Enjoy!
THE ETSI MAG

APRIL 2019

THE INTERVIEW
Colin Whorlow, NCSC - p.4-5

TECH HIGHLIGHTS
New Trust Services - p.10

CYBERSECURITY ROADMAP
ETSI Technical Committee CYBER - p.18-19

INTERNET SECURITY: DREAM OR REALITY?

ETSI

Editorial

> “Internet security is a topic that must involve all stakeholders.”

At this year’s Mobile World Congress, alongside 5G product demonstrations everywhere, security was the main discussion topic. So, is 5G secure? The answer is yes, 5G is by design more secure than previous generations, provided we ensure careful deployment and make sure that the applications running over these networks are also secure. This edition of Enjoy! should provide some insight on what ETSI, 3GPP and oneM2M are working on to make our systems “cybersecure”.

Our “In the spotlight” article showcases various cyber attacks and threats, data leakages, ransomware and human errors, to name a few. Also addressed in this issue are topics such as privacy, European regulations with eIDAS, the NIS directive, GDPR, the Cybersecurity Act and security for enterprises as well as for end users. Our use case on page 16 announces the first commercialised quantum-safe TLS testbed based on ETSI standards while our exclusive interviews with NCSC and Alastria highlight different angles of approaching security.

Eventually, the underlying message in most articles of this edition is that Internet security is a topic that must involve all stakeholders. The story of the ANSSI logo is a good example of this approach.

In February 2012, ANSSI, the French Agency for the Security of Information Systems published its new logo, stating in a cryptic sentence: “The curious will appreciate the background images”. Geeks started scrutinizing the logo and… it contained a security challenge! Security experts and researchers took up the challenge, decrypted the easiest pieces of the jigsaw and decided to create a dedicated website to exchange their ideas, their successes and failures. Then a fascinating journey began, worthy of a spy novel, where codes, ciphering, cryptography, and other methods are used to decipher the different layers and messages hidden within the logo.

This challenge, that led to a healthy competition amongst those who hadn’t given up, lasted for 2 years before someone unlocked the last mystery… The moral of the story? It took a whole community of experts with diverse backgrounds - hackers, researchers, security experts, etc. - to crack the enigma… And in ETSI we follow the same mantra: in order to make sure that we develop sound security standards, we encourage all stakeholders to participate in their development.

Enjoy reading!

Luis Jorge Romero,
ETSI’s Director General

Enjoy! The ETSI Mag

Edited and published by ETSI
Quarterly edition
Copyright ETSI 2019
Director of Publications: Nadja Rachow
Editor-in-Chief: Claire Boyer
Design: Le Principe de Stappler

Editorial office: ETSI,
650 route des Lucioles,
06560 Valbonne France
Tel.: +33 (0)4 92 94 43 35
enjoy@etsi.org

ETSI group on **BLOCKCHAIN:** come and join!

Officials of the recent Industry Specification Group on Permissioned Distributed Ledgers (ISG PDL) were elected during the kick-off meeting in January. Diego Lopez, Telefónica, was elected as the Chair of the group while Raymond Forbes, Huawei was elected as Vice Chair. The group will analyse and provide the foundations to operate permissioned distributed ledgers to be deployed across various industries and governmental institutions. ISG PDL will also ensure a common approach is taken by most blockchain actors. During the meeting, participants suggested work topics such as a gap analysis, applicability of permissioned distributed ledgers, compliance with data processing requirements and potential application scenarios. Want to join this exciting new activity? Contact ISGsupport@etsi.org.

SECURITY WEEK is coming!

ETSI has announced topics for its annual Security Week! The event will take place on 17-21 June 2019. This year will see continued debate on different aspects of cybersecurity. We will first set the scene with the cybersecurity landscape and policy action thread. The artificial intelligence thread will focus on the security angle to artificial intelligence (AI), following ETSI's AI Summit in April. And we'll discuss how security can keep pace with the rapid change of technology, networks and society. We will also host a Hackathon event on the new Middlebox security protocol standards and have ETSI explanatory sessions every day. These are half-hour sessions where you can learn about ETSI's latest work on hot security topics in depth. Register on our website.

Security Week
17-21 June 2019
ETSI, Sophia Antipolis, FR

INTEROPERABILITY EVENT on cross-border data exchange

ETSI is organizing the first Plugtests™ event on the interoperability of the Handover Interface between Law Enforcement Monitoring Facilities (LEMFs), on 1-5 July 2019 at ETSI in Sophia Antipolis, France. This event will focus on the cross-border data exchange for electronic evidence, based on the specification developed by the ETSI Committee in charge of Lawful Interception. This standard supports European Investigation Orders related to Lawful Interception and Retained Data. It will be the first time that vendors of Law Enforcement Monitoring Facilities get together to exchange data from different countries using ETSI standards to help them comply with the law.

ETSI summit on **ARTIFICIAL INTELLIGENCE**

This year's ETSI Summit reviews the current and future applications of Artificial Intelligence (AI) and identifies the potential challenges and opportunities of deploying AI at scale across the industry. The event seeks to separate the hype from the science and provide better understanding of Artificial Intelligence, Machine Learning and Deep Learning, as well as describing where AI is currently deployed using practical examples. The summit takes place on 4 April and there is still time to register. But if you missed it, go to our website for more information.

Interview
Colin Whorlow,
Head of International Standards at NCSC

In our exclusive interview Colin Whorlow explains why Government should be engaged in security standardization.

Colin Whorlow has worked in the UK National Cyber Security Centre (NCSC), and its predecessor CESG, for 20 years. He has spearheaded NCSC's active involvement in global security standards work including within ETSI and 3GPP. He convened the ETSI Quantum Safe Cryptography ISG, now a Working Group within the cybersecurity committee, and is a Programme Committee member for the annual ETSI/IQC Quantum-safe cryptography workshops. Colin is a member of the Management Board of ENISA and of the SOG-IS Management Committee. In previous roles Colin led CESG's engagement on EU and NATO information assurance issues, and he chaired the Information Security Technical Working Group at the Wassenaar (export control) Arrangement for some years. Colin's degree is in mathematics, which he studied at Oxford University.

Which technology do you find the most interesting in the context of security?

All new technologies are interesting but currently it is the possibilities and threats presented by quantum computers which are the most mindblowing. A viable large-scale quantum computer may be some years away, but we need to be getting ready for it now. Preparing for what will need to be a wholesale change of the algorithms used to secure the internet is both a mathematical and logistical challenge. NIST is leading on algorithm selection, and the ETSI QSC group addresses matters concerning transition and implementation. NCSC believes the answer to the quantum computing threat lies with mathematics.

The answer to the quantum computing threat lies with mathematics.

What is the role of a government body like NCSC in Standards Bodies?

NCSC was created to help protect the UK's critical services from cyber attacks, manage major incidents, and promote technological improvement and advice to citizens and organizations. Our public-facing role, including our work on standards, supports our mission to make the UK the safest place to live and do business online. Government can have important and unique roles in standards bodies – as a user with specific responsibilities, hence the Mission Critical work we have been doing in support of the UK Home Office in 3GPP; as a participant whose views are not influenced by commercial concerns; and as a body who can take a view of the entire ecosystem. NCSC is also a supplier of expertise, especially though not exclusively on encryption.

NCSC is a participant whose views are not influenced by commercial concerns.

How do you see ETSI helping in this area?

ETSI is an industry-led body, and NCSC's view is that industry-led bodies are the ones to engage in. If industry is putting resource into creating the standard, then it's because it intends to use it. We are not interested in helping develop standards for academic interest only! One focus for us has been the ETSI Technical Committee on Cybersecurity (TC CYBER), where we have been involved with creating standards on items as varied as Protection measures for ICT in the context of critical infrastructure, and quantum-safe identity-based encryption. More recently the ETSI committee has created a standard on cybersecurity for consumer Internet of Things, TS 103 645, and both we and another UK Department, DCMS, have contributed to this. The aim here is to give demonstrably useful security advice, and to reduce the burden on users by making technology easy to use securely.

If industry is putting resource into creating the standard, then it's because industry intends to use it.

Does NCSC engage in other standards bodies?

We have been active in 3GPP for a few years, primarily working on securing Mission Critical communications, but also now taking a wider interest in 5G security as a whole. The scale of 3GPP is enormous, and the level of expertise just in the security group, SA3, is staggering. All those involved, but particularly ETSI and their Mobile Competence Centre department supporting 3GPP, deserve enormous credit for enabling its continued effectiveness. We also contribute to the IETF, where our current focus is the launching of the new SMART Research Group – that's Stopping Malware And Researching Threats for those of you who enjoy "bacronyms"! One of my colleagues is co-chairing this group, and the aim is to ensure that cybersecurity is properly considered in protocol design. NCSC is also active in ISO, particularly in SC27 Working Group 3 which is where Common Criteria is being updated. As Government we are also involved with security work in the ITU, a very different environment from ETSI.

