SECURITY GROUPS @ETSI

CYBER

The rapid evolution and growth in the complexity of new systems and networks, coupled with the sophistication of changing threats, present demanding challenges for maintaining the security of ICT systems and networks. Security solutions must include a reliable and secure network infrastructure, but they must also protect the privacy of individuals and organizations. Security standardization, sometimes in support of legislative actions, has a key role to play in protecting the Internet and the communications and business it carries. We offer **market-driven cyber security standardization solutions**, along with advice and guidance to users, manufacturers, network, infrastructure and service operators and regulators.

ESI

Our work deals with **digital signatures and related trust services.** This activity covers the format of digital signatures, as well as procedures and policies for creation and validation. TC ESI also covers policy, security and technical requirements for trust service providers (TSP) such as certification authorities, time-stamping authorities, TSP providing remote signature creation or validation functions, registered e-delivery providers, and long-term data preservation providers. We address Trusted Lists that enhance the confidence of parties relying on certificates or other services related to digital signatures by indicating whether a given TSP was operating under the approval of any recognized scheme. Our work also aims at supporting the eIDAS Regulation as well as the general requirements of the international community to provide trust and confidence in electronic transactions.

PDL

We analyze and provide the foundations for the operation of **permissioned distributed ledgers**, with the ultimate purpose of creating an open ecosystem of industrial solutions to be deployed by different sectors, fostering the application of these technologies, and therefore contributing to consolidate the trust and dependability on information technologies supported by global, open telecommunications networks. While distributed ledgers are mostly known because of their use as cryptocurrencies, there are many other uses besides those, with examples such as the so-called smart contracts, support to digital identity attributes, object tracking, or the verification of service level agreements.

CYBER QSC

The emergence of quantum computing will present a serious challenge to current cryptographic techniques. Previously secure and encrypted information – such as bank account details, identity information and military data – will become subject to discovery and possible misuse. New 'quantum-safe' cryptographic techniques have emerged in recent years that provide protection against quantum threats. QSC's focus is on the **practical implementation of quantum safe primitives**, including performance considerations, implementation capabilities, protocols, benchmarking and practical architectural considerations for specific applications.

QKD

Our work enables digital keys to be shared privately without relying on computational complexity. The security offered by **Quantum Key Distribution** will not be vulnerable to future advances in algorithms, computational power or the emergence of a quantum computer. Important actors from science, industry and commerce address standardization issues in quantum cryptography and associated quantum technologies. The work is specifying QKD system interfaces, implementation security requirements and optical characterization of QKD systems and their components. We are contributing towards making QKD a robust deployable solution to protect next-generation telecommunications.

NFV

ISG NFV works on the **virtualisation of network functions.** NFV publications describe and specify virtualisation requirements, architecture framework, functional components and their interfaces, as well as the protocols and the APIs for these interfaces. ISG NFV also studies VNF performance, reliability, and resiliency matters, analyses the security challenges linked to virtualisation (trust, attestation, regulation).

SAI

The rapid expansion of Artificial Intelligence into new industries with new stakeholders, coupled with an evolving threat landscape, presents a tough challenge for security. The ETSI Industry Specification Group on **Securing Artificial Intelligence** (ISG SAI) focuses on three key areas: using AI to enhance security, mitigating against attacks that leverage AI, and securing AI itself from attack. The ETSI ISG SAI works alongside a landscape of huge growth in AI, creating standards to preserve and improve the security of Artificial Intelligence.

E4P

In the context of tracing persons potentially infected with a transmittable virus such as SARS-CoV-2, the ISG Europe for Privacy-Preserving Pandemic Protection (E4P) develops a framework and consistent set of specifications for proximity tracing systems, to enable the development of applications and platforms, and to facilitate international interoperability.

Such a standardization framework will enable developers to build interoperable mobile apps for proximity detection and anonymous identification and will allow the development of interoperable systems to automatically trace and inform potentially infected users in addition to manual notification methods, whilst preserving users' privacy and complying with relevant Data Protection regulation.

