantum-Safe Hybrid Key Exchanges (Revision of TS 103 744)

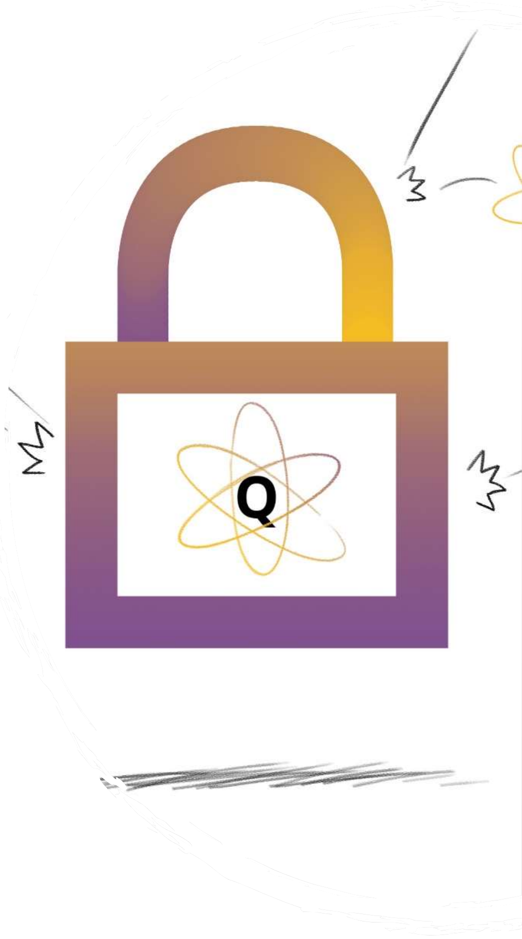
Impact of Quantum Computing on Cryptographic Security Proofs (TR)

Impact of Quantum Computing on Symmetric Cryptography (TR)

A Repeatable Framework for Quantum-safe Migrations (TR)

Efficient Quantum-Safe Hybrid Key Exchanges with Hidden Access Policies (TS)

QSC Protocol Inventory (TR)



TC ESI

Electronic signatures and trusted Infrastructures

TC ESI - Digital signatures and Trust Services Standards Framework

Trust Services (eIDAS)

Signature-enhanced Services

New Trust Services (eIDAS 2)

e-Attributes

e-Ledgers

e-Archiving

Signature creation & validation formats and procedures

Signing Devices

Crypto Suites

EU Digital Identity Wallet

TC ESI - Trust service issuing certificates

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

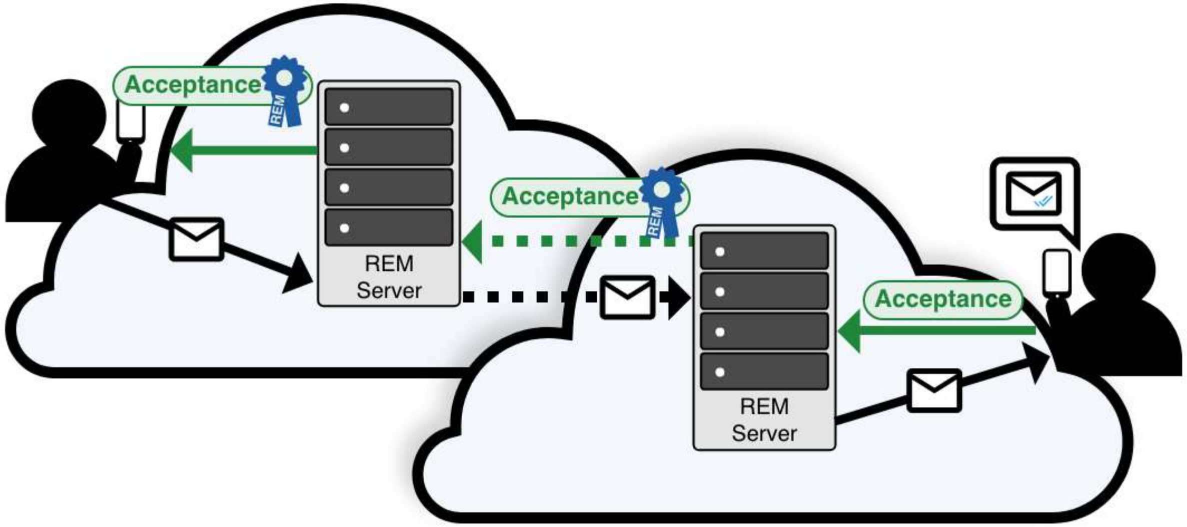
TC ESI - Signature Enhanced Trust Services