How do you see ETSI responding to the EU Cybersecurity Act?

The Cybersecurity Act brings ENISA and the European Standard Development Organizations, particularly ETSI, closer than ever before. It says that ENISA shall facilitate the establishment and take-up of European and international standards for risk management and for the security of ICT processes, products and services. This indicates a pathway whereby ENISA can identify requirements for cybersecurity standards; ETSI, through its cybersecurity committee, can create the standards; and then both ENISA and ETSI can promote them. As a member of the Management Board of ENISA I know that both organizations are keen for a closer relationship and are working towards it. As well as providing ENISA with a permanent mandate the other main plank of the CSA is the creation of an EU certification framework. The framework envisioned should have the global context very much in mind. Reducing fragmentation within the EU is valuable, but nowhere near as valuable as reducing global fragmentation. In this context ETSI is well-placed, being a global standards body, which just happens to be based in Europe.

Reducing fragmentation within the EU is valuable, but nowhere near as valuable as reducing global fragmentation.

■ *Colin Whorlow, Head of International Standards at UK National Cyber Security Centre (NCSC).*

Welcome to our NEW members

2pi-Labs GmbH, United States

2-Pi Labs takes your product idea from concept to working prototype and beyond. They do electronics design, embedded software development, product physical modelling, and prototyping with in-house 3D printers, electronic PCB assembly machines, CNC mills, lathes and other machine processes.

ACB Europe Ltd, United Kingdom

American Certification Body provides certification services for wireless equipment manufacturers. They are accredited to provide the widest scopes of Wireless Certification in the FCC's TCB, ISED FCB and EU CE Marking programmes, certifying the most challenging state-of-the-art products.

Alastria, Spain

Alastria is a semi-public, independent, permissioned and neutral Blockchain/DLT network. The consortium is open to organizations that wish to develop their own Blockchain/DLT strategy and distribute and organize products and services for the Spanish market.

AsiaInfo Technologies Inc, China

AsiaInfo is a provider of telecommunications software products and related services for telecom operators and other large enterprises. Their customers come from the world of broadcasting, postal and financial services industries and include China Mobile, China Unicom and China Telecom.

CANON CRF, France

CRF is the R&D Centre of Canon in Europe. They develop high-performance communication networks, high-quality data video processing and web protocols such as video surveillance, technologies to transmit high speed wireless data for video streaming, and compression on Internet.

Convida Wireless, United States

Convida Wireless is a joint venture created to combine Sony's consumer electronics expertise with InterDigital's pioneering Internet of Things (IoT) expertise and drive new research in IoT communication, 5G technologies and other connectivity areas.

Element Materials Technology, Netherlands

Element is a global provider of testing, inspection and certification services for a diverse range of materials and products in sectors such as global aerospace, fire and building products, infrastructure and environmental, transportation and oil and gas.

FH Campus Wien University, Austria

FH Campus Wien is a university of applied sciences. Students can choose from more than 60 bachelor's and master's degree programmes and master courses in the departments of Applied Life Sciences, Building and Design, Health Sciences, Nursing Science, Public Sector, Social Work and Engineering.

Landeskriminalamt Niedersachsen, Germany

The State Criminal Police Office of Lower Saxony is the central office to fight crime in Lower Saxony. As a service and service provider, it supports regional police departments in the field of security and the prosecution of criminal offences.

Matrixx, United States

MATRIXX provides a multi-patented Digital Commerce platform to serve the next-generation IT architectures capable of powering rapid transformation. Through innovations in engineering, product, sales and deployment, they empower Communications Service Providers with the speed, agility and autonomy they need.

NETO, France

NETO is a consulting firm which provides strategic advisory services to ICT companies. It is focused on regulatory, economic, and technical support, as well as business planning and market access in Europe and worldwide.

Newtec Cy NV, Netherlands

Newtec is specialized in designing, developing and manufacturing equipment and technologies for satellite communications. Newtec is dedicated to creating new possibilities for the broadcast, consumer and enterprise VSAT, government and defence, cellular backhaul and trunking and mobility, offshore and maritime markets.

Not for Radio LLC, United States

NFR is advancing the state of the art in software-defined network infrastructure by overcoming challenges in performance, complexity, and scale. Employing its unique expertise in hardware, software, and applied cryptography, the company delivers solutions via its own products as well as custom development.

Nordic Telecom Systems a.s., Czech Republic

Nordic Telecom Systems focuses on tailored solutions for critical communications. They have also operated a push-to-talk service (PTT) for customers in the fields of construction, engineering, industry, transport, taxi, courier services, forwarding, logistics, security, tourism and festivals.

Open Source Initiative, United States

The Open Source Initiative (OSI) is a non-profit corporation with global scope formed to educate about and advocate for the benefits of open source and to build bridges among different constituencies in the open source community.

P.I. WORKS, Turkey

P.I. Works offers AI-driven mobile network planning, management and optimization solutions. Their solutions enable Mobile Network Operators to accelerate 5G transformation and improve network quality. P.I. Works has deployed its solutions for more than 40 mobile network operators in 34 countries.

Polizia di Stato, Italy

The Polizia di Stato (State Police or P.S.) is one of the national police forces of Italy. Along with Carabinieri, it is the main police force for providing police duties. It is also responsible for highway patrol, railways, airports, customs, certain waterways, and assisting the local police forces.

Russian Quantum Center, Russia

The RQC conducts scientific research that could lead to a new class of technologies. These include safe data transmission networks, new materials, optical sub-micron transistors, high-frequency optical electronics, new systems for ultrasensitive imaging of the brain and accurate clocks for navigation systems.

SEFIRA, Czech Republic

SEFIRA specializes in services for the development, verification, and storage of electronic documents. They offer consulting on IT security and deliver solutions in the areas of electronic identity, authentication, public key infrastructure (PKI), and management identity. They provide system integration services.

SEMIC RF, Germany

SEMIC provides solutions in the field of high and ultra-high-frequency technology from DC to Terahertz (THz) range frequencies. It has diversified into the industrial and medical markets where it provides artificial intelligence (AI) based solutions to improve efficiency and accountability.

SpaceX, United States

SpaceX designs, manufactures and launches advanced rockets and spacecraft. The company was founded in 2002 to revolutionize space technology, with the ultimate goal of enabling people to live on other planets.

Security & Standards Associates, United Kingdom

The organization is a consultancy company offering advice in the financial, government and commercial sectors on the application of standards for security. Its Director has over 20 years' experience supporting customers on software and the use of cryptographic devices for security in the financial and government sectors across Europe.

Tallinn University of Technology, Estonia

TalTech is the only technological university in Estonia. It creates a synergy between different fields such as technological, natural, economic and health sciences to foster innovation. The university hosts more than 11,000 students from 94 different countries.

Valeo peiker acustic GmbH, Germany

Peiker acustic, part of Valeo group, manufactures components in communications technology for auto manufacturers, industrial firms, government agencies, and mobile phone manufacturers worldwide. Among other products, it offers passive components, electromechanics, acoustics, active components, cables, printed circuit boards, metal parts, plastics, and connectors.

Voipfuture, Germany

Voipfuture develops technology for monitoring and analysing media quality in IP networks – to control and evaluate network performance and the quality of Voice over IP services. The monitoring solution covers all standard VoIP services. It easily integrates into existing IT infrastructures with off-the-shelf server hardware.

Interview Julio Faura,

Chairman of Alastria

Blockchain is a technology that people discovered via Bitcoin; the Chairman of Alastria explains why it goes beyond that and impacts many sectors.

Julio Faura is one of the most prominent leaders in the application of blockchain technology for enterprises and institutions. During his decade-long term at Santander, he led R&D and Innovation for the Group, founded Santander's Blockchain Lab and led Santander's activities around crypto-currencies and distributed ledgers for years. He co-founded collaborative industry initiatives in the space such as the Enterprise Ethereum Alliance (which he chaired), Ripple's GPSG, the USC consortium, and Alastria. In July 2018 he became a full time entrepreneur and founded Adhara, a funded startup that builds international payments, fx and liquidity management technology based on smart contracts over permissioned blockchain networks.

Blockchain has been in the air for a few years now; why did you decide to create Alastria?

After years of exploration of the possibilities of blockchain technology and particularly smart contracts, we realized that it was challenging to use the existing public blockchain networks for enterprise purposes due to their cost, the lack of governance or regulation, the lack of tools to ensure privacy and confidentiality, and their remarkably low performance. We then decided to create a regulated version of the public Ethereum network, leveraging the increasingly mature, enterprise-grade versions of the technology that we have today. Such a network would be permissioned, would have enterprise-grade performance and functionality, and would provide proper digital identification of all participants, so the applications they deploy and execute can be legally binding and can conform to existing regulatory frameworks.