ETI

The Encrypted Traffic Integration group defines requirements and identifies the use cases of Encrypted Traffic Integration techniques to mitigate against threats to networks and users arising from the deployment of encrypted traffic. The underlying rationale for ISG ETI is that a paradigm of "encrypted by default" has been adopted by many network and service providers without taking due account of any threats to network resilience and security. The network management oversight that is accepted for non-encrypted traffic may be lost when an all encrypted paradigm is adopted.

3GPP SA3

3GPP^{TM} is a partnership project bringing together national Standards Development Organizations (SDOs) from around the globe initially to develop technical specifications for mobile telecommunications. SA WG3 is responsible for **security and privacy in 3GPP systems**, determining the security and privacy requirements, and specifying the security architectures and protocols. The WG also ensures the availability of cryptographic algorithms which need to be part of the specifications. The sub-WG SA3-LI provides the requirements and specifications for lawful interception in 3GPP systems.

SCP

We are responsible for the development and maintenance of specifications for **Secure Elements (SEs)** in a multi-application capable environment, the integration into such an environment, as well as the secure provisioning of services making use of SEs. Our work includes the development and maintenance of specifications for the SE and its interface to the outside world for use in telecommunication systems, for general telecommunication purposes as well as for Machine-to-Machine (M2M)/Internet of Things (IoT) communications. The work comprises the interface, procedures and protocol specifications between the SE and entities (remote or local) used in its management. It also includes interfaces, procedures and protocol specifications used between such entities for the secure provisioning and operation of services making use of the SE.

LI

We develop standards that support the technical requirements of national and international obligations for law enforcement, including the lawful interception and retention of the communications-related data of electronic communications. **Lawful Interception (LI) and Retained Data (RD)** play a crucial role in helping law enforcement agencies to investigate terrorism and serious criminal activities. We have pioneered the development and maintenance of LI and RD capabilities, and its standards are being adopted around the world due to the increased efficiency and lower cost resulting from their use. Global interest in the committee's work continues to grow, with new organizations joining in the standardization process.

oneM2M & SmartM2M

oneM2M is the global standards initiative that covers requirements, architecture, API specifications, **security solutions** and interoperability **for Machine-to-Machine and IoT** technologies. To accomodate the wide range of devices and deployment scenarios faced in the IoT, oneM2M provides considerable flexibility for the implementation of service layer security features: initial provisioning of security credentials, authentication infrastructures, confidentiality, integrity, authorization, access control services.

SmartM2M developed reports providing the standards landscape and best practices in **IoT privacy and security**, as well as teaching material for education on IoT security and privacy to ensure trust in IoT.

SAGE

The Security Algorithms Group of Experts (SAGE) is responsible for creating reports (containing confidential specifications), draft ETSI deliverables in the area of **cryptographic algorithms** and protocols specific to fraud prevention/unauthorized access to public/private telecommunications networks and user data privacy. The group's output includes algorithms for audiovisual services, 3GPP^{TM}, DECT^{TM}, GSM^{TM}, TETRA, GPRS and Universal Personal Telecommunications (UPT). Where appropriate, the group collaborates with other ETSI committees and with other organizations in order to ensure that the algorithms produced fully meet the needs of the technologies and services in which they are used.

ITS

We are responsible for standardization to support the development and implementation of **Intelligent Transport Systems (ITS)** service provision across the network, for transport networks, vehicles and transport users, including interface aspects, multiple modes of transport and interoperability between systems. ETSI TC ITS develops standards defining the security framework for cooperative ITS including a PKI. This security framework supports PKI trust model requirements from the EU C-ITS deployment platform and brings privacy protection mechanisms for users and drivers, e.g. using pseudonym certificates and regularly changing pseudonyms IDs in ITS G5 communications.

RRS

We are responsible for the standardization of **Reconfigurable Radio Systems** (RRS), including reconfigurable equipment architecture and Cognitive Radio. We define the security requirements for reconfigurable radio systems. They apply to the lifecycle of Radio Application Packages between a Radio application store and an RRS Reconfigurable Equipment.