Remote Signing

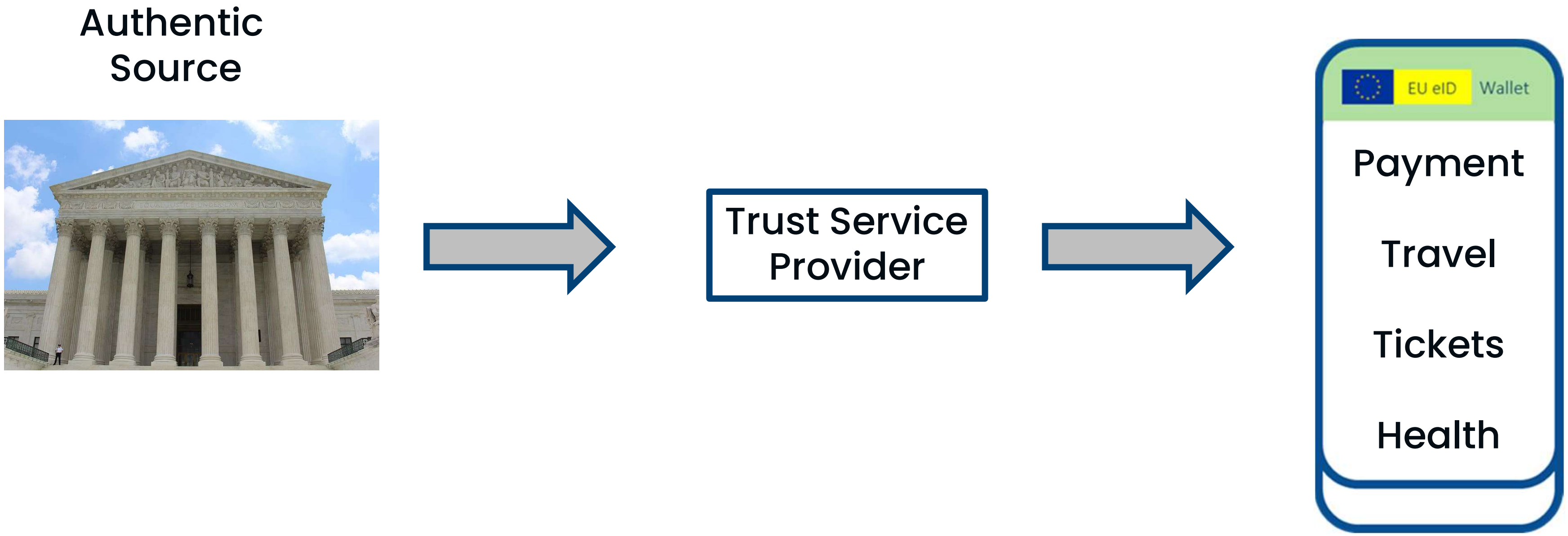
Validation Services

Long-term Preservation

TC ESI - Electronic Registered Delivery (ERDS) and Registered Electronic Mail (REM)