Alastria brings a shared digital realm on top of which very different actors can collaborate and transact.

Alastria is a platform for multiple sectors but what exactly do you bring to the ecosystem?

Alastria intends to provide "just" the underlying smart-contract-enabled blockchain network and digital identity framework for members to develop, deploy and execute distributed applications – be it by themselves or in collaboration with other members from their sector or from different sectors. The key value it brings is a shared digital realm on top of which very different actors can collaborate and transact, including financial and non-financial companies, specialized startups, services firms, government and public institutions, and academia. It also seeks to identify collaborative, multi-sectorial applications that can benefit from this technology, and tries to foster collaboration between members to develop them.

In your opinion, what are the sectors that will benefit the most from this technology in the coming years?

Arguably the financial sector was the first to spot the possibilities of this technology and is probably the one farthest along exploring its practical applications, in particular on payments, liquidity management, and issuance and trading of digital assets in the capital markets. But many other sectors are beginning to see its benefits, including different industrial sectors (related to supply chain management and provenance tracking), healthcare or insurance, as well as governments and public bodies. But what is really exciting is to think about the cross-sectorial possibilities of all this, e.g. by mixing tokenized electronic money with non-financial digital assets over smart contracts. The possibilities are endless.

You said earlier that blockchain needed to address specific requirements and regulations; is this compliant with a standardized solution?

The short answer is no, and we are still early in the process of promoting the necessary standards. First of all we do need better standardization of enterprise blockchain technology, so the basic requirements of performance, security, privacy and interoperability are clear and universally accepted – this is what the Enterprise Ethereum Alliance is working hard on, and mostly includes a good set of technical issues. But then we need standards at a higher level, e.g. for the issuance and management of digital assets (e.g. tokenized electronic money or digital capital market instruments) or for creating digital identity with smart contracts. These last standards need to be designed to comply with existing regulatory frameworks so we can make sure they can be used in the real economy. And these regulatory frameworks tend to be national or regional at most, which makes this effort a non-trivial one – yet achievable, thanks to the simplicity and the universal nature of the underlying, smart-contract-enabled blockchain solution.

The financial sector is the first to benefit from blockchain.

Alastria joined the new Permissioned Distributed Ledgers group in ETSI; why?

While we believe that Alastria is a very innovative initiative, in fact the only one of its kind, we also see that it is the first time that such a wide array of such different actors is working together to implement a permissioned blockchain network that serves as a sort of public infrastructure that is to be governed through a previously inexistent, innovative, decentralized model. It this context, ETSI seems the perfect venue to table and discuss the issues we are encountering, with the objective of setting the standards we need globally to fix them. And at the same time we believe that Alastria can contribute as well to the discussions in the working group, in particular sharing our experience in aspects such as network topology, permissioning mechanisms, and digital identity.

ETSI seems the perfect venue to table and discuss the issues we are encountering.

When should we expect the market to implement a unified solution for blockchain?

In my personal opinion, blockchain and – more generally – distributed ledger technologies are still in their infancy, and so it is difficult to think about unification of standards and consolidation at this point. There are also significant misconceptions about what blockchain really is and what its distinctive features are, in particular in the context of commercial firms offering solutions that are not truly decentralized and do not offer a single, shared ledger where smart contracts can be deployed and executed in a truly decentralized way. I think winners are already emerging in relation to the (very) different approaches being proposed, but we still need to see significant evolution in all of them in terms of performance, privacy and governance before thinking about unification or market consolidation. Establishing some of the standards for some of these aspects will certainly help in the process.

New Trust Services
helping in the fight against fraud

Standards for new types of "Trust Services" provide an important toolset to counter growing Internet fraud.

The Internet is becoming the essential medium for business and government, and every year there is more and more fraud being reported, with cybercrime costing the global economy $600 billion in 2017. An important tool for protecting against such crime is to use third party trust services to support the security of data exchanged. Work in ETSI started around the year 2000 with standards for the use of digital signature techniques, based on Public Key Infrastructures, to ensure the authenticity of a document. Now, with the publication of Regulation 910/2014 on electronic identification and trust services (commonly called eIDAS), the work of the ETSI Committee in charge of Electronic Signatures and Trust Infrastructures (TC ESI) includes a whole new set of trust infrastructures which can be used to counter fraud targeting online business and government.

General features of the new generation of trust infrastructures

All the trust services addressed by ESI depend on third party trust infrastructures which assist transacting parties in securing the data they exchange. ETSI provides an essential assurance of the trust services through a generic audit framework, ETSI EN 319 403, with best practice standards for each type of trust service.

Secure website access and payment services

In line with the eIDAS regulation, ETSI-based trust infrastructures have been about securing access to websites following internationally accepted guidelines. For payment services, working with the European Banking Authority and Open Banking Europe, ETSI has adapted its standards for trust infrastructures to meet the needs of new payment services in its standard ETSI TS 119 495.

Registered e-Delivery/e-Mail

ETSI has produced a set of standards which extends e-Delivery or e-Mail services to provide secure and reliable delivery of electronic messages between parties with proof of the delivery process giving legally accepted accountability.

Cloud-Based Signatures

Newly published ETSI specifications TS 119 431 part 1, TS 119 431 part 2 and TS 119 432 support the creation of electronic signatures in the cloud, facilitating electronic signatures by avoiding the need for specialized user software and secure devices.

Other recent standards for cloud-based support for electronic signatures include specifications for signature validation and signature preservation.

■ *Nick Pope, ETSI's TC ESI Vice Chair*

"The Economic Impact of Cybercrime- No Slowing Down" (PDF). McAfee. 2018. Retrieved October 24, 2018

Information Security Indicators:
specifications implemented in Europe

The 9-specification ETSI GS ISI-00x series addresses the full scope of the main security incidents and behavioural vulnerabilities.

The core and most important specification ETSI GS ISI-001 part 1 and 2 provide a full set of 98 operational indicators for organizations to use to benchmark their security posture. Based on these, seven other specifications have been developed. We can highlight GS ISI-004, which addresses only events detected through technical means, and only security incidents (of a malicious nature) and behavioural vulnerabilities, excluding software, configuration and general security vulnerabilities, simpler to detect with well-identified and well-established methods and tools. The specification GS ISI-005 proposes a way to produce security events and to test the effectiveness of existing detection capabilities while GS ISI-007 provides a set of requirements to build and operate a secure SOC (Security Operations Centre).

The strength of these specifications lies in the fact that they are already widely implemented in industry and organizations and have proven effective for various reasons:

- Providing a far more accurate knowledge of both threats and vulnerabilities through detailed state-of-the-art data regarding the main types of security events (building up future advanced threat intelligence).
- Reconciling top-down (security governance) and bottom-up (IT ground operations) approaches, through clear event detection objectives.

- Bringing new information to make a decision on the best trade-offs between IT security prevention and security event detection and response.
- Developing a way to bring more automation to ISI indicators.
- Providing a model to build and operate a secured SOC positioned at the heart of a whole enterprise-wide cyberdefence approach.

These contributions are decisive milestones towards a truly professional and more mature “Dymanic IT security”, beyond risk management and information security management systems.

At the 1st edition of a workshop on Cybersecurity and Data Protection standards in support of European policy in Brussels on 19 September 2017, ETSI specification GS ISI-001 was considered as key regarding information security indicators and associated metrics.

More recently, the ETSI Information Security Indicators Industry Specification Group was mentioned at the EU Certification Framework Conference in Brussels on 1 March 2018 as one of the four ETSI standards in cybersecurity which could help implement the new certification framework, the EU Cybersecurity Act.

Finally, these specifications are key to implementing the Network and Information Security (NIS) Directive in Europe.

■ *Gérard Gaudin, ETSI's ISI ISG Chair*

Cybersecurity
for consumer IoT

The ETSI Technical Committee on Cybersecurity has just released ETSI TS 103 645, a standard for cybersecurity in the Internet of Things, to establish a security baseline for Internet-connected consumer products and provide a basis for future IoT certification schemes.

People entrust their personal data to an increasing number of online devices and services. In addition, products and appliances that have traditionally been offline are now becoming connected. Poorly secured products threaten consumers' privacy and some devices are exploited to launch large-scale DDoS (Distributed Denial of Service) cyber attacks.

ETSI's new specification, TS 103 645, addresses this issue and specifies high-level provisions for the security of Internet-connected consumer devices and their associated services. IoT products include connected children's toys and baby monitors, connected safety-relevant products such as smoke detectors and door locks, smart cameras, TVs and speakers, wearable health trackers, connected home automation and alarm systems, connected appliances (e.g. washing machines, fridges) and smart home assistants.

