

Introduction

The world has never been more connected than it is today. The Internet has become critical to our everyday lives, for businesses and individuals, and so too has its security. With our growing dependence on networked digital systems comes an increase in the variety and scale of threats and cyber attacks.

A variety in the protective methods used by countries or organizations can make it difficult to assess risk systematically and to ensure consistent, adequate security.

Therefore, standards have a key role to play in improving cyber security – protecting the Internet, its communications and the businesses that rely on it – and TC CYBER is the most security-focused technical committee in ETSI.

Roles & Activities

TC CYBER is recognized as a major trusted centre of expertise offering market-driven cyber security standardization solutions, advice and guidance to users, manufacturers, network, infrastructure and service operators and regulators. ETSI TC CYBER works closely with stakeholders to develop standards that increase privacy and security for organizations and citizens across Europe and worldwide. We provide standards that are applicable across different domains, for the security of infrastructures, devices, services, protocols, and to create security tools and techniques.

TC CYBER covers the following areas: cybersecurity ecosystem; protection of personal data and communication; IoT security and privacy; cybersecurity for critical infrastructures; enterprise/organization and individual cybersecurity; cybersecurity tools; forensic activities; support to EU legislations; and quantum-safe cryptography.

Some of our latest standards have been in network security (implementing the NIS Directive TR 103 456, the Middlebox Security Protocol TS 103 523 series, a survey of network gateways TR 103 421), cryptography for access control and personally identifying information (Attribute-Based Encryption TS 103 458 and TS 103 532), Critical Security Controls (the TR 103 305 series), protecting PII in line with GDPR (TR 103 370), Quantum-Safe Key Exchanges (TR 103 570), a survey of security techniques for protecting software in a white box model (TR 103 642), and the specification of an interface to offload sensitive functions to a trusted domain (TS 103 457).

The emergence of quantum computing will present a serious challenge to current cryptographic techniques. Previously secure encrypted information – such as bank account details, identity information and military security – will become subject to discovery and possible misuse. New ‘quantum-safe’ cryptographic techniques have emerged in recent years that provide protection against quantum threats. We are addressing these security issues and developing recommendations and specifications for the transition to quantum-safe Information and Communication Technology (ICT) applications through our Working Group on Quantum Safe Cryptography (QSC) within our TC CYBER. Our focus is on the practical implementation of quantum safe primitives, including performance considerations, implementation capabilities, protocols, benchmarking and practical architectural considerations for specific applications. Our objectives do not include the development of cryptographic primitives

In addition to TC CYBER, other ETSI groups also work on standards for cross-domain cybersecurity, the security of infrastructures, devices, services and protocols and security tools and techniques.

They address the following areas:

- Cross-domain cybersecurity
 - o Information Security Indicators
- Securing technologies and systems
 - o Mobile/Wireless systems (3G/4G, TETRA, DECT, RRS, RFID...)
 - o IoT and Machine-to-Machine (M2M)
 - o Network Functions Virtualisation
 - o Intelligent Transport Systems, Maritime
 - o Broadcasting
- Security tools and techniques
 - o Lawful Interception and Retained Data
 - o Digital Signatures and trust service providers
 - o Smart cards / Secure elements
 - o Exchangeable CA/DRM solutions
 - o Security algorithms

For further details on Cybersecurity please visit:

<http://www.etsi.org/cybersecurity>



Q4 2018

ETSI provides members with an open and inclusive environment to support the timely development, ratification and testing of globally applicable standards for ICT-enabled systems, applications and services across all sectors of industry and society. We are at the forefront of emerging technologies. We address the technical issues which will drive the economy of the future and improve life for the next generation. We are a not-for-profit body with more than 850 member organizations worldwide, drawn from 68 countries and five continents. Members comprise a diversified pool of large and small private companies, research entities, academia, government and public organizations. ETSI is one of only three bodies officially recognized by the EU as a European Standards Organization (ESO).

www.etsi.org

ETSI, 650 Route des Lucioles, 06921 Sophia Antipolis Cedex, France. Tel: +33 4 92 94 42 00 - info@etsi.org