TC ESI - eIDAS2 Electronic Attribute Attestation



Authentic Source

Trust Service Provider

EU eID Wallet

Payment

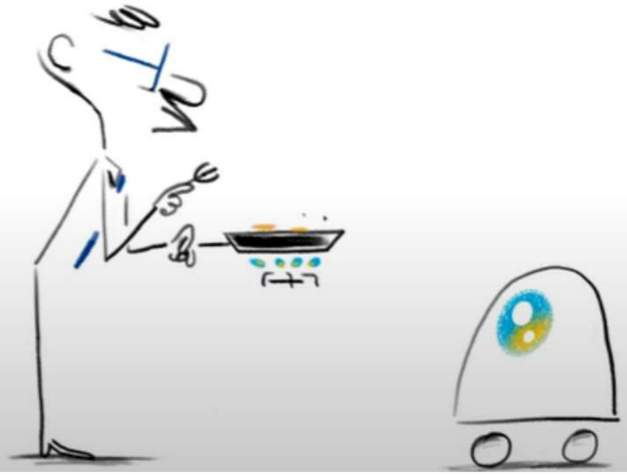
Travel

Tickets

Health

TC SAI

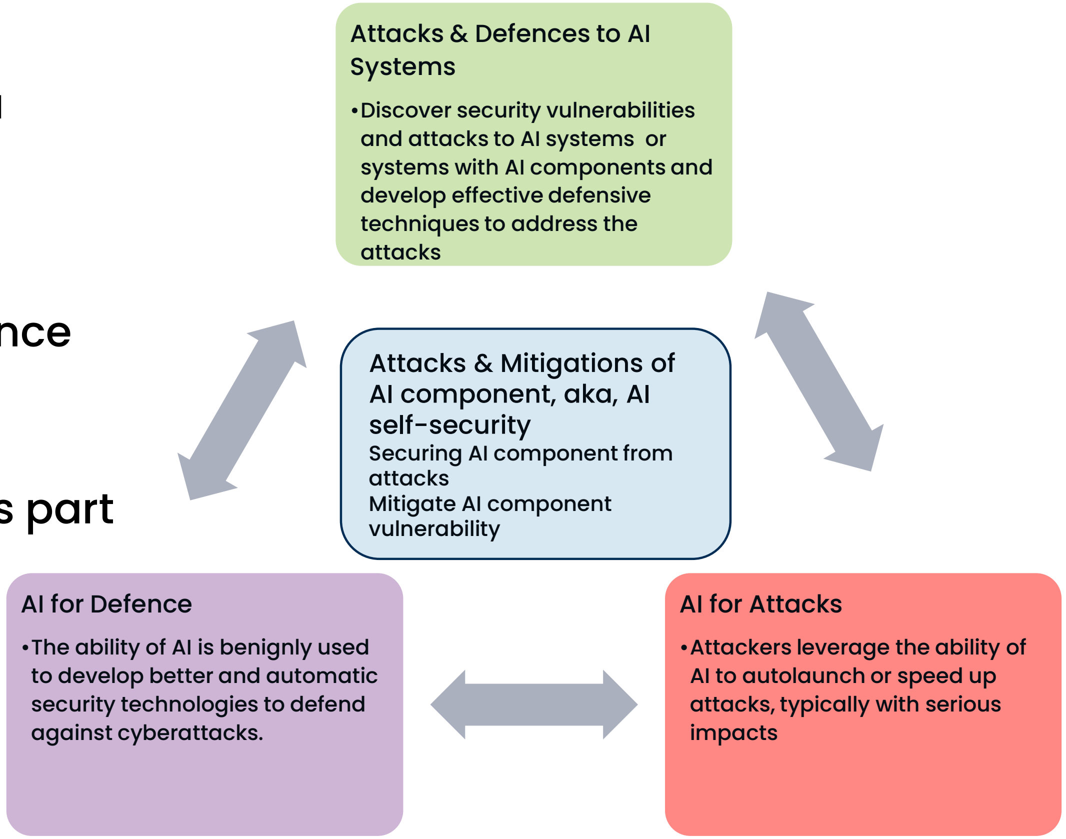
Securing Artificial Intelligence



ETSI TC* SAI Scope

1. Securing AI from attack e.g. where AI is a component in the system that needs defending.
2. Mitigating against AI e.g. where AI is the ‘problem’ (or used to improve and enhance other more conventional attack vectors)
3. Using AI to enhance security measures against attack from other things e.g. AI is part of the ‘solution’ (or used to improve and enhance more conventional countermeasures).

(*) ISG SAI is becoming a new TC SAI.



Attacks & Defences to AI Systems

- Discover security vulnerabilities and attacks to AI systems or systems with AI components and develop effective defensive techniques to address the attacks

Attacks & Mitigations of AI component, aka, AI self-security
Securing AI component from attacks
Mitigate AI component vulnerability

AI for Defence

- The ability of AI is benignly used to develop better and automatic security technologies to defend against cyberattacks.