Secure privacy and ID
management

The ETSI committee on cybersecurity has completed the first of 3 documents addressing the technical provisions that reinforce privacy and identity management. ETSI TR 103 370, entitled "Practical introductory guide to Technical Standards for Privacy", guides developers on the core principles for achieving privacy protection and identifies technical standards. When implemented in products and services, it will provide most of the technical protections of user privacy. Specification TS 103 485, "Mechanisms for privacy assurance and verification", is expected to be finalized for publication in late Q1-2019. TS 103 485 specifically addresses the use of sets of functional capabilities from the Common Criteria in the technical provisions for privacy protection. Finally, TS 103 486, "Identity management and naming schema protection mechanisms", is in development for finalization and publication in Q2-2019, specifying Obligation of Trust frameworks that are to be used to build trusted networks for sharing of identity.

Standard to secure
sensitive virtual functions

ETSI has released specification ETSI TS 103 457, which tackles the challenge of secure storage – where organizations want to protect customer data whilst still using a cloud that is not under their direct control. Many organizations need to protect this data, but when it is held in a virtual network or cloud, the organization often doesn't have control of this storage solution.

TS 103 457 solves this problem, by standardizing an interface between a "secure vault" that is trusted and a cloud that could be anywhere, where such sensitive data is stored in the vault. This allows a sensitive function to exist in a lower security environment, with data held securely.

This interface can be used with new network function virtualization (NFV) technology to allow secure authentication of users for billing purposes. Virtualization means that processing can happen anywhere and might be untrusted, therefore these secure vaults are needed to protect sensitive functions and data.

INTERNET SECURITY: DREAM OR REALITY?

The development of computers began in the 1950s and the first message was sent on the internet in 1969. 50 years ago, security was not a priority. Data which later transited via the world wide web had nothing to do with the amount of data generated today. The number of connected devices is becoming paramount.

Many technology areas are potentially concerned by cybersecurity attacks: 5G, Internet of Things, automated vehicles, intelligent transport systems, health care, supply chain, utilities, to name a few. Challenges keep coming up as the creativity of cyber criminals seems limitless but solutions to prevent many attacks exist and have already been identified by European and global security experts, including those participating in ETSI groups.

"In the spotlight" tells you more about it and the use case on page 16 introduces a member's new agile quantum-safe TLS Testbed based on ETSI VPN work. So keep reading!

Internet Security: Dream or Reality?

The history of the Internet began with the development of computers in the 1950s. The initial concept of wide area networking originated in several computer science laboratories in the United States, the United Kingdom, and France. At the time, security was a concern but not a priority; today, in the worldwide digital ecosystem, security is paramount.

The beginning of the Internet

The U.S. Department of Defense awarded contracts as early as the 1960s, including for the ARPANET project, directed by Robert Taylor and managed by Lawrence Roberts. The first message was sent over the ARPANET in 1969 from computer science Professor Leonard Kleinrock's laboratory at the University of California, Los Angeles (UCLA) to the second network node at Stanford Research Institute (SRI). Fifty years ago, security was a concern but not a priority, as the impact of poor security at that early time was limited.

Today, the fourth industrial revolution will lead to a total digital worldwide ecosystem. At the same time, humanity will face climate and digital changes. These things do not exist in isolation: the emergence of huge data centres and cloud computing infrastructure will have a significant impact on climate change, which will require more technology to master energy savings and achieve a safe Internet.

A fully interconnected world

Digital transition will result in a highly connected world in multiple ways: optical fibre, 5G networks, Bluetooth, NFC (Near Field Communication), Wifi, Li-fi (Light Fidelity), etc. The number of connected devices is also on the rise. Many technology areas are potentially concerned: 5G, Internet of Things, automated vehicles, intelligent transport systems, health care, supply chain, utilities, etc.

There is no escaping it!

There are multiple threats to defend against (see table) and the creativity of attackers has no limits

Large scale attacks

Data leakages
- The firm Exactis leaked 2 terabytes of personal data, 340 million records (06/2018).

Ransomware
- WannaCry in 2017; major companies affected: Vodafone, Fedex, Deutsche Bahn, etc.

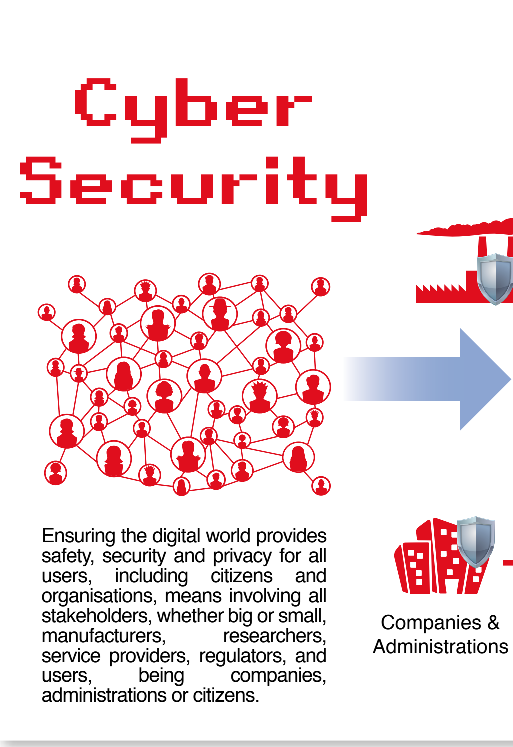
Human errors
- The personal data of 14 million Verizon customers was not protected (12/2017).

Software bug
- Eurocontrol sky control management software: more than 36,000 flights affected (4/2018).

Major challenges in security…

Cybercrime is a fast-growing and continuously changing type of crime. Therefore, security measures must be continually adapted in a permanent technology evolution. For example, smart cards used in banking have constantly improved their technology, and fraud is now at an acceptable level of 0.034% on a total market of 600 billion Euros. This has been possible through constant improvement of technology based on evolving risk analysis. Criminals are increasingly exploiting the speed, convenience and anonymity of the Internet to commit a variety of illicit activities which know no borders, either physical or virtual, cause serious harm and pose real threats to victims worldwide. As security affects all of us today, all stakeholders and relevant experts need to be involved to secure current networks, which are more and more virtualized, while considering future evolutions. Quantum computers are part of ICT future technology and working on quantum safe cryptography is essential. This is one of ETSI's areas of work.

> Improving security will improve resilience and awareness.



Ensuring the digital world provides safety, security and privacy for all users, including citizens and organisations, means involving all stakeholders, whether big or small, manufacturers, researchers, service providers, regulators, and users, being companies, administrations or citizens.

...Involving all stakeholders

The cybersecurity landscape is manifold with "securing people", "secured people" and regulators.

"Securing people" includes companies delivering security products, solutions and services. These companies have strong expertise in development, the current risk landscape and how to manage it.

The "secured people" comprise the users of security: from small and medium enterprises (using the Internet connection, providing e-services) to citizens (e-commerce, e-administration) and municipalities.

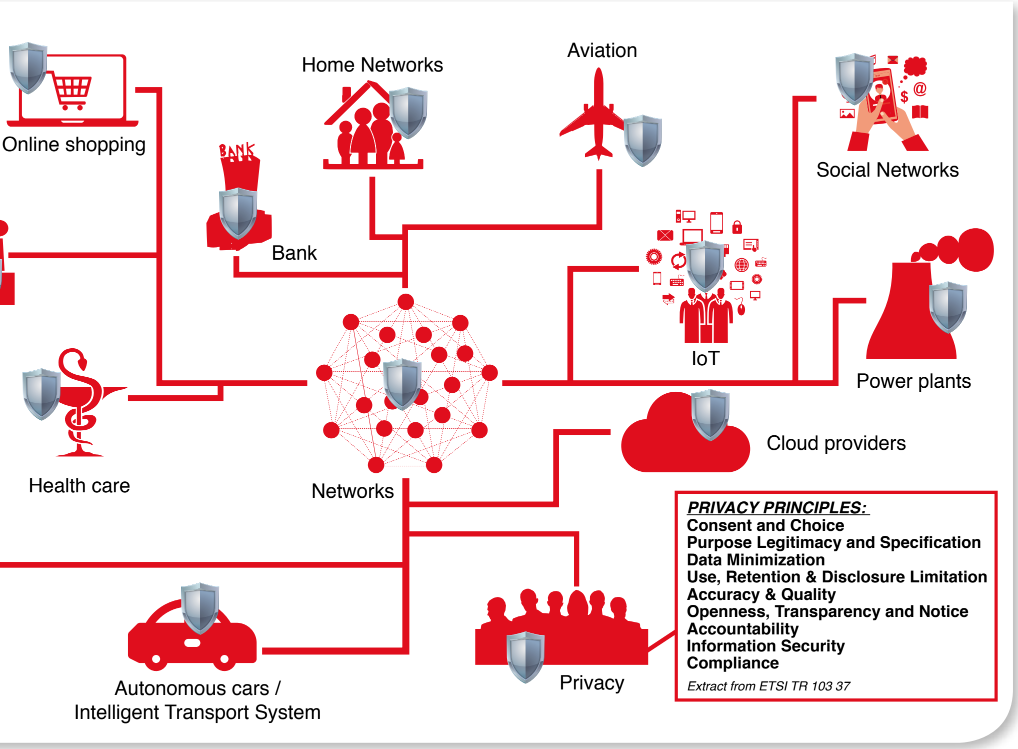
Raising security awareness has become vital. But one size does not fit all these use cases and we must find the right balance between security measures and security risks.