AI for Attacks

- Attackers leverage the ability of AI to autolaunch or speed up attacks, typically with serious impacts

SAI Publications

Publications

- GR SAI 001 AI Threat Ontology
- GR SAI 002 Data Supply Chain Report
- GR SAI 004 Problem Statement
- GR SAI 005 Mitigation Strategy Report
- GR SAI 006 The Role of Hardware in Securing AI
- GR SAI 007 - Explicability and transparency of AI processing
- GR SAI 009 - Artificial Intelligence Computing Platform Security Architecture
- GR SAI 011 - Automated Manipulation of Multimedia Identity Representations
- GR SAI 013 - Proofs of Concepts Framework

SAI Ongoing work

Ongoing work

- WI3 - Security Testing of AI
- WI8 - Privacy aspects of AI/ML systems
- WI10 - Traceability of AI models
- WI12 - Collaborative Artificial Intelligence
- WI14 - Security aspects of using AI/ML techniques in the telecom sector
- WI15 - Artificial Intelligence Computing Platform Security Framework

ISG SAI will become a Technical Committee with its first meeting on 04 December 2023. Any ETSI member is welcome to join!

OneM2M Partnership

Security in onM2M

Security in oneM2M Release 2- Release 4

oneM2M
The IoT Standard

Device Configuration
TS-0022

Security Solutions
TS-0003

MEF & MAF interfaces
TS-0032

Enrolment services (RSPF / MEF)

Credentials Provisioning/Security Configuration of the M2M System

Secure communications services (SAEF / MAF)

Methods for Securing Information (PSK/PKI/Trusted Party)

Point-to-point and end-to-end solutions (TLS / DTLS)

Access Control & Authorization services

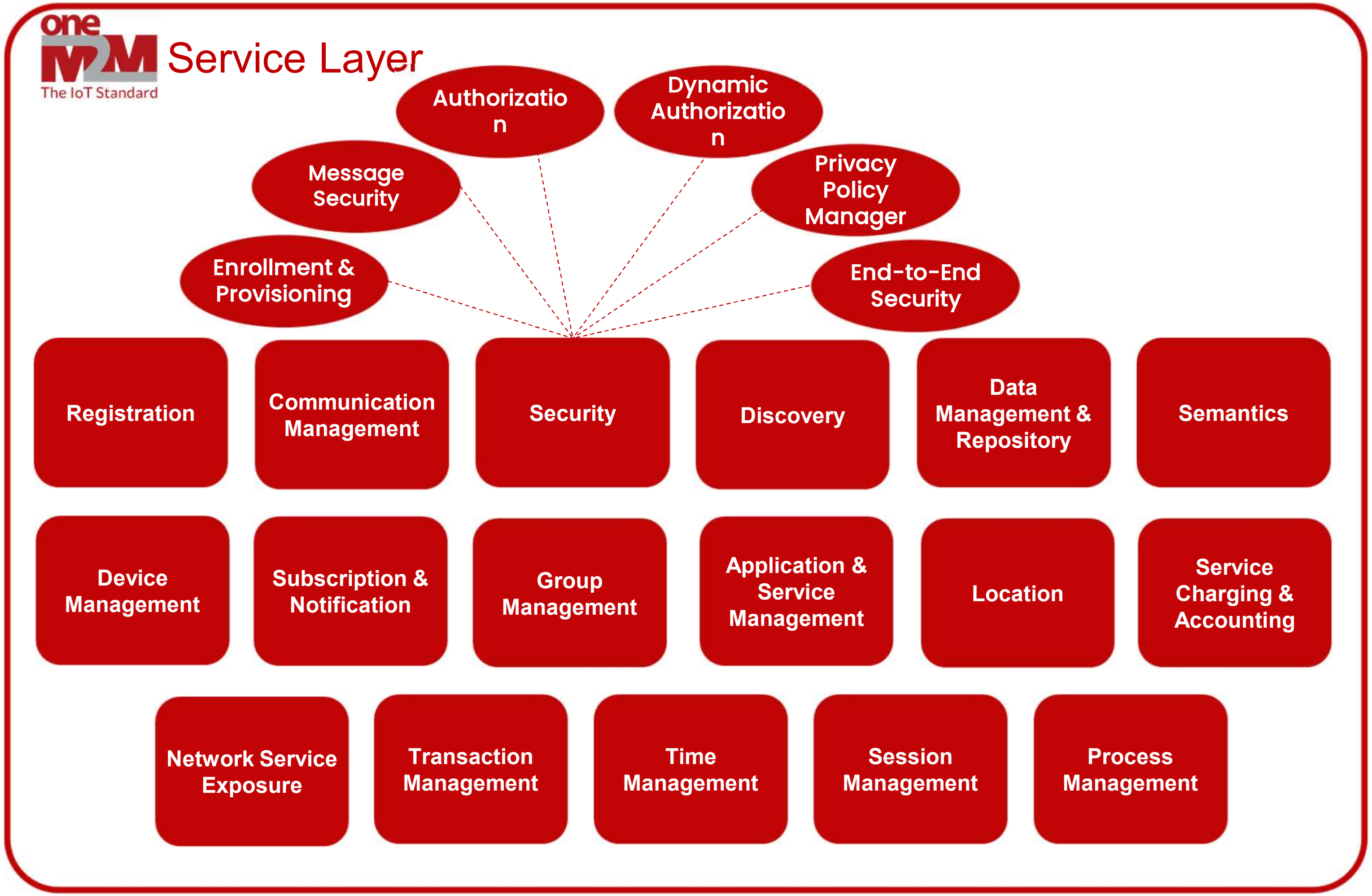
Requester Authentication

Information access Authorization(ACL based)

Static and Dynamic solutions

Privacy Policy Management

oneM2M Security Framework



oneM2M provides a common set of security capabilities to secure IoT devices and applications and prevent/ mitigate attacks

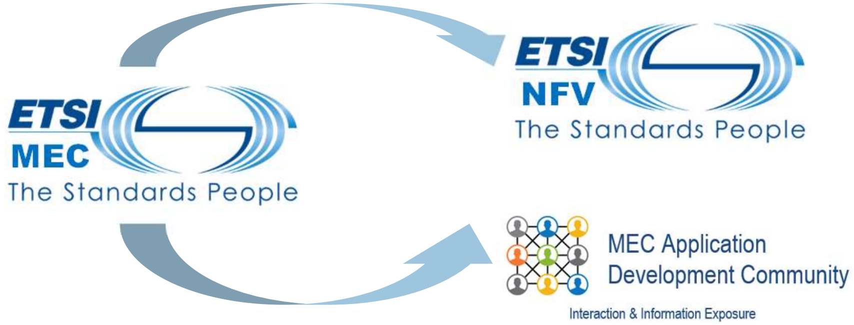
oneM2M exposes an abstracted set of security related APIs to help simplify security for IoT devices and applications

ISG MEC

Multi-access Edge Computing

ETSI MEC – What we do

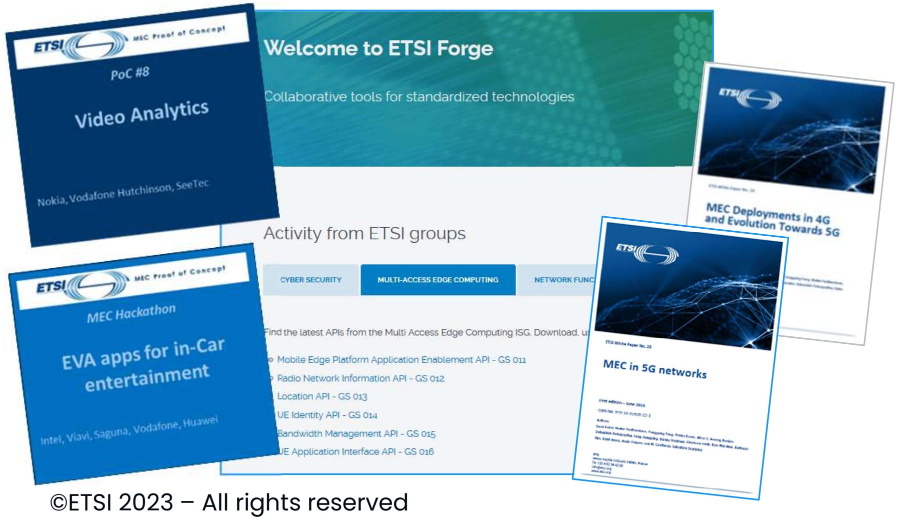
Foundation for Edge Computing created – Fully standardized solution to enable applications in distributed cloud created by ETSI MEC + 3GPP


ETSI MEC
The Standards People
ETSI NFV
The Standards People
MEC Application Development Community
Interaction & Information Exposure

Application Life Cycle Management

RESTful based APIs for Runtime Application Services

The number of MEC members increases regularly.