In Europe, regulators and European bodies include member states, security authorities, the European Commission, ENISA and ECSO. They play a key role in harmonizing EU regulations and promoting a European cybersecurity strategy. All European regulations are taken into account in ETSI standards.

> There are multiple threats to defend against and the creativity of attackers has no limits.

Security and privacy for the end user

Where organizations are not able to secure their networks, the result is often a huge privacy hit: personal data is stolen. There is a strong demand for privacy from citizens and governments, and this requirement leads to needing to secure organizations' networks and data. Privacy and security are not mutually opposed: we need more of both. The European regulation GDPR is a strong means to enforce personal data privacy and its reach may go beyond Europe. Standardization bodies are actively working on developing standards on privacy impact assessment; in ETSI, this work is going on in TC CYBER, which has released a report on Privacy Principles.



PRIVACY PRINCIPLES:
Consent and Choice
Purpose Legitimacy and Specification
Data Minimization
Use, Retention & Disclosure Limitation
Accuracy & Quality
Openness, Transparency and Notice
Accountability
Information Security
Compliance

Extract from ETSI TR 103 37

The role of standardization bodies

Standardization bodies have a leading role to play in supporting the improvement of Internet security.

A lot has been already done: ISMS, Common criteria security evaluation (ISO/15408, ISO/IEC 18045) and PIMS (Privacy impact management systems) ISO/IEC 27552, to name a few.

ETSI is a major contributor with its TC CYBER, and security by design has always been a concern in ETSI's work. ETSI specifications address enterprises in various domains, government bodies and, most recently, end users. Very practical reports and guides facilitate implementation for experts and non-experts. Standardization will facilitate interoperability between technologies, exchange of information on threats and risks (see the ISI group which will shortly join TC CYBER) and mutually recognized security evaluation according to the Cyber Act recommendations.

> There is a strong demand for privacy from citizens and governments.

There is still plenty to do, however, as Internet security is not a dream but a permanent work in progress.

As Lao Tzu rightly said, "Whoever invented the boat also invented the shipwreck", something to bear in mind…

■ *Jean-Pierre Quemard, ETSI's Vice Chair TC CYBER*

ISARA quantum-safe TLS testbed based on ETSI VPN work

Quantum computers will be able to break current public key cryptography algorithms. Data transiting via Virtual Private Networks is at risk. To anticipate this issue, ISARA Corporation has recently introduced an agile quantum-safe TLS testing product.

A large-scale quantum computer, which experts estimate will be available in 7-15 years, is expected to solve particular, complex problems enabling advancements in areas such as material design, pharmaceuticals and traffic optimization. However, a quantum computer will also be able to break the complex maths problems that underlie ubiquitously used public key cryptography causing pervasive cybersecurity vulnerabilities.

The two primary areas of concern are the threats to confidentiality and authentication. The most immediate risk is to confidentiality due to “harvest and decrypt” attacks. Secure, encrypted information is harvested and stored today with the intent to decrypt at a later date when a cryptographically-relevant quantum computer is available. At risk now is data shared today with confidentiality requirements beyond a decade, such as classified information, patient health records, and intellectual property. It’s a matter of urgency to protect the confidentiality of data in transit over VPNs (Virtual Private Networks), which rely on protocols that use vulnerable public key cryptography.

To protect against the threat of quantum-enabled adversaries data needs to be secured using quantum-safe cryptography. In the absence of standardized quantum-safe algorithms, the NIST-recommended approach is to use hybrid cryptography. VPNs and the protocols they rely on for cryptographic security need to support “hybrid key establishment.” Hybrid key establishment combines a key generated using a classic scheme, such as Elliptic-curve Diffie-Hellman (ECDH), with key(s) created using one or more quantum-safe schemes, protecting against attacks using existing computers while protecting against future quantum-enabled attacks. The keys are combined such that the security of each scheme remains intact. ETSI describes this as the “best of both worlds approach.”
Recently, ISARA Corporation announced the availability of the ISARA Catalyst™ TLS Testbed for vulnerable organizations to test hybrid key establishment using their existing systems. ISARA used the common requirements for hybrid use cases from ETSI’s Technical Report “Quantum-Safe Virtual Private Networks” to implement hybrid key exchange in TLS 1.2:

- Satisfy the need for quantum-safe cryptography now
- Ensure backwards compatibility (for interoperability)
- Ensure FIPS compliance (for classical algorithms only)
- Provide cryptographic agility without future limiting assumptions about the properties of algorithms within the protocols
- Limit the amount of exchanged data

Also, ETSI recommends that TLS implementers “use at least 2 algorithms… to be negotiated over a combination of at least one classical handshake and one or more quantum-safe handshakes.” ISARA’s implementation uses quantum-safe algorithms combined with one classical.

Every day confidential information is shared over VPNs increasing the risk and impact of harvest and decrypt attacks. Fortunately, forward-looking organizations can start protecting now by testing hybrid use cases, such as hybrid key exchange, using the ISARA Catalyst TLS Testbed.

■ *Mark Pecen, Chief Operating Officer, ISARA Corporation.*

The EU Cybersecurity Act -
where are we today?

Following the political agreement that was reached in December 2018, the EU Cybersecurity Act is finally on the last stretch and it is due for adoption by mid-2019. The European Union Agency for Network and Information Security (ENISA), an ETSI partner, tells us more.

It is a significant milestone that is expected to give a new impetus to the European industry while meeting policy requirements at Member State level. Under the Act, the key role reserved for ENISA is to assist in the preparation of candidate cybersecurity certification schemes. In doing so, ENISA needs to interact with both the EU Member States and the industry stakeholders, to gather opinions and advice to feed into candidate schemes. ENISA looks forward to this newly acquired role and the opportunity it represents for cybersecurity in the EU. As an example of successful collaboration, on 21 January 2018, the Agency, along with CEN, CENELEC and ETSI, organized a conference entitled "Cybersecurity Standardization and the Cybersecurity Act: Where are we today?".

This conference was attended by stakeholders representing a broad range of industry sectors. It was commonly agreed there that the momentum should be leveraged to allow Europe to move to the forefront of the market for cybersecurity solutions.

While key limitations of the current situation with cybersecurity certification stem from market fragmentation and uncertainty with regard to the assurance provided by current arrangements and schemes, concrete mitigation measures have been deemed necessary, especially in the aftermath of massive cyber attacks.

With a view to pursuing the policy goal of a common cybersecurity certification framework across the EU, the newly founded role for the EU on cybersecurity certification seeks to put on a different footing the ability of consumers and the government to acquire better cybersecurity products, services and processes. By providing rated levels thereto, it is expected that a level of cybersecurity commensurate with the risk profile of the application involved will be attained, and thus reduce the risk footprint that would have to be mitigated by the end user. Moreover, it is expected that industry too is likely to benefit from this internal market framework and produce better outputs that will stand up to global competition.

Clearly, the success of the role of ENISA depends on support from and cooperation with key stakeholders who have an interest in EU schemes for the certification of ICT products and services.

With regard to standards, there are key issues that may need further clarification. The Cybersecurity Act (CSA) does elaborate partially on standards, which leads to open questions on, for example, criteria for selecting appropriate standards, handling of areas where gaps exist (and the over-standardized ones) and consideration for commercial solutions. ETSI is a leading actor in that field and our partnership is essential to move things forward.

The aim is to have the bulk of open questions answered and resolved by mid-2019, when the CSA should enter into force. This will be the time to move into implementation. Therefore, continued dialogue between all stakeholders remains essential.

■ *Sławomir Górniak, Expert at ENISA*

Introducing...

ETSI Technical Committee CYBER

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 cybersecurity – protecting the Internet and IoT, securing communications and providing security tools for businesses that need them. ETSI TC CYBER is making these standards for today and for the future.

The ETSI committee is recognized as a major trusted centre of expertise offering market-driven cybersecurity 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.

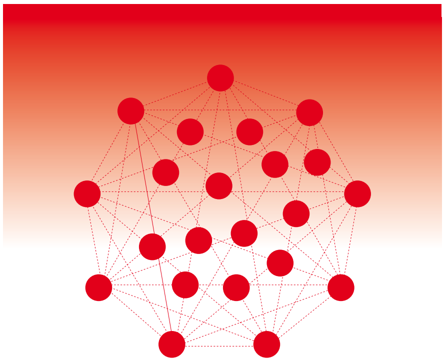
We provide standards that are applicable across different domains, for the security of infrastructures, devices, services, protocols, and to create security tools and techniques.