MEC Proof of Concept

PoC #8

Video Analytics

Nokia, Vodafone Hutchinson, SeeTec

Welcome to ETSI Forge

Collaborative tools for standardized technologies

Activity from ETSI groups

CYBER SECURITY | MULTI-ACCESS EDGE COMPUTING | NETWORK FUNC

Find the latest APIs from the Multi Access Edge Computing ISG. Download, u

- Mobile Edge Platform Application Enablement API - GS 011
- Radio Network Information API - GS 012
- Location API - GS 013
- UE Identity API - GS 014
- Bandwidth Management API - GS 015
- UE Application Interface API - GS 016

MEC Proof of Concept

MEC Hackathon

EVA apps for in-Car entertainment

Intel, Viavi, Saguna, Vodafone, Huawei

MEC Deployments in 4G and Evolution Towards 5G

MEC in 5G networks

126 members - Operators – Technology Vendors – IT players – Application developers

Hewlett Packard Enterprise
ATHONET
KDDI
MAVENIR
HUAWEI
intel
NOKIA
interdigital
ZTE
NEC
SAMSUNG
5GAA
NTT
中国移动 China Mobile
SoftBank
Qualcomm
vmware
Saguna
docomo
accenture
SK telecom
Telefonica
TIM
BOSCH
ETRI
iLink Digital
NPL
redhat
AT&T
verizon
ROGERS
LG
MITSUBISHI ELECTRIC
VOGO
China unicom中国联通
TNO
Rakuten
中国电信 CHINA TELECOM
OPENET
XFLOW RESEARCH
amdocs
DOLBY
Türk Telekom
IBM
radware
afnor
cnrs
ubiwhere
orange
MINISTERE DE L'INTERIEUR
Quortus
LEMKO
vodafone
EQUINIX
netrounds
Pgallery
SONY
flex
NEXTRA PARTNERS
Western Digital
KEYSIGHT TECHNOLOGIES
PT
UNIVERSITY OF SURREY
ITRI
ADLINK
FUTUREWEI
Silicom
IOTECC
CERAGON
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ
東京大学 THE UNIVERSITY OF TOKYO
RADCOM
ECI
THE ELASTIC NETWORK
CTTC
POLITECNICO DI TORINO
DELL
CAICT
EURECOM
COMMSCOPE now meets next
FSCOM
Accelleran
LEAR
tcs TATA CONSULTANCY SERVICES
SYNC TECHNO
MITRE
kpn
NEXTWORKS
ALTIOSTAR
cnit
JUNIPER NETWORKS
SCILD INNOVATIONS TELECOM FORESIGHT CONSULTING
Tech Mahindra
NIFE
ACS
ASTRI
VIAVI
UBiqube
CPLANE NETWORKS
Qwilt
ARTESYN
uc3m
PTS
AsiaInfo 亚信科技
STC
SES
LINKS
telenity
Akamai
nabstract.io
GSMA

MEC reference architecture

APIs

- Application Support
- Service Management
- Radio Network Information
- Location
- UE Identity
- Bandwidth Management
- Fixed Access Information
- WLAN Information
- V2X Information Service

- Application Package lifecycle and operation granting
- Device application interface