TC CYBER is the most security-focused technical committee in ETSI, and we have many strands of work. In this article, I'll discuss our roadmap and those key areas where standardization can help on the journey to better security.

Understanding the cybersecurity ecosystem

TC CYBER created a Technical Report on the global cybersecurity ecosystem, ETSI TR 103 306, which discovers and assembles lists of global cybersecurity constituents. This knowledge is important to find where TC CYBER can best contribute to the global security landscape.

It attempts to be as inclusive as possible to expand our collective insight into the extent and diversity of the ecosystem, including: forums, activities for information exchange, techniques, standards, operational standards, centres of excellence (global and national) and reference libraries.



Protection of personal data and communication

Protecting personal data has become a hot topic, especially since publication of the GDPR. TS 103 532 is one specification in TC CYBER that focuses on Attribute-Based Encryption, one of our newer areas, aiming to provide user identity protection whilst preventing disclosure of data to an unauthorized entity.

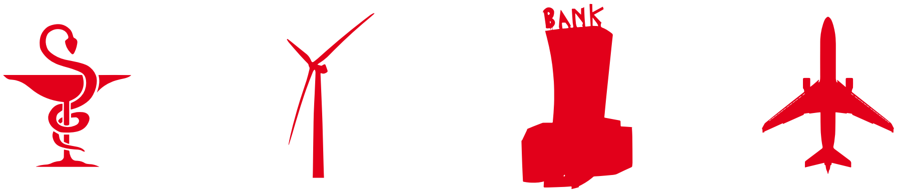
TS 103 458 describes high-level requirements for Attribute-Based Encryption and defines personal data protection on IoT devices, Wireless Local Area Networks (WLAN), cloud and mobile services, where secure access to data is given to multiple parties.

IoT security and privacy

As more devices in our homes connect to the Internet and as people entrust their personal data to an increasing number of services, the cybersecurity of the Internet of Things is becoming a growing concern. Poorly secured products threaten consumers' privacy and some devices are exploited to launch large-scale DDoS cyber attacks.

TC CYBER has recently released a standard for Cybersecurity in the Internet of Things, TS 103 645, to support a good security baseline for Internet-connected consumer products.

Cybersecurity for critical national infrastructures



Critical infrastructure is defined in ETSI TR 103 303 as: “any infrastructure for which loss or damage in whole or in part will lead to significant negative impact on one or more of the economic activities of the stakeholders, the safety, security or health of the population”.

Security is clearly important in this sector, so TC CYBER is active in this area, recently standardizing metrics for supporting critical national infrastructures and creating a Technical Specification to improve smart meter security.

Direct support to EU legislation

We recognize our key role to play in helping stakeholders comply with regulation, such as the NIS Directive, ePrivacy, GDPR and the Cybersecurity Act, demonstrated by our publications giving guidance to meet the legal measures and technical requirements of the NIS Directive, TR 103 456, and to technical standards for privacy, TR 103 370.

TC CYBER understands its responsibility in supporting EU legislation and is even hosting a Cybersecurity Policy track at its annual Security Week event in June to discuss how standards can help industry to implement EU policy.

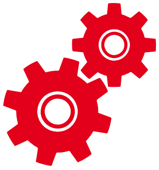
Forensics

We are working to standardize the process of receiving, transforming and outputting material which can be assured digitally. Specifically, the assurance of the material is not dependent on the process having been carried out by a qualified or trained human expert. The aim is to provide assurances so strong that material can be used in legal proceedings.

Enterprise/organization and individual cybersecurity

ETSI creates standards that are driven by industry need. In 2017, we published TR 103 421, which recommended providing standards-based solutions to the evolving needs of industry, networks and middleboxes, sparking TC CYBER’s subsequent work on middleboxes: a crucial part of network function and defence today, whether you call them proxies, firewalls or intrusion detection systems. We also produced the Critical Security Controls, TS 103 305, a five-part series of pragmatic guidance and advice that are widely applicable to many enterprises – and very understandable.

Cybersecurity tools



TC CYBER works on several specific techniques and tools to enhance cybersecurity. One technique is for protecting software in a white box model – a growing need in security today, as more software finds itself in a white box model.

Another specification creates a secure interface to offload sensitive functions to a trusted domain: essential for securing virtual functions. We are now working on external encodings for the Advanced Encryption Standard (AES) and a guide to Identity-Based Encryption.

Quantum-safe cryptography

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.

■ *Alex Leadbeater, ETSI’s TC CYBER Chair*

3GPP 5G Security
stable foundations

Intense standardization activity has begun to support various business sectors requiring new capabilities and features from 3GPP networks.

A major focus of the 3GPP Security Working Group (SA3) is to make sure that security features created for LTE can be evolved and expanded for 5G and that all new 5G security enhancements to cover new services also consider the impact to existing LTE systems. This dual approach is a time saver, helping to reduce any duplication of the group's efforts on threats to radio interfaces, the signalling plane and the user plane, as well as masquerading, privacy, replay, bidding down, man-in-the-middle and inter-operator security issues.

A recent article by the SA3 leadership "3GPP 5G Security"[1] describes, in depth, the "new radio" (NR) and the 5G core (5GC) security challenges, explaining the underlying trust models in the system, for roaming and non-roaming cases.

Building on the first set of 5G specifications, the latest work plan for Release 16 will take a further big step to cover the Internet of Things (IoT) and the variety of possible scenarios and threats that it will bring. The 3GPP Study on "Cellular IoT support and evolution for the 5G System", TR 23.724, looks at alternatives for supporting both wide-band and narrow-band IoT, bringing to light several areas that will need specific SA3 security work – including work on power-saving functions, overload control, high latency communication, monitoring and service capability exposure, as well as other features, as they are specified.

The list of ongoing SA3 studies reveals a real movement towards new industry sectors in the current work plan, bringing in a new set of 5G use case scenarios. Around twenty studies on security aspects – with a heavy focus on IoT and on new industry sectors – are being completed, building on the progress already made in Release 15.

In TS 33.501, the reader can find a full description of the 3GPP 5G security architecture, with all the security features and procedures performed within the 5G System specified or referenced there.

■ *Kevin Flynn, Communications Professional 3GPP*

Ongoing 3GPP SA3 Studies

Security of URLLC for 5GS
Security for 5GS Enhanced support of Vertical and LAN Services
Study on evolution of Cellular IoT security for the 5G System
Security of enhancements to the 5GC location services
Security of the Wireless and Wireline Convergence for the 5G system architecture
Mission Critical Services Security Enhancements
Security aspects of Enhancements for Network Slicing
Security Assurance Specification for 5G
Security Aspects of the 5G Service Based Architecture
Security aspects of single radio voice continuity from 5G to UTRAN
Supporting 256-bit algorithms for 5G
5G security enhancement against false base stations
KDF negotiation for 5G System Security
Long Term Key Update Procedures
Long Term Key Update Process (LTKUP) Detailed solutions
User Plane Integrity Protection
Authentication and key management for applications based on 3GPP credential in 5G
SECAM and SCAS for 3GPP virtualized network products
Security Impacts of Virtualisation
Security aspects for LTE support of V2X services

Source: www.3gpp.org/specifications/work-plan

[1] *3GPP 5G Security, August 6, 2018 - http://www.3gpp.org/news-events/3gpp-news/1975-sec_5g*

Insight into oneM2M security

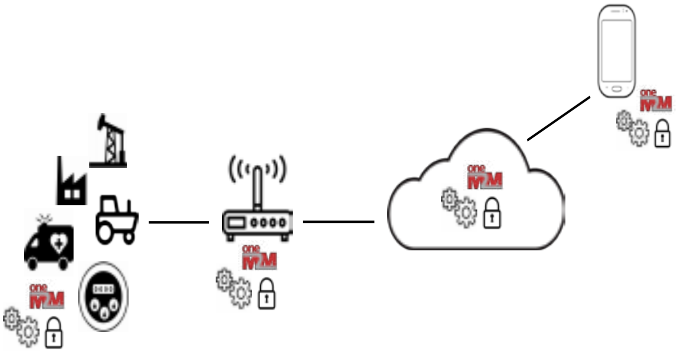
At oneM2M, security is a serious matter. Security services include enrolment, security mutual authentication, authorization, end-to-end security, privacy management.

Reducing complexity of IoT apps

oneM2M defines a set of commonly used services that can be realized as software services within various types of endpoint devices, gateways/edge nodes and servers. The supported set of functions includes services that are commonly required by IoT devices and applications. Regardless of its deployment model, oneM2M reduces the complexity of IoT applications/devices by offloading the burden of having to implement these services. oneM2M also enables interoperability since it supports services to enable standardized communication and interaction between IoT applications/devices from different developers and manufacturers.