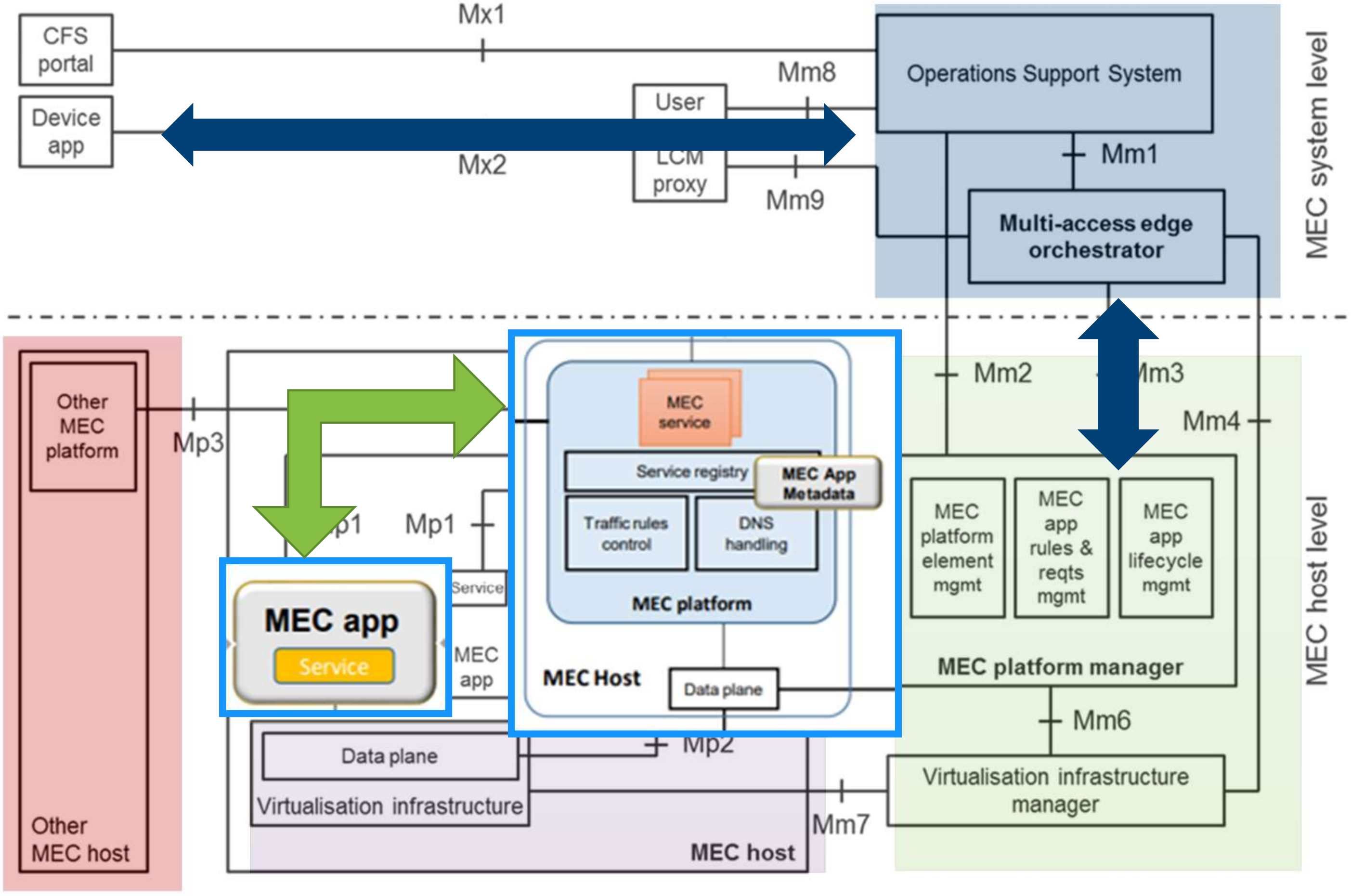


Figure 6-1: Multi-access edge system reference architecture

ETSI MEC – Foundation for Edge Computing

Application Enablement and Framework

Service definition framework and baseline platform services authorized applications.

- Registration, discovery and notification;
- Methodology for authentication and authorization of apps providing/consuming services;
- Communication support for services (query/response and notifications).

API Principles

Principles and guidance for developing and documenting APIs

- Developer-friendly approach to foster development
- ***Ensures that a consistent set of APIs*** are used by developers.
- Defines approach for authentication and authorization of apps providing/consuming services
- Based on TMF and OMA best practices

Specific service-related APIs

Standardized service-exposure APIs for key services that

- Expose network and context information
- Allow definition of localized, contextual services
- Support key use cases (e.g. enterprise, vehicular)
- Allow fine-grained edge traffic management

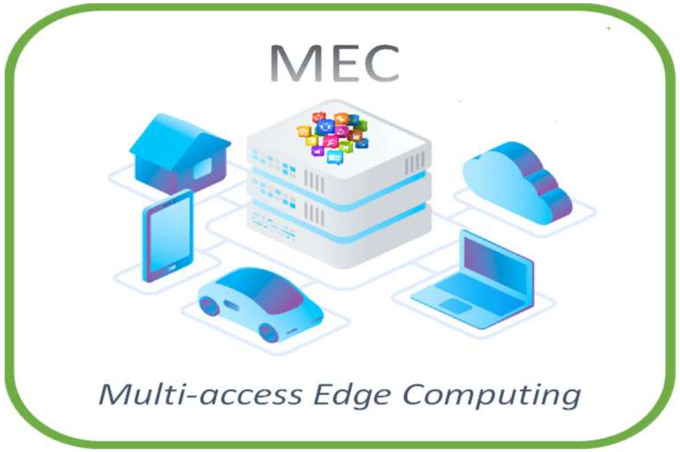
Management and Orchestration related APIs