One important service supported by the oneM2M Service Layer is security. This service supports the following capabilities:

- enrolment
- security association establishment
- authorization
- end-to-end security
- privacy management



Enrolment

IoT devices/applications typically require - during the initialization or joining process - provisioning and configuration of identifiers and security credentials before they can securely connect and become trusted. oneM2M supports the capability to remotely bootstrap and provision IoT devices and applications with these necessary identifiers and credentials. This entity is called the MEF, or M2M Enrolment Function.

Security association establishment

To be able to securely use services offered by the oneM2M Service Layer, devices/applications need to be mutually authenticated and establish what is known as a oneM2M security association with the Service Layer. oneM2M supports security associations based on pair-wise symmetric keys, public key certificates, and mutual third-party authentication. The security association results in a TLS or DTLS session being established between two oneM2M components (IoT device/application, Gateway, server, …).

Authorization

oneM2M supports several options for authorizing the access to services and information stored within the Service Layer. The owner of the service or information has the possibility to define policy rules to grant access to other oneM2M components. Many possibilities are defined for the access rules by the Service Layer: static through an access list, dynamic with token generation, or distributed authorization system.

End-to-end security

Besides having security associations between two oneM2M communicating components, the standard offers the possibility to have end-to-end secure communication between source and destination IoT device/application endpoints. Hence, oneM2M supports the capability to end-to-end protect the confidentiality and integrity of oneM2M messages that flow through the Service Layer via intermediate oneM2M nodes.

Privacy management

oneM2M supports user privacy protection via a personal data management framework which converts a User's privacy preferences into access control information that protects the User's Personally Identifiable Information. oneM2M offers users the possibility to set up their privacy preferences.

■ *Mr. Wei Zhou, Datang, Vice Chair System Design and Security (SDS) Working Group, Mr. Dale Seed, Convida Wireless, Chair SDS WG and Saïd Gharout, Orange, Chair Requirements and Domain Models WG*

A European Certification Framework
based on suitable standards

The fourth industry revolution denotes a complete makeover of our societies, economies, businesses and infrastructures, at the same time resulting in an increasing number of opportunities for hackers to conduct large scale cyber attacks.

Europe needs high-quality, affordable and trustworthy cybersecurity solutions to protect the European Digital Single Market.

The European Cyber Security Organisation (ECSO) implements, together with the European Commission, the very first Public-Private Partnership on Cybersecurity (cPPP). Established in 2016, it federates a wide range of stakeholders, thus making ECSO the voice of the European Cybersecurity Community.

Created with the intent to bridge the gap between research and innovation activities and the market needs to strengthen the European ecosystem, ECSO is also developing a coherent industrial policy looking at key aspects like vertical sector demand, supply chain management, training and certification.

The political agreement on the Cybersecurity Act lays down major building blocks to enhance cyber resilience in Europe and sets the rules for the creation of the framework for European cybersecurity certification.

A very broad set of security certification schemes and standards (SOTA) exists, since there is no unified solution suitable for addressing the market needs and challenges the industry (COTI) is facing.

The ECSO Meta-scheme Approach represents a key step towards fostering trust by defining transparent rules to harmonize the minimum security required, define a unified levelling across verticals, and propose a common way to determine the scope and required security claim. There are still many questions to answer for full implementation of the Cybersecurity Act in terms of applicability of standards, criteria for selecting from among possible competing standards, and how to handle areas where there are no standards to ensure alignment of the timeline for the definition of standardization and certification schemes.

Standards are a key instrument for supporting certification by promoting best practices, interoperability and cybersecurity requirements in a consistent way relevant to the interdependence across the ICT industry value chain. Certification based on suitable standards would contribute to the development of a fully trustworthy European supply chain. In this context, ECSO has established collaborations with ETSI and CEN/CENELEC.

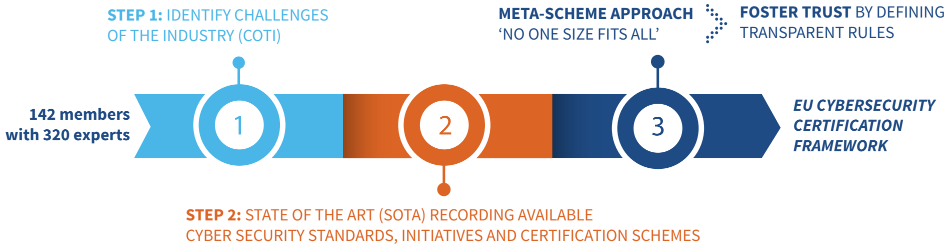
ECSO is working on an update of the Meta-scheme approach, to make it a suitable toolbox to accommodate different business requirements and identify the gaps in standardization and complementarity between standards from the analysis of the COTI.

The toolbox will include the criteria for deciding on the fit-for-purpose type of assessment and procedures for advising on characteristics under which certification schemes can be viewed and selected.

ECSO will continue its efforts to provide the building blocks and meet the needs of the private sector across the supply chain with the aim of contributing to the establishment of an innovative, secure and resilient global information infrastructure.

■ *Luigi Rebuffi, Secretary General, ECSO*

TO FOSTER TRUST IN DIGITALISATION, TRANSPARENT RULES FOR CYBER SECURITY ARE NEEDED


STEP 1: IDENTIFY CHALLENGES OF THE INDUSTRY (COTI)
META-SCHEME APPROACH 'NO ONE SIZE FITS ALL'
FOSTER TRUST BY DEFINING TRANSPARENT RULES
142 members with 320 experts
1
2
3
EU CYBERSECURITY CERTIFICATION FRAMEWORK
STEP 2: STATE OF THE ART (SOTA) RECORDING AVAILABLE CYBER SECURITY STANDARDS, INITIATIVES AND CERTIFICATION SCHEMES

New educational material: **TEACHING STANDARDS**

ETSI

UNDERSTANDING ICT STANDARDIZATION:
PRINCIPLES AND PRACTICE

Dr. habil. Nizar Abdelkafi
Cees J.M. Lanting
Marina Thuns

Prof. Raffaele Bolla
Dr. Alejandro Rodriguez-Ascaso
Dr. Michelle Wetterwald

ETSI has just completed a 3-year project to develop teaching materials for a comprehensive education course on ICT standardization.

This action was taken with the support of the European Commission and the EFTA Secretariat.

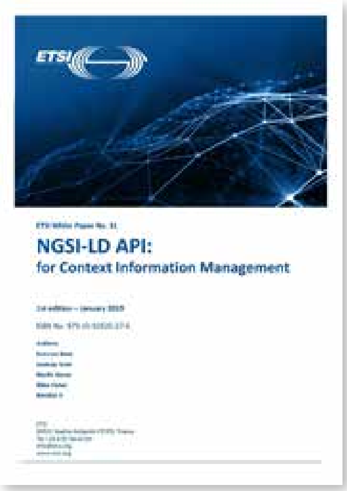
The materials, a textbook and a comprehensive set of slides, are now available from the ETSI website free of charge and are designed to be adapted by lecturers and teachers according to their specific needs. The materials are being trialled in universities and we expect usage to grow as we update and promote them over the coming years.

Download the teaching materials from: www.etsi.org/standardization-education

White paper: **CONTEXT INFORMATION MANAGEMENT API**

This White Paper, developed by the ETSI CIM group, explains the main concepts behind a new data exchange protocol called NGSI-LD whose goal is to make it easier to find and exchange information with open databases, mobile Apps and IoT platforms. The document describes an open framework for the exchange of contextual information for smart services, using a RESTful API named NGSI-LD.

The term NGSI points to earlier work from the Open Mobile Alliance V2 and the term LD points to concepts of Linked Data as the other major influence. This paper also highlights the advantages of NGSI-LD for smart service solution providers and for software developers



ETSI

ETSI White Paper No. 31

NGSI-LD API:
for Context Information Management

1st edition – January 2019

ISBN No. 979-10-92620-27-6

Authors:
[illegible]

ETSI
06921 Sophia Antipolis CEDEX, France
Tel +33 4 92 94 42 00
info@etsi.org
www.etsi.org

White paper: **MULTI-ACCESS EDGE COMPUTING SOFTWARE**

This white paper, Developing Software for Multi-Access Edge Computing, provides guidance for software developers on how to properly approach architecting and developing applications with components that will run in edge clouds, such as those compliant with ETSI's MEC standards. It summarizes the key properties of edge clouds, as distinct from a traditional cloud point-of-presence, as well as the reasons why an application developer should choose to design specifically for these. It also provides high-level guidance on how to approach such design, including interaction with modern software development paradigms, such as micro-services -based architectures and DevOps.