Management of MEC hosts either as ***stand-alone*** entities or part of a larger ***NFV-managed*** framework

- Facilitate running of 3rd party application
- Enable deployment ***at the correct location at the right time***, based on technical and business parameters
- Integrate into telco operations systems, e.g. OSS

Enables a myriad of new use cases across multiple sectors as well as innovative business opportunities

MEC security

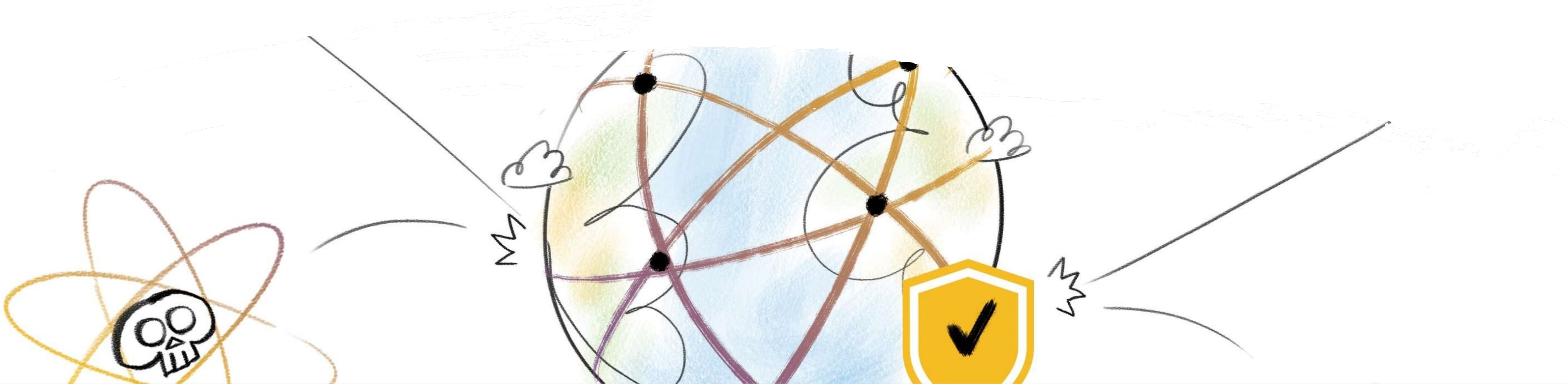


- **MEC scenarios** are characterized by a complex multi-vendor, multi-supplier, multi-set of equipment including both HW and SW devices. Given this overall level of **system heterogeneity**, areas of security, trust, and privacy are key topics for the edge environments.
- In that perspective, MEC stakeholders should pay attention to the vulnerability and integrity of any third-party elements, and a truly **end-to-end approach to MEC security** needs to consider not only the current standards in ETSI ISG MEC, but also the other available standards that can be applicable to the MEC environment.

- ETSI white paper, authored by many experts (in the domain of edge computing, security and involved in various standard bodies), provides an overview of **ETSI MEC standards** and current support for security, which is also complemented by a description of other relevant standards in the domain (e.g. **ETSI TC CYBER**, **ETSI ISG NFV**, **3GPP SA3**) and **cybersecurity regulation** potentially applicable to edge computing.
- GR MEC 041: a study on MEC Security topics and paradigms that apply to MEC deployments, will broadly cover the themes of application and platform security, Zero-Trust Networking, and security requirements for MEC Federations. If needed, normative work will be developed afterward.

ISG QKD

Quantum Key Distribution



About ISG QKD

An ISG is composed of ETSI Members and ISG Participants

- ETSI membership is not a requirement to participate in an ISG

QKD specifications require a broad range of expertise

- ISG QKD benefits from the expertise of Members and Participants from:
  - QKD vendors
  - Telecom operators
  - Application vendors
  - National Bodies and Certification Labs
  - National Metrology Institutes
  - Academic experts
- International profile: Europe, Japan, South Korea, Canada, US, etc.

Areas of activity of ETSI ISG QKD

Security

- Implementation security
- Evaluation activities
- Protocol security proofs
- Authentication

Interoperability

- Application / key delivery interfaces
- Interoperable KMS interface
- QKD in SDN networks
- Network architectures

Optical characterisation

- Optical components
- Complete QKD modules

Vocabulary

- Improving and aligning use of terminology

Any further questions?

Contact us:

cybersupport@etsi.org