ETSI

ETSI White Paper No. 20

Developing Software for
Multi-Access Edge Computing

2nd edition – February 2019

ISBN No. 979-10-92620-29-0

Authors:
Dario Sabella, Vadim Sukhomlinov, Linh Trang, Sami Kekki, Pietro Paglierani, Ralf Rossbach, Xinhui Li, Yonggang Fang, Dan Druta, Fabio Giust, Luca Cominardi, Walter Featherstone, Bob Pike, Shlomi Hadad

ETSI
06921 Sophia Antipolis CEDEX, France
Tel +33 4 92 94 42 00
info@etsi.org
www.etsi.org

New ETSI Video coming soon: **CYBERSECURITY**

In today's connected world, it has become even more essential to secure our systems, hardware, software and data to keep our society working. But the evolving nature of security risks makes cyber security a complex challenge. Each stakeholder has a different perspective and as such is part of the overall solution. ETSI brings all these stakeholders together to produce resilient and globally applicable cyber security standards. Stay tuned for our new video! It will be out soon.

How *editHelp!* really helps!

The editHelp! team

With over 100 years of combined experience, *editHelp!* is a team of practical and dedicated editors always aiming to provide efficient and extensive service to the ETSI Technical Bodies, Industry Specification Groups and Partnership Projects, which require swift editing and document management support.

Our purpose is to assist our members and our partners in their on-going drafting process and to help them produce better and cleaner drafts, which will ultimately guarantee excellent quality standards. Our proactive support ensures that all standardization documents are made publicly available in a timely and cost-efficient manner.

Over the years, the department has mastered the delicate balance of being rigorous when it comes to quality control and flexible to meet our member's constraints.

Our drive for continuous improvement has led us to explore different and innovative ways to simplify and accelerate the overall drafting process of a standard. Our dedicated website is one of them; a simple design helps our members visualize everything they need to know at a glance. It gathers a wealth of information for all, including updated video tutorials for newcomers. To make sure we stay up to date with our customers' needs, we regularly produce surveys. We also organize specific training sessions and presentations for our experts and technical writers upon request. And since we're always looking ahead we, The Standards People at *editHelp!* ensure a continuous technological watch seeking out new tools and methods to continually improve the editing process for standards.

Any questions? Feel free to visit the *editHelp!* website at https://portal.etsi.org/Services/editHelp!.aspx or to come and speak with the team of editors at our offices in Sophia Antipolis: the door is open!

eSignatures for internal use

We tend to forget it, but the ETSI Secretariat is also using ETSI Standards on a daily basis. An example? The digital/electronic signature developed by the Technical Committee on Electronic Signatures and Infrastructures. All our Industry Specification Group agreements, our Special Task Force expert contracts and our Plugtests Non-Disclosure Agreements (NDAs) are now signed electronically thanks to ETSI standards, in particular ETSI EN 319 142 defining signatures for PDF documents.

A day to remember

On 13 October, 2018, in the beautiful parklands of Mougins Etang de Fontmerle, ETSI joined volunteers from Sophia Antipolis companies, local universities, sports clubs and care homes, to accompany residents from six centres for mentally handicapped adults - in a day of competitive sport.

The Comité Départemental Sport Adapté des Alpes Maritimes (CDSA-06) runs a large variety of sports activities all year round, for several adult centres.

The 2018 edition of the “Défi sport handi-valide 06” was the eighth of its kind and ETSI’s sixth consecutive appearance.

Although the event was created to raise money for the Association, it also exists to help bridge the gap between so-called ‘able’ and ‘disabled’ workers.

Each year the participating companies form teams with residents from the centres.

All ten teams had a winning feeling: Like you get when you turn up to something on your Saturday morning, slightly regretting it, but you go home very happy and a little bit wiser.

For the sixth consecutive year, everyone of us left with the feeling that people really are ok - generally - and some people are brilliant (especially the residents, families, educators and volunteer students).

The organizers said it best: “Let’s stay together despite our differences.” Sometimes a little bit of effort is enough. Here’s looking forward to next year’s games.

Fédération Française du Sport Adapté

Alpes-Maritimes

Welcome to our new staff members

Antoine Mouquet,
Junior Technical Officer

Guillermo Vietti,
Technical Officer

Originally from the North of France, Lille, Antoine used to spend his holidays on the Côte d’Azur. When he applied for “Polytech”, the largest pool of Engineering schools in France, he naturally turned to the Sophia Antipolis campus for his Master’s.
But the sun wasn’t the only reason; his choice was mainly due to the networks and telecommunications curriculum focused on innovative technologies.
During his internship period at Vinci, in Nice, he worked on the extension of the Nice tramway and was in charge of low-voltage applications such as access control, fire detection and CCTV, to name a few.
He actually improved his English in Gdansk, Poland, during his six months of study there, as it was the common language among international students.

Born in Argentina, Guillermo obtained his PhD in Electronic and Telecommunications Engineering at the Polytechnic University of Turin in Italy and worked at the university Research Electronic department on Applied Electromagnetic Fields and Radio Devices Sector. In 2011 he joined Pirelli in the “Cyber Tyre” department. In this department, sensors fitted in tyres can “read” the road condition and interface in real time with other electronic car systems, transmitting data to improve driving conditions in high-performance cars. After being a Project Manager, he became the technical account manager of this technology, in California, following innovative customers in the automotive sector. He is also the convenor of the TPMS Working Group within the standardization organization ETRTO and an active member of ISO, VDA and ACEA.

Hear from us in conferences

and meet with us at exhibitions.

Find more information and register on our website at: www.etsi.org/news-events

April 2019

MPLS + SDN + NFV World Congress

9-12 April, Paris, FR

The Congress, endorsed by ETSI, will once again bring together major stakeholders from among service providers and enterprise networks evolution.

5G Realised

10-11 April, London, UK

The summit, endorsed by ETSI, will look at use cases for 5G across different industry sectors.

Smart Transportation & Mobility

10-11 April, London, UK

This event, endorsed by ETSI, will tackle the three pillars of Connected and Autonomous Vehicles on the road: connectivity, electrification and automation.

EENA Conference 2019

10-12 April, Dubrovnik, HR

At the European Emergency Number Association (EENA) annual conference, ETSI's Technical Officer Chantal Bonardi will chair a session on NG112, creating a direct link with ETSI's TC EMTEL.

Network Transformation Congress

29 April-1 May, San Jose, US

This congress, endorsed by ETSI, will address new network and services automation with NFV and SDN technologies.

May 2019

5G Huddle

14 May 2019, Tokyo, JP

ETSI is once again pleased to endorse the 5G Huddle and ETSI's CTO Adrian Scrase will deliver a keynote at the event.

NFV Europe

21-23 May, Berlin, DE

The event will address NFV, SDN, Cloud Native Infrastructure, Service Assurance, Service Enablement, 5G, Open Source, Orchestration & Security.

DSP Leaders Forum

22-23 May, London, UK

Communication Service Providers will debate the challenges they face transitioning into Digital Service Providers. ETSI members: visit telecomtv.com/dspetsi and use code "DSPETSI" for a discount.

ETSI Neighbours Day

28 May 2019, 16-19h, ETSI, Sophia Antipolis, FR

ETSI is creating this opportunity for local members and potential members to get together for networking and exchange and at the same time will showcase ETSI to its guests via technology info stands and f2f discussions.

June 2019

4th NFV PLUGTESTS

03-07 June, ETSI, Sophia Antipolis, FR

Building on the experience of the Remote NFV API Plugtests, the event will extend the scope of the interoperability test sessions among different VNFs, MANO solutions and NFV platforms to include additional features and conformance checks.

London Tech Week

10-14 June, London, UK

The event, endorsed by ETSI, will include Internet of Things World Europe, VR & AR World, the AI Summit, 5G World, Mission Critical Technologies and Blockchain for Business Summit.

ETSI Security Week

17-21 June, ETSI, Sophia Antipolis, FR

This event comprises cybersecurity landscape, cybersecurity and policy actions, Artificial Intelligence and security, cybersecurity and the dynamic nature of technology, networks and society and a Middlebox Security Protocol Hackathon.

ETSI SNAPSHOT

January – February 2019

871
members

26%
SMEs

60
technical groups

149
standards

+1022
standards under development

1.7M
standards' downloads

57
meetings

139
eMeetings

2126
participants

1308
eParticipants

108
partnerships

9
conferences & Plugtests

@ETSI Secretariat

122
people

15
nationalities

ETSI
650 Route des Lucioles
06560 Valbonne France
Tel: +33 (0)4 92 94 42 00

64
countries

About ETSI

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 a not-for-profit body with more than 800 member organizations worldwide, drawn from 66 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).
For more information please visit: www.etsi.org

For any information on Enjoy!,
to contribute, to be removed from the list of hard copies or subscribe to it, contact us at: enjoy@etsi.org

ETSI The Standards People

Follow us on: