Enjoy!

THE ETSI MAG

APRIL 2021

THE INTERVIEW

Paul Browne
CTO Assa Abloy UK. p.4-5

TECH HIGHLIGHTS

Deep dive on quantum safe hybrid key exchange. p.10-11

IN THE SPOTLIGHT

Standards to the rescue: Saving IoT security for consumers. p.13-14-15

HOME & OFFICE: SWEET AND SECURE?

ETSI

Editorial

Our ubiquitous connected environment opens new doors to cybersecurity breaches.

IoT devices have become commonplace at home. We open our doors with smart locks, switch on light and music with a smart home voice controller and make sure our cake will be ready on time in our smart oven when it's time for dinner. We share our computers and tablets among family members and overall increase our activity online, bridging office and home when working remotely. But this ubiquitous connected environment opens new doors to cybersecurity breaches and raises the question of ensuring that our homes and offices are as sweet and secure as we would expect them to be. In this new edition of Enjoy! we let you discover how standards come to the rescue to improve security in our private and professional life.

In the Spotlight** section focuses on our EN 303 645 security guidelines for IoT consumer devices which have been adopted by manufacturers and governmental bodies round the world, Midea dishwashers being the example of our **showcase.

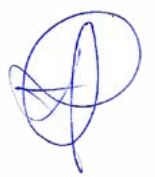
*SpyCloud CEO Ted Ross, one of our **new members,** explains why human intelligence remains key to prevent cyber crimes while in an exclusive **interview,** Assa Abloy UK CTO, Paul Browne, tells us how ARGE, the European Federation of Associations of Locks & Builders Hardware Manufacturers can contribute to cybersecurity standards for smart homes.*

*To address future needs, our **Technology Highlights** outlines how to exchange a cryptographic key with classical and post quantum security and in a second article the Vice Chair of our pandemic tracing apps group explains how they tackle the challenge of digital fragility. And then, the Chair of our Permissioned Distributed Ledger group tells us why standards for distributed ledger technologies (commonly addressed by people as blockchain) will be key for industry and governmental institutions.*

To help manage our ever-increasing online activity, we have also developed guidelines and standards supporting it. US based Digicert explains why Europe has led the world in unifying identity proofing standards. An upcoming Plugtest™ will let industry test our guidelines for modern Electronic Registered Delivery Services while our Centre for Testing and Interoperability has developed a now popular free online tool that performs numerous checks to verify the conformity of the ETSI Advanced Electronic Signatures, those we use for signing contracts online.

And there's more, so now Enjoy reading!

Luis Jorge Romero,
Director-General ETSI



Enjoy! The ETSI Mag

Edited and published by ETSI
Quarterly edition

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 IoT Week 2021 goes virtual

The *ETSI IoT Week* is back on 26-30 April 2021 as a fully virtual event providing the latest IoT industry and standards updates. This year's edition will focus on the major IoT standards achievements that support the digitalization of society, business, and multiple Industries across numerous sectors. It will also focus on how such digitalization enables countermeasures against the current pandemic. The event will cover oneM2M with service experiences and best practices; IoT in the face of the pandemic addressing digitalization and countermeasures; IoT cybersecurity for consumers, smart cities, e-Health and SMEs; Artificial Intelligence in IoT as well as other key topics. Register Now!

New group on IPv6 Enhanced Innovation

In the 5G and cloud era, IPv6 will grow rapidly. Strengthening new generation IP network technologies based on IPv6 and its innovative technologies has become the common direction of the IP industry.

To tackle the increasing Industry needs for IPv6 adoption in multiple use cases and scenarios, ETSI has recently launched *ISG IPv6 Enhanced innovation (IPE).* IPE members include 45 organizations to date, comprising carriers, vendors, and academia, working together to improve the industry ecosystem and accelerate innovation.

The group will first analyse the current landscape of existing IPv6 standards deployed on prime technologies such as 5G, IoT and Cloud Computing to identify gaps and thus accelerate IPv6-based innovations. Two other reports will cover data centre and Cloud use cases on one hand and 5G Transport use cases on the other hand. The last pieces of work will define Industrial IoT/ enterprise requirements and IPv6 only transition requirements across new and evolving technology domains and areas.

ETSI at ENISA Cybersecurity Standardization Conference

The European Standards Organizations, CEN, CENELEC and ETSI, joined forces with ENISA, the European Union Agency for Cybersecurity, to organize their *annual conference* virtually this year. The event, which took place from 2 to 4 February, attracted some 1500 participants from the EU and from around the world. The conference addressed standardization in relation to the Radio Equipment Directive (RED) and certification under the provisions of the Cybersecurity Act (CSA). ETSI Director-General, GA Chair and Board Chair as well as several cybersecurity experts from the technical committee CYBER and 3GPP outlined ETSI's strong achievements for enterprise and consumer cybersecurity standards and its input to harmonized legislation with testability of security requirements. They highlighted as well ETSI's contribution to the Cybersecurity Act as regards consumer IoT security, 5G Network Security Assurance, Trust Services, and AI security.

From his CTO office in the UK, Paul Browne tells us why an association of locks and builders hardware manufacturers entered the world of cybersecurity standardization.

How did ASSA ABLOY, a leading hardware locks manufacturer, enter the digital lock market?

It started ten years ago when we, in ASSA ABLOY UK, developed a digital door lock for residential use. At the time, we already had extensive experience in home security systems and we had the vision that people's homes in Europe would eventually become connected so that they could have the convenience and the security of controlling devices around their home.

Paul Browne

CTO & Business Development Director, Assa Abloy UK, Board Member ARGE

Paul Browne is the Chief Technology Officer and Business Development Director of *ASSA ABLOY UK.* He started his career at Creda, the largest manufacturer of white goods in the UK, which became part of a joint venture between GE USA and General Electric Company (GEC UK) held several executive sales and marketing positions in the company before becoming the general manager of one of their business divisions.

In 2000, he joined ASSA ABLOY where he now leads product innovation and new product introductions as well as business development and strategy across channels, products and end-user markets. He is also responsible for standards development and IP. Paul is a Board Member of ARGE, the European Federation of Associations of Locks & Builders Hardware Manufacturers, member of ETSI.

It was at about that time that ASSA ABLOY acquired iRevo, a Korean company, which was the largest manufacturer of digital door locks for home use in the world. You have to bear in mind that in Korea, at least 50 to 60% of all homes, probably more now, have a digital door lock.

> "In Korea, at least 50 to 60% of all homes have a digital door lock."

So for us as a manufacturer, digital door locks, and in particular now smart door locks, have a strategic importance.

What are the benefits of digital locks for the market?

If I take the UK market, we sell a mechanical door lock for around 25 euros, and that will last 20 years. A digital door lock typically costs 200 to 300 euros and will last ten years or so. You can see that from a commercial point of view, digital door locks and smart door locks are a terrific opportunity for manufacturers.

Now when you look at it from a consumer point of view, smart locks bring enhanced functionality. People can send keys by phone to family members, allow access to their homes, or check on the status of their doors and windows remotely. But unlike mechanical door locks, the life cycles of digital door locks change every two, three or five years. So as you can see, the whole dynamic is more exciting, more appealing. Digital and smart door locks, but also smart alarms, smart home security are a big opportunity for the end user's enhanced lifestyle and for the industry.

However, when we launched our digital door lock around 2010 in the UK, we had a problem. The police, insurance companies and the locksmiths were asking us to develop a standard at the request of consumers who wanted their digital or smart door locks to be secure and, at the time, there was no standard to reassure them.

> "The police, insurance companies and the locksmiths were asking us to develop a standard."

You mean that the standard was actually initiated at the consumers' request?

Absolutely. The best standards originate from end users. The worst standards are those that are imposed by central governments or by European governments. We therefore started working with our national standards body, the British Standards Institute, to develop a technical specification for digital door locks. But we wanted to develop a performance standard which would give consumers the reassurance that the products are secure, that would give insurance companies a standard on which to base home insurance policies, and that would enable the police and locksmiths to give guidance and advice to consumers.

Since connected IoT devices are a relatively new marketplace, we felt that unless we got a performance standard in place, with locks being potentially vulnerable to cyberattacks, that this would damage the credibility and the reputation of the market before it even took off.

And this is when you heard about ETSI?

Yes, that was two years ago when I met with the Minister of the UK Department for Digital, Culture, Media and Sport, along with other suppliers of smart home products. It was clear that the DCMS was keen to address the security of IoT devices from a cybersecurity standpoint. That's where we found out that the DCMS had worked in ETSI TC CYBER to develop the technical specification TS 103 645.

That was when ARGE, in its role as the European Industry Association, made an important decision. As hardware manufacturers in ARGE, we knew that we could identify the standards for the mechanical, electromechanical and the electronic aspects of a smart door lock with CEN, but we were lacking on the cybersecurity aspect. During that meeting, we realized that the experts were in ETSI. So last year, when ARGE became a member of ETSI and we joined TC CYBER, we suggested that we create a smart door lock technical specification, which is currently under development.

In parallel, we found out that ENISA's remit is to develop certification schemes, particularly for consumer IoT devices.

So, certification schemes are important as well?

Yes, we've been participating in ENISA's Cyber Certification Stakeholder Group and feeding back into the Union's Rolling Work Programme. In the European Commission, it's very clear that there is an appetite to develop certification schemes for consumer IoT devices. They see this as being important, but they also see that the level of home security connected devices needs to be somewhere between "substantial" and "high", which backs into our thinking.

> "The EC wants to develop certification schemes for consumer IoT devices."

Within the ETSI cyber group, they identified that a smart door lock technical specification could form a pilot for a vertical product certification scheme. A smart lock standard is holistic in nature but adding the cyber security aspect combined into a certification scheme will reassure consumers. For example, in the UK, they will see the Kitemark certification logo on the box, in France, that might be the A2P logo.

But as I said earlier, we were thinking of a whole series of standards.

This series of standards would be developed in ETSI?

Yes, to complement the smart door lock, they would address vertical sector products such as connected alarms, connected CCTV, connected door viewers, and so on.

What we like about ETSI is the fact that they recognize and appreciate that product life cycles are shorter, that technology and cyberattacks change. And they adopt a much more flexible and pragmatic approach to standardization and developing technical specifications than other standards bodies. So, for us at ARGE the way that ETSI approached the whole concept of certification and standardization for connected IoT devices for the home is very appropriate.

Welcome to our NEW members

Avanti Communications, United Kingdom

Avanti Communications is a world leading provider of agile, secure and pioneering satellite technology across Europe, the Middle East and Africa. They have a proven track record of satellite connectivity services, and bring a world of opportunities to carriers, defence and security departments, government agencies and the satellite industry.

Bandwidth, USA

Bandwidth provides cloud-ready voice, messaging, and emergency service connectivity built for the enterprise. It is the only API platform provider that owns a Tier 1 network that gives better quality, rates, and control. It is also a leader in the cloud communications space, uniquely positioned to have enterprises who need high reliability and scale.

Commsquare NV, Belgium

Commsquare provides mobile data network monitoring, analysis and optimisation products and services, helping mobile operators measure network performance and extract actionable business intelligence. Their products and services deliver a holistic view of radio access and PS data network performance from a subscriber's point of view.

eID - Electronic Identification, Spain

eID is the leading provider of remote user iDentification systems via video streaming. It created VideoID which identifies the User in seconds and offers the same level of security as the face-to-face iDentification made in a commercial office.

ELA (European Lift Association), Belgium

ELA represents the lifts, escalators and moving walks active associations and their components manufacturers in the European Union and the European Free Trade Area. It has become the main communication vector of this industry to the European Commission and the European Parliament.

evolutionQ, USA

evolutionQ provides information on quantum-safe services. evolutionQ offers a standard set of services proven to help ensure your company's quantum-safe cyber security migration is progressive, sensible and orderly.

Exacta Global Smart Solutions, USA

Exacta offers a range of services that help companies bring Internet of Things solutions based on the oneM2M global standard from concept to deployment. It offers oneM2M project support, oneM2M training, support for deployment of the industry recognized Chordant implementation of oneM2M service layer.

Gatehouse Satcom A/S, Denmark

GateHouse delivers the software that guarantees effective and secure communication between systems. They support live tracking and monitoring of more than 150,000 assets within different businesses and delivers mission critical solutions in satellite communication for maritime authorities, coastguards, ports and related businesses.

IASME, United Kingdom

IASME is a cyber security business with products and services dedicated to help individuals and organizations to protect themselves against cyber-attacks. The IASME Governance assessment includes a Cyber Essentials assessment and GDPR requirements and is available either as a self-assessment or on-site audit.

Innovile, Spain

Innovile provides smart network management and optimisation solutions and services. Innovile offers a wide range of innovative and future-proof portfolio of self-organising network, configuration management, performance management and expert services that empower mobile network operators with real-time network intelligence and operational dynamics.

ISEE SSU, Ukraine

The Ukrainian scientific and research Institute of special equipment and forensic expertise of SSU is part of the Security Service of the Ukraine and ensures cyber security of the state thanks to complex measures to counter online terrorism, prevent cyber espionage, defeat hacker attacks and refute subversive activities online.

Kimeggi, France

Kimeggi consulting provides support to business in radio strategy, radio solutions and standardization. They currently monitor, attend and/or contribute in many committees to bring the most up-to-date information on standards, technologies and spectrum regulations.

MaxLinear, USA

MaxLinear delivers high-performance broadband and networking semiconductors based on its highly integrated radio frequency analogue technology, high-performance optical networking technology and its pioneering MoCA and direct broadcast satellite ODU single-wire technology. Customers include telephone, cable and satellite operators, set-top box manufacturers, networking equipment and consumer technology providers.

Mercedes-Benz, Germany

Mercedes-Benz AG is one of the largest manufacturers of premium passenger cars. The company aspires to be leading in the fields of connectivity, automated driving and alternative drives. With over 40 production sites on four continents, they align themselves to meet the requirements of electric mobility.

Schindler, Switzerland

Schindler is one of the world's leading providers of elevators, escalators, and moving walks, as well as maintenance and modernization services. The company specializes in the latest-technology engineering, as well as mechanical and microprocessor technology products designed and tested for safety, comfort, efficiency and reliability.

SK ID Solutions AS, Estonia

SK ID Solutions (SK) specializes in international e-identity solutions. They enable citizens of different countries to log in to e-services and give electronic signatures. Their main business is the certification and time-stamping service developing technology and applications for electronic signing and their validation services.

SpyCloud Inc., USA

SpyCloud prevents online fraud via solutions which protect billions of employee and consumer accounts from account takeover. They are the trusted account takeover fraud prevention partner for B2B organizations and consumer brands and some of the most innovative financial services, retailers, and technology companies around the globe.

Universidad de Malaga, Spain

Málaga University (UMA) is a public institution which promotes outstanding research and teaching within the European Higher Education Area. It follows an educational model to promote competitive, quality teaching which is employment-orientated and accredited in Europe.

In this exclusive interview, SpyCloud CEO and founder shares his insight on the company's mission to make the internet a safer place by preventing criminals from profiting from stolen information.

Are you seeing any trends in cyberattacks so far in 2021?

It pains me to say it, but what we saw the start of in 2020 – attacks resulting from our collective pivot to digitally managed lives – has spilled over into 2021. This shift to remote work, virtual school and online food shopping has substantially expanded the attack surface for both individuals and organizations, and criminals are taking advantage. People are sharing devices among family members at home, increasing the amount of activities done online, and managing new accounts – some that reuse compromised passwords already in criminals' hands.

Ted Ross

CEO & Co-Founder of SpyCloud

Ted Ross is an industry veteran of twenty-nine years in the network and security industries. His career began in the U.S. Air Force, after which he became Director of Network Engineering at West Corp, Strategy Architect at Walmart, Executive Technology Director at TippingPoint, and VP of the Office of Advanced Technology at HP.

At HP, he created a new team and built the threat intelligence practice from the ground up as Director, Threat Intelligence, HP Security Research. This team created reports on nation-state threat groups that, at the time of publication, were considered to be the most comprehensive reports on select adversarial nations' cyber capabilities.

After HP, Ted led Exodus Intelligence as CEO. In 2016, Ted launched ***SpyCloud*** as CEO and Co-Founder.

All of this aids our daily lives, and I think a lot of businesses would say they've seen a rise in productivity since the start of the pandemic, but it also provides threat actors with a plethora of new targets.

So far this year, we're seeing criminals continue to leverage the tactics they found most profitable last year: malware campaigns designed to siphon personal

> "So far this year, we're seeing criminals continue to leverage the tactics they found most profitable last year."

and machine data from victims, phishing attacks aimed at stealing credentials (which then often lead to ransomware attacks), and credential stuffing (often represented by the media as a 'data breach,' when in fact it's just criminals performing account takeover by leveraging old passwords on new accounts).

How do you protect customers from Account Takeover Fraud?

Criminals are clever and will keep inventing ways to steal from you, and users will keep making mistakes that put their accounts at risk. There is one sure-fire way to get ahead of account takeover, which is to check users' account credentials against recently-breached data and identify compromised accounts. Then you have the choice

> "To stop Account Takeover Fraud, you need to beat attackers at their own game."

to force a password reset or send the user through a step-up authentication process, proving that the user is who they claim to be and not a criminal leveraging a stolen password. The goal is to beat attackers at their own game, negating the value of the stolen information before they have a chance to use it.

SpyCloud fuels global enterprises' ability to safeguard more than 2 billion employees' and consumers' accounts from cyberattacks including account takeover and follow-on attacks like credit card fraud, phishing, ransomware and more, which can be extremely costly and disruptive.

You state that you're using Human Intelligence for breach data collection; in the AI era, it sounds anachronistic. Can you elaborate on this?

The vast majority of the valuable breach data we collect is via human intelligence (HUMINT) – SpyCloud researchers embedded in the criminal underground who social engineer data from bad actors within days after a breach. These researchers are specialists in their field, with extensive expertise that isn't easy to replicate. The reason we rely on HUMINT

> "Human intelligence can deliver data much sooner than dark web scanning."

is because it delivers data so much sooner than dark web scanning. Most people don't realize that by the time data shows up on the dark web, it could be years after the breach occurred. By that time, the data has been fully monetized and is of very little value. We're focused on the early part of the breach timeline, when the data is fresh and most valuable to criminals. In fact, human intelligence capabilities enable us to be the first to find out a breach has occurred and notify the affected victim organization.

All that said, automated technology is still critical to the process of making breach data ingestible by enterprises.

Tell us more about the technology that underlies HUMINT.

Breach data isn't delivered in a neat .csv file with standardized columns and plaintext passwords that enable easy matching to users' credentials. The process to parse and normalize that data and make it machine-readable requires extensive technology – not to mention the automation required to crack passwords at scale. Without cracking passwords, there would be no way for enterprises to exactly match passwords to determine if a user's account is truly compromised and worth the little bit of friction to force a password reset or fire off MFA.

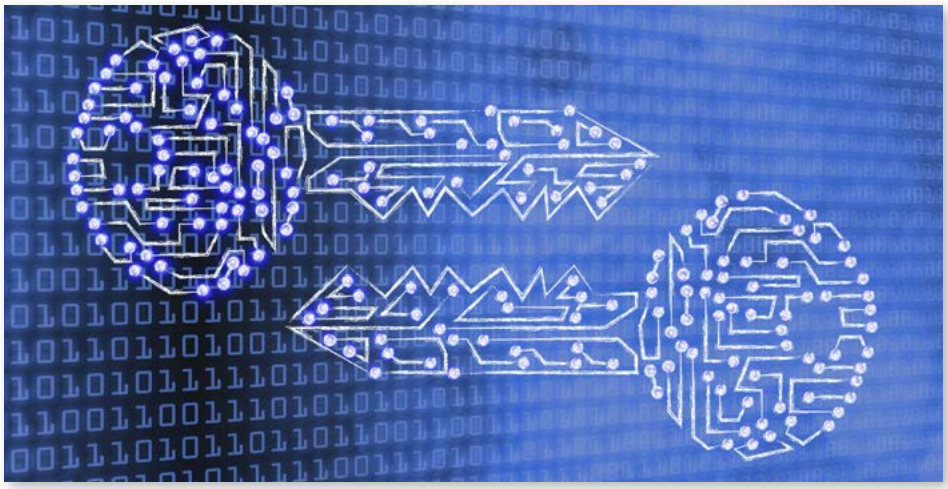
You have joined ETSI's TC CYBER lately, what is the added value of standardization for your activity?

SpyCloud is often the first to confirm to victim organizations that a breach has occurred, and we want to leverage our industry-leading capabilities and database to work as a good citizen with others in the industry to help alleviate account takeover and its associated cybercrime. SpyCloud has joined ETSI TC Cyber so we can more effectively and openly collaborate with other industry leaders to put effective standards in place that can most optimally benefit enterprises and consumers globally. ETSI's work on Mobile Device and IoT security guidelines and best practices are complementary to the use of SpyCloud's data – and the use of a corpus of recovered breach data or recovered botnet logs could provide valuable data points that augment existing security best practices. For example, even if a device appears to be "secure" both at the hardware and software levels, it may be of value to also know if any other factors associated with that device are compromised, such as the user's account, password, IP address, or phone number.

> "ETSI's work on Mobile Device and IoT security guidelines and best practices are complementary to the use of SpyCloud's data."

Deep dive on quantum safe hybrid key exchange

Engineers and developers can now rely on ETSI's specification to exchange a cryptographic key with classical and post quantum security and build, test and deploy quantum-resistant ICT systems today.



Some background

In 1994, Peter Shor showed how to factor large RSA modulus and solve the discrete log problem. His algorithm breaks the public key cryptosystems we use today for public-key based key exchanges but it requires a large-scale, fault-tolerant quantum computer to break cryptographically relevant instances of ECC and RSA. As we know, there are a number of challenges in building such a computer and while progress is routinely made on these challenges, it is uncertain if or when such a quantum computer will be available. Yet, we need to anticipate and work on quantum-safe cryptography.

Post-quantum or quantum-safe cryptography refers to cryptographic schemes for which there is no known vulnerability by a large-scale quantum computer. The National Institute of Standards and Technology (NIST) Post-Quantum Cryptography Standardization Process is evaluating solicited submissions for quantum-resilient public-key cryptographic algorithms and has announced is 3rd Round finalists. *ETSI TS 103 744* specification is using a mechanism from these candidates.

The problem statement

Today, the existing key exchanges are at risk from a future adversary with a quantum computer. Many Information and Communication Technology (ICT) solutions utilize these public-key mechanisms to provide long-term confidentiality. The confidentiality requirement of the data in these ICT systems vary from short-lived (days and months) to long-lived (20-30 years). If a large-scale quantum computer arrived on the market during the security lifetime of this data, it could result in the loss of confidentiality.

ETSI has worked on the issue and the CYBER Quantum-safe Cryptography group developed *ETSI TS 103 744,* a Technical Specification that defines how to exchange a cryptographic key with classical and post quantum security. The specification called "CYBER; Quantum-safe Hybrid Key Exchanges," combines a classical elliptic curve Diffie-Hellman ephemeral (ECDHE) exchange with a proposed post-quantum key encapsulation mechanism (KEM) from the NIST Round 3 candidates. Hybrid key exchanges are a migration technique to move to quantum-safe technology in advance.

We know from experience it takes a decade to adopt new public-key algorithms into ICT systems. It starts with in-depth analysis of the fundamental security claims of the algorithm, testing and standardization. Once the cryptographic standard is complete, engineers and developers can include it into other ICT standards. We can parallelize this work today to reduce the time to deploy standardized quantum-safe systems, ensuring the long-lived confidentiality of data in ICT systems. By standardizing and using quantum-safe hybrid key exchanges, we can define and deploy ICT systems today that provide both classical and quantum-resistant security.

■ *Matthew Campagna, Chair of the ETSI Quantum Safe Cryptography working group.*

Digital fragility: a challenge faced by COVID-19 tracing apps

"Fragility" is not a term that one hears or reads very often when it comes to digital. "Agility" is much more common, particularly when it refers to the buzzword "agile". It seems now that everything must be agile: every business, every system and, to a certain extent, every one of us must be agile. The recently released "Comparison of existing pandemic contact tracing systems" Report, developed by ETSI's E4P group, includes the term "digital fragility" among its definitions in its clause dedicated to terms, symbols and abbreviations.

Digital fragility

Today, "digital" permeates all aspects of society and will continue doing so. Fragility, unfortunately, permeates all things digital as the overall degree of digital dependency also increases. In such a context, mobile device-based digital contact tracing is no exception. Digital fragility can be said to be an entity-organization, system, application, etc.- which may suffer an incident of a "digital" nature disturbing its normal activity without, at times, being aware of it. A more usual expression would be "weak [digital] security". Indeed, most people refer to it as a lack of "cybersecurity".

Leading to ETSI's group

On 23 March 2020, as part of the European Commission's response to the coronavirus, the Internal Market Commissioner, Thierry Breton, held a videoconference with CEOs of European telecommunication companies and GSMA to discuss how to join forces to mitigate the spread of CoV-SARS-2. On that day, digital fragility in solutions to fight the pandemic was mentioned: the need to discuss telecommunication network resilience; the need to collect, share and analyse anonymized metadata for modelling and predicting the propagation of the virus; the need to comply with the GDPR & ePrivacy legislation and, last but not least, the relevance of protecting the networks against cyber attacks. Two months later, as a result of this joint effort, ETSI E4P held its kick-off meeting on 26 May.

And cybersecurity

So far, digital fragility has been present in every step taken by experts in the ETSI E4P group. The *GR E4P-002* considers this issue among the most relevant challenges current digital contact tracing systems have to face, along with responsiveness, privacy preservation, interoperability, etc. Other incoming deliverables describing technical requirements of these solutions also include security recommendations and requisites. Stay tuned, you will be able to enjoy them in the following weeks!

In summary, attention should be paid to the number of digital risks, from software glitch, error, negligence, misuse or fraud to even sabotage during the development, deployment and operation/use stages of Government-sponsored digital contact tracing systems. These constitute a set of risks that could threaten the feasibility of any of these counter-pandemic solutions. Once again, rigour in training, processes and the availability of these systems' source code (which will make it possible to audit all their details in the area of cybersecurity, as should be done regarding trust, ethics, privacy, etc.) will contribute to minimizing digital contact tracing's cyber-fragility.

■ *Miguel García-Menéndez, Vice Chair ETSI E4P ISG.*

ETSI blockchain group releases major Reports

ETSI ISG on Permissioned Distributed Ledger has recently released Reports to support the need on the part of industry and government institutions for what is commonly known as blockchain. *ETSI GR PDL 002,* "Applicability and compliance to data processing requirements", describes the implications of the conduits used to connect data sources (sensors, gateways etc.) to distributed ledgers in utility and related industries. The Report also defines how regulatory aspects for data infrastructure security and privacy can be satisfied. *ETSI GR PDL 003* details the application scenarios and operational requirements for permissioned ledgers to help telecom operators, Internet and over-the-top service providers implement the technology. The latest one, *ETSI GR PDL 004,* defines an architecture and functional framework for smart contracts and their planning, coding and testing. *"Most ledgers in ICT have been centralized so far, but the recent approaches based on distributed ledgers provide higher openness and better resiliency,"* says Diego Lopez, Chair of ETSI ISG PDL.

Middlebox Security Protocols for fine-grained access control

The ETSI Technical Committee CYBER has released *ETSI TS 103 523-2:* Transport Layer MSP (TLMSP), Part 2 of the Middlebox Security Protocol (MSP) series, which defines a protocol for varied (fine-grained) access control to communications traffic.

Middleboxes are vital in modern networks – from new 5G deployments, with ever-faster networks that need performance management, to resisting new cyberattacks with evolved threat defence that copes with encrypted traffic, to VPN provision. Network operators, service providers, users, enterprises, and small businesses require being granted varied (fine grained) permissions. *ETSI TS 103 523-2,* MSP Part 2 addresses this gap by specifying a protocol that allows fine-grained access and nuanced permissions for different portions of traffic, allowing middleboxes to perform their functions securely whilst keeping up with the rapid pace of technical development.

First Report in Securing Artificial Intelligence

The ETSI Securing Artificial Intelligence Industry Specification Group released its first Group Report, *ETSI GR SAI 004,* which gives an overview of the problem statement regarding the securing of AI. ETSI SAI is the first standardization initiative dedicated to securing AI. The Report describes the problem of securing AI-based systems and solutions, with a focus on machine learning, and the challenges relating to confidentiality, integrity and availability at each stage of the machine learning lifecycle. It also points out some of the broader challenges of AI systems including bias, ethics and ability to be explained. A number of different attack vectors are outlined, as well as several cases of real-world use and attacks. *"There are a lot of discussions around AI ethics but none on standards around securing AI. Yet they are becoming critical to ensure security of AI-based automated networks,"* explains Alex Leadbeater, Chair of ETSI ISG SAI.

HOME & OFFICE: SWEET AND SECURE?

IoT has become commonplace at home as more devices connect to the internet. People now share their personal data with an increasing number of services and the cybersecurity of the Internet of Things (IoT) is a growing concern. If consumer IoT is an established global phenomenon, ETSI's world-leading work in that field can help to improve security for a variety of devices and appliances. Alex Leadbeater, Chair of the ETSI Technical Committee CYBER, in our "spotlight" is leading us through our current and future activities for the consumer market. The *ETSI EN 303 645* standard is a first of its kind and is already a highly successful achievement with worldwide uptake by manufacturers who now benefit from several certification schemes to enhance the security of their products. Today the *Roborock vacuum cleaner* has been certified by TUV-Rheinland against the ETSI standard. And more recently, Midea dishwashers, air conditioners and dehumidifiers have all been certified by TÜV SÜD as Luffy Deng explains in our showcase on page 16. In the future, consumers can expect more secured IoT home devices in their living room, kitchen, to unlock their door and make their life easier.

Standards to the rescue:

Saving IoT security for consumers

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 (IoT) has become a growing concern. Consumer IoT is an established global phenomenon, with its security improved by ETSI's world-leading work on Consumer IoT security.

ETSI's Consumer IoT Security work demonstrates the value of standards; one innovative and high-quality standard has underpinned many assurance schemes and provided flexibility in certification - whilst achieving a world-leading increase in baseline security.

From dishwashers to doorbells...

With an explosion in marketability, IoT has become commonplace in the home – from health trackers to home assistants, from smart TVs to smart lightbulbs, and from dishwashers to doorbells. Estimates regularly state there are more than 30 billion connected devices in the world today, with the consumer IoT sector showing no signs of slowing down its growth.

New devices, same old security issues

But when a market moves quickly, the pressure to be first to innovate can result in a loss of dedicated security effort. This happened in consumer IoT, where default passwords are widespread and poorly secured products threaten consumer's privacy, and some devices are exploited by attackers to launch large-scale DDoS cyber attacks, mine cryptocurrency and spy on users in their own homes.

> The pressure to be first to innovate can result in a loss of dedicated security effort.

Standards to the rescue - saving IoT security

Two years ago, ETSI TC CYBER published the first globally applicable standard on IoT security to address these security shortcomings, encouraging manufacturers to build security into IoT products from their design, rather than awkwardly bolting security measures on at the end. This baseline focuses on 13 security areas as well as data protection.

This standard achieved global adoption and evolved into an EN standard, *EN 303 645,* designed to prevent large-scale, prevalent attacks against smart devices that cybersecurity experts see every day. It establishing a security baseline for connected consumer products and provides a basis for future IoT certification schemes.

ETSI EN 303 645 supports a good security baseline for connected consumer products, provisioning a set of recommendations for 13 security areas, with the top three being: no default passwords, implement a vulnerability disclosure policy, and keep software updated. There are also specific data protection provisions for consumer IoT devices.

> EN 303 645 provides a significant security baseline, achievable by SMEs.

Global uptake and accreditation schemes

ETSI EN 303 645 is a cohesive and achievable standard that provides a single target for manufacturers and IoT stakeholders to attain. It's no surprise, given the urgent need for increased security in this sector and the momentum in ETSI's work, that many organizations have already based their products and certification schemes on *EN 303 645.* These include:

- Singapore's national Cybersecurity Labelling Scheme
- Finland's national consumer IoT certification scheme
- PSA Certified (backed by Arm)
- The Global Certification Forum accreditation
- TÜV SÜD testing

Many organizations have already based their products and certification schemes on EN 303 645.

- TÜV Rheinland worldwide testing and certification
- VDE Institute testing
- SESIP by Global Platform mapping
- SGS IoT Testing and Conformity Assessment Program
- DEKRA security evaluations
- UL's IoT Security Rating assessment, verification and labeling solution
- Safeshark and BSI IoT cyber security assessments, testing and certification
- And many more: Eurosmart, KIWA, Secura, Nemko, ACCS, IASME…

The future of Consumer IoT Security

Yet, we are not done! TC CYBER's dedication to improve IoT security is ongoing, and currently includes the development of three further standards to complement and support EN 303 645: an assessment specification, an implementation guide, and a vertical smart door lock standard.

1. The assessment specification specifies baseline conformance assessments against the provisions of *ETSI EN 303 645.* It sets out mandatory and recommended assessments, to be used by testing labs, certifying bodies and manufacturers that wish to carry out a self-assessment. Completion is targeted for summer 2021 – so get involved soon!
2. The implementation guide gives easy-to-use guidance to help manufacturers and other stakeholders to meet the provisions defined for Consumer IoT devices in *ETSI EN 303 645.* It sets out example implementations that meet the provisions in the EN.
3. As ETSI EN 303 645 provides a baseline that spans a variety of consumer IoT devices, sometimes additional sector-specific requirements need to be stipulated to standardize device security. Currently, TC CYBER is working on one such vertical standard for smart door locks, based on *ETSI EN 303 645* (read our interview on page 4-5).

ETSI's Consumer IoT Security work can't stop gaining momentum! These initiatives demonstrate the value of quality and timely standards. One innovative and high-quality standard has underpinned many assurance schemes and provided flexibility in certification - whilst maintaining a world-leading security baseline for a huge security problem

Alex Leadbeater, ETSI's Chair TC CYBER.

Midea and TÜV SÜD join forces to inspire trust in smart-home appliances

People-focused technology can make our home life smarter and happier. However, cybersecurity and the protection of personal data are critical considerations whenever people enjoy the convenience of their smart homes.

Addressing consumer concerns

Improving cybersecurity and data protection capabilities of smart home devices and building customers' trust are among the top priorities of consumer IoT manufacturers. In keeping with its vision of "bringing great innovations to life", the Midea Group is committed to a systematic smart home security and privacy programme in accordance with international and industry standards, which extends from lower-level hardware to user-friendly software and covers threat and risk monitoring, cloud security and the security of connection modules and chips, apps and smart-home appliances. Given this, Midea has joined forces with TÜV SÜD for the assessment of its smart-home appliances in accordance with the ETSI EN 303 645 standard to ensure best practices in data security and data protection.

First appliances compliant with EN 303 645

TÜV SÜD, a leading global provider of quality, safety and sustainability solutions, assessed the implementation of important security baseline functions against the 14 provisions of the ETSI EN 303 645 standard. The relevant mandatory provisions of the standard address product design, mobile application, communication and document review. For example, to keep software updated, the update communication of Midea IoT appliances is established over secure channel encrypted by a dynamic session AES256 key. In addition, the update also ensures not only the mutual authentication by RSA 2038 but also the integrity check by SHA256. Once the updated is completed, a user may receive notification pop-up on the APP. TÜV SÜD then tested several series of Midea dishwashers, air conditioners and dehumidifiers and issued certificates of conformity with the ETSI EN 303 645 standard, which help to inspire consumer trust in the use of smart-home appliances.

Technology makes life better but consumer protection requires the joint efforts of all parties. With "4S + 1M" (Cloud Security, Communication Security, Smart Home Appliance Security, Application Security, and Data Protection Management) smart home business group Midea has developed a comprehensive framework for smart-home cybersecurity, privacy and data protection which it continually improves and advances in accordance with various international and industry standards.

ETSI has revised and improved the standards in line with the state of the art, providing a vital basis and operational guidelines for consumer protection. The testing and certification organisation TÜV SÜD has been passionate about technology since day one and strives to inspire trust and add value.

■ *Luffy Deng, Senior Project Engineer, TÜV SÜD Shenzhen.*

"Localized" certification:
the Indian example

Global standards ensure that products will be able to address markets beyond national or regional borders. However, attention needs to be given to the local certification programmes that may ultimately bring in additional requirements for local market access. Discover how ETSI works towards minimizing such cases through international cooperation.

Ready?

So your product is ready, in line with the latest global standards it has to comply with. Everything is ready for distribution in your region and you are eyeing other markets, your team abroad reports great demand for this new product and sales prospects are bright. But there is a catch: to begin distribution of your product, you need to get a stamp stating that it meets all the local requirements. Ideally, it should only be a matter of showing the test results obtained when preparing for distribution in your first target market. Unfortunately, such recognition is not always possible and upon inspection, local compliance testing appears to tweak and add requirements in such manner that there is no avoiding running another full round of testing, with a locally accredited laboratory. This costs time and money and therefore affects the product's time to market and price.

Partners will help

ETSI and the Partnership Projects it is part of (*3GPP, oneM2M*) strive to deliver a full package: use cases and requirements, architecture and technical solutions, as well as testing specifications used to verify conformance/interoperability. Such specifications need to be leveraged to the maximum extent when establishing technical requirements for market access. Leveraging its Partners network and through projects like SESEC, SESEI, EU-India or *InDiCo,* ETSI brings players together, in technical and political spheres, to assess discrepancies in certification requirements for ICT products and work towards increasing commonality, with partial or full recognition of testing/certification results already obtained.

The Indian example

ETSI, the European Commission and the Delegation of the European Union in Delhi have recently worked with members of the European industry and of the Indian government to understand and compare the European requirements re. safety and EMC to those from India's Mandatory Testing and Certification of Telecom Equipment (MTCTE). Subsequently, representatives of India's Telecom Engineering Center (in charge of MTCTE) visited key European laboratories to fully grasp the extent of the testing performed, even for products meeting requirements of legislation developed under the lightweight New Legislative Framework.

The work continues with exchanges on security requirements for telecom equipment, looking at the European 5G Toolbox, the 3GPP specifications, the GSMA NESAS and the Indian Telecom Security Assurance Requirements (ITSAR). This will in the end result in closer alignment of the requirements in Europe and India and reduce additional efforts in the testing of products aimed at both markets. Similar initiatives will take place in other countries/regions as needed.

■ *Xavier Piednoir, Head of External Relations, ETSI.*

An Industrial Framework for Blockchains

The general public is familiar with blockchains through the popular cryptocurrency Bitcoin but there is much more to it, and distributed ledgers are important tools to address industry and governmental institutions.

Blockchain or not blockchain?

Often identified with the catchy name of blockchains, distributed ledgers have brought a wide range of disruptive applications enabling highly valuable goals such as data sovereignty or disintermediation. Distributed ledgers store any kind of data as a consensus of replicated, shared, and synchronized digital records distributed across multiple sites, without depending on any central administrator. They provide as main features immutability (and therefore non-repudiation) and multi-party verifiability of the stored data and their temporal succession, addressing a wide range of application scenarios, and new interaction models among those entities willing to record the transactions associated to those interactions through these ledgers.

Distributed ledgers

These technologies have become the intrinsic foundation of today's secure decentralized cryptocurrencies, and distributed ledgers owe their popularity and many of the main use cases to this fact, focusing on different ways to provide decentralized multi-party compensation and therefore avoid the need for centralized clearinghouses. But we must not forget we are talking about the many additional scenarios where a consensual, replicated, and synchronized data ledger could become a game changer. While distributed ledgers are mostly known because of their use as cryptocurrencies, there are many other uses besides them, with examples such as smart contracts, support to digital identity attributes, object tracking, or the verification of service level agreements.

Permissioned and permission-less

Further on, it is important to remark distributed ledgers can be considered as permissioned or permissionless, regarding the requirements for a node to be approved to validate the transactions and record them on the ledger. While permissionless ledgers are the ones that have received most attention from the general public, with the paradigmatic example of Bitcoin, permissioned distributed ledgers are the ones best qualified to address most of the use cases of interest to the industry and governmental institutions. This is due to reasons both technical and organisational. Among the technical ones we can consider the cost and delay of the recording of a transaction, the cost of the consensus algorithm, or the preservation of fairness among participants. In the second category, the most relevant are the support from external legal agreements and the regulatory enforcement in critical sectors.

Permissioned Distributed Ledger in ETSI

Within the ETSI Industry Specification Group on Permissioned Distributed Ledger (ISG PDL), we have been working for the last two years on analysing and providing the foundations for the operation of permissioned distributed ledgers. The group has already produced

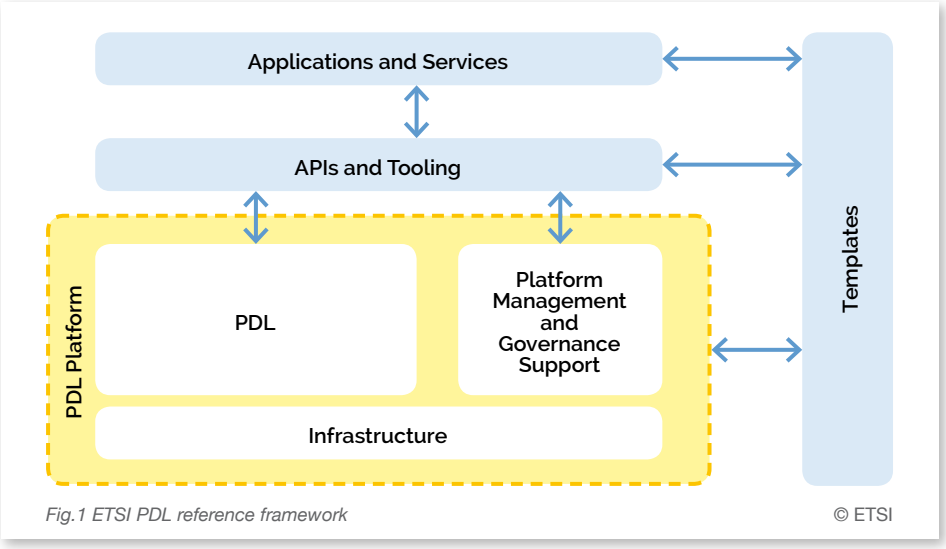


Fig.1 ETSI PDL reference framework

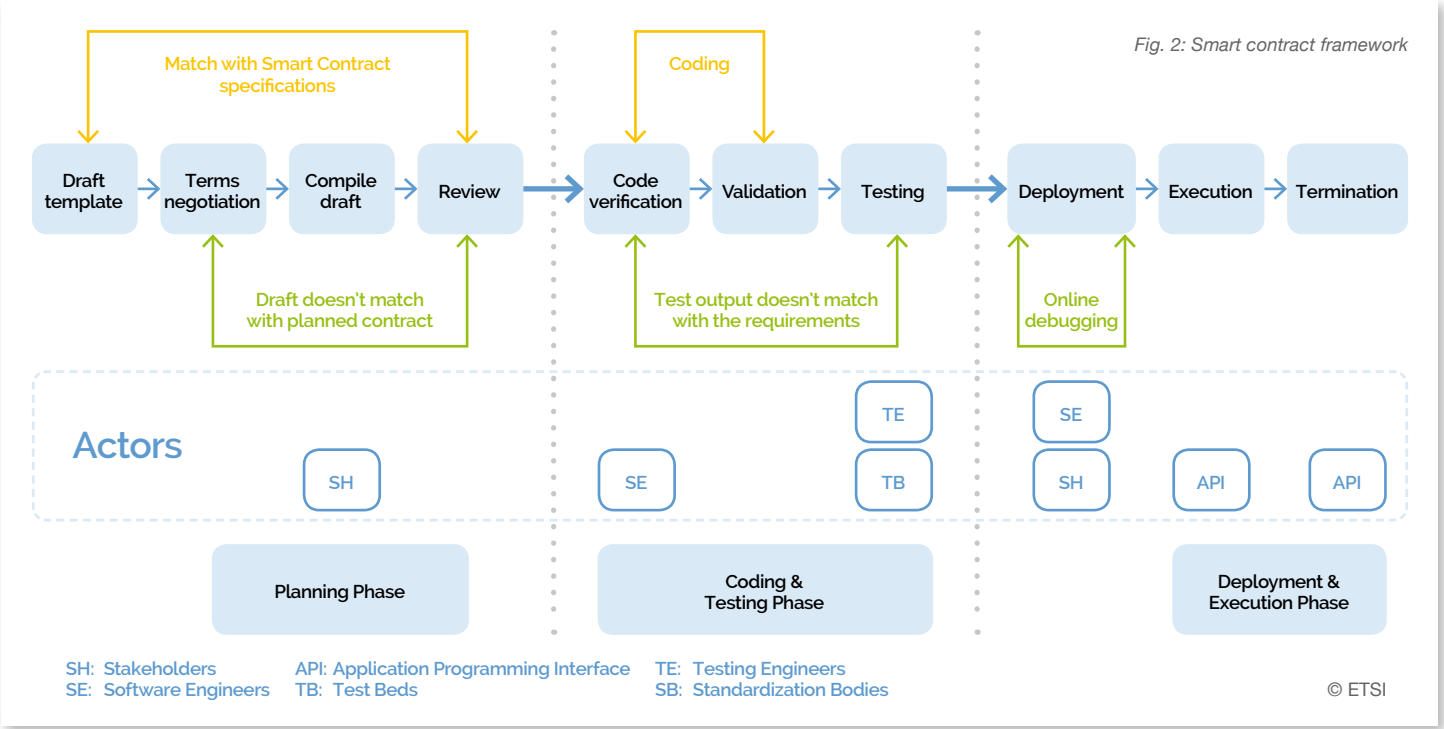


Fig. 2: Smart contract framework

a first set of documents, and a second term has recently started, 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.

Collaborative work

The ISG PDL works in tight coordination with other groups in ETSI and elsewhere, including open-source initiatives and a clear connection with research activities, especially the collaborative research projects within framework programmes such as Horizon 2020 and the future Horizon Europe. As in other ETSI ISGs on transformative technologies, the group work items are oriented to produce not only specifications of normative nature, but also informative deliverable in the form of technology reports and recommendations for future work, and, what is especially relevant in an environment so much populous as distributed ledger standardization, demonstrative deliverables focused on the execution of proof-of-concept demonstrations and on supporting early interoperability assessment events. Two of these proofs of concept have already been carried out.

Achievements

During its first term, the group started by addressing a *landscape document,* intended to identify current activities in standardization and research which are particularly relevant to the PDL activities. Apart from performing opportunities and gaps to address, this spawned a specific activity focused on the identification and collaboration of research projects, that has translated in the direct involvement of several of these projects willing to progress in the standardization of their results.

The group has produced another report as a result of examining the essential needs in terms of trust, security and effective conformity assessment, analysing *essential requirements* for PDL technology to ensure regulatory compliance to preserve security and privacy in the conduits providing the data to be incorporated into the ledgers. Work on applicability foundations was completed by another report describing potential *application scenarios* for the operation of PDLs, including provision models with special emphasis on 'as-a-service' paradigms, PDL infrastructure governance aspects, and identifying the definition of common terms to be used in our future standardization work.

The last work completed by the PDL group is a report on *smart contracts,* their components, planning, coding and testing. The scope of this report covers a reference architecture of the technology enabling smart contracts, the methods for engaging in a smart contract using this architecture, and a discussion on possible threats and limitations.

For its new term, the ISG PDL continues its work on ledger interoperability as a cornerstone for the operational framework and has already started working on key aspects such as the interaction with federated data frameworks and off-line operation. The group is committed to ensure the application of its principles and work items in new application environments, especially those enabled by the emergence of next-generation networking infrastructures, such as those related to resource trading at all levels, from compute nodes to spectrum, as well as new industrial scenarios.

■ *Diego Lopez, Chair ETSI ISG PDL*

5G Cellular IoT security in Rel-16

With the completion of Release-16, 3GPP SA3 has finished standardizing the security aspects of 5G Cellular IoT (CIoT). The work currently only comprises the E-UTRA radio access; with NR radio access to be available to CIoT in coming releases. However, in terms of security, 5G CIoT and 4G CIoT are on a par.

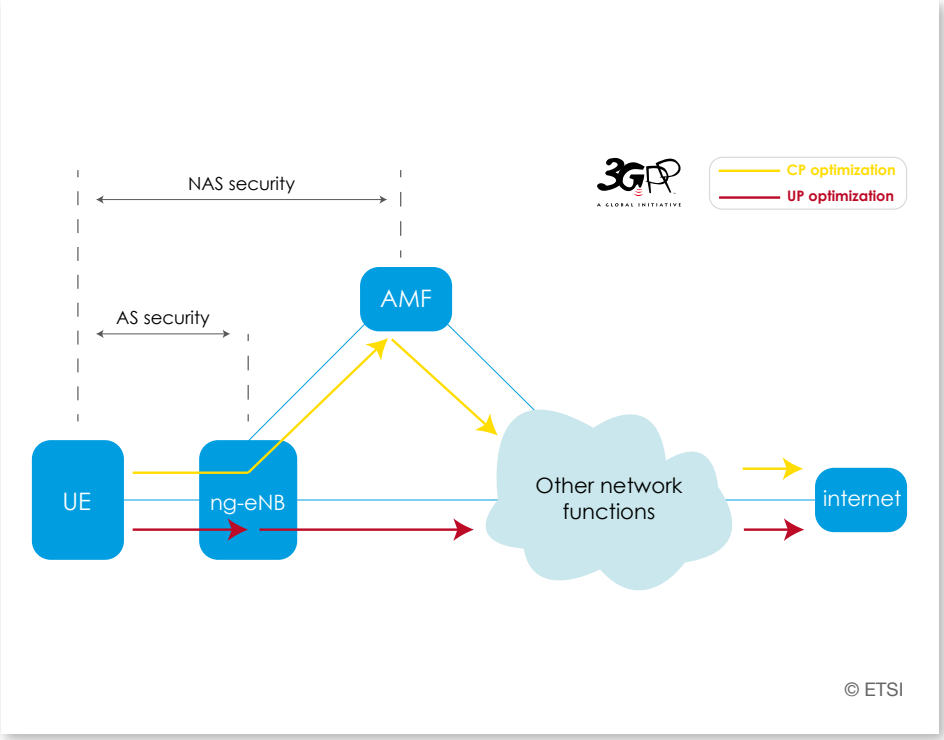
CIoT consists of a wide range of user equipment (UE), including smart meters and sensors, which are typically constrained in terms of battery consumption and data transfer volume. To overcome these constraints, there are two types of optimizations standardized by 3GPP.

Security handling in CP Optimization

In control plane (CP) optimization, the CIoT data is transferred between the UE and the core network in Non-Access Stratum (NAS) messages, i.e., Service Request, and uplink/downlink NAS transport messages. The security of these messages is achieved by using algorithms and keys from existing 5G NAS security context.

Security handling in UP Optimization

In user plane (UP) optimization, the CIoT data is transferred between the UE and the base station in Access Stratum (AS) messages, i.e., user plane packets. In uplink, the UE can send the CIoT data either separately or multiplexed with a control plane message called Resume Request. The latter is known as early data transmission (EDT). The user plane optimization is based on a special – so-called suspended – state in which the UE and the base station retain AS parameters including AS security context even when the UE is not actively communicating with the base station. The security of messages in this optimization is achieved by using algorithms and keys from existing AS security context.



Secure handling of RRC UE capability transfer

What is also worth noting in Release 16 is the additional requirements for the protection of the UE capability transfer in AS layer. Before running the RRC UE capability transfer procedure, the base stations should activate security. If the base station is running the RRC UE capability transfer procedure before activating AS security, then the base station shall not store these UE capabilities locally for later use and shall not send them to other network nodes. These requirements are set to ensure that tampered UE's capabilities are not perpetually affected.

The abovementioned security handlings are covered in Clauses 6.16 and 6.5.3 of 3GPP TS 33.501 - Security architecture and procedures for 5G system.

■ *Monica Wifvesson, 3GPP Working Group SA3 – Security and Privacy.*

A Standardized Roadmap for IoT Security

Security for the Internet of Things (IoT) covers a wide range of issues. oneM2M addresses the many facets of IoT security in a logical sequence.

Security for IoT is not as straightforward as encrypting the transmission of data between a sensor and an application. Deployed IoT systems are much more complex. Many involve large numbers of connected devices and sensors. Communications paths might involve multiple hopes via intermediate gateways, for example. Beyond the technical level, there are issues of remotely managing field devices in a secure manner. And there may be requirements to integrate equipment supplied by different vendors and their chosen technology protocols.

Three issues define IoT security

In developing standardized solutions for IoT security, it is important to work back from three key issues. The first is the proliferation of connection standards, device operating systems and use cases. Security has to work across a large number of permutations. As a result, IoT users need a standardized and systems-based approach.

Secondly, designers must presume that IoT devices and applications will operate as unattended applications. That involves designing security from the outset and automating many security functions.

Finally, IoT devices generally operate with long service lifecycles with limited scope for access or physical replacement. However, user expectations move as fast as the consumer market. Security needs to bridge these timing differences. This requires life-cycle management and cost-efficient security management tools which are more likely to result from standardization.

oneM2M's IoT Security Roadmap

oneM2M started to look at new requirements for IoT security well before the market caught on to these issues. Early work began in 2008, on remote provisioning for machine type devices, in 3GPP SA3. oneM2M took the early ideas into normative specification work. oneM2M's certificate-based credentials are now a fundamental part of the GSMA's eSIM specifications and solve the requirements for SIM-based credentials.

From a broader context, oneM2M addresses the many facets of IoT security in a logical sequence through its standardization roadmap. oneM2M Release 1 provided basic security features in the form of a common service function (CSF) that any IoT device or application entity can call upon. The security CSF enables Mutual Authentication to ensure that only legitimate applications can access resources and that applications can confirm that the requested resources are legitimate.

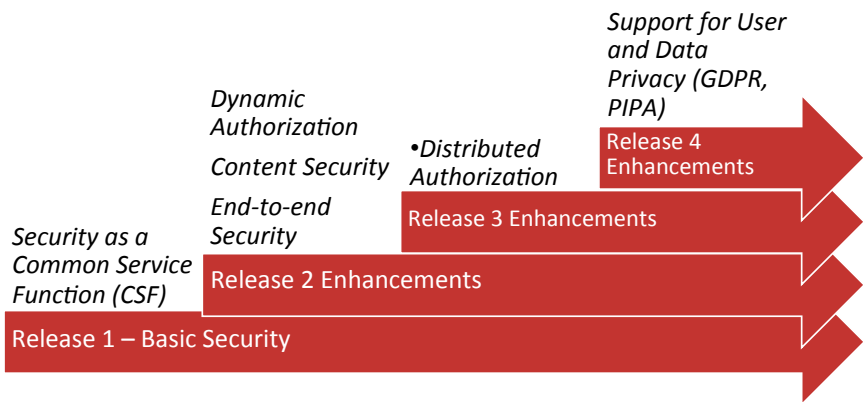
Release 2 added features to dynamically add and withdraw authorisation using tokens. Release 2 also added end to end encrypted set-up messages and message content, so that intermediate nodes in the path do not need to be trusted. This enables an end-to-end security framework allowing all nodes to be trusted so that they do not modify or leak the information being relayed.

Releases 3 and 4 add features for identifying and authorising human users with features to protect their privacy as required by local regulations, such as GDPR (Europe) and PIPA (Korea).

In parallel with standardizing a family of security capabilities for IoT systems, oneM2M is transposing its security specification into an ITU-T SG20 Y series for M2M Security and Privacy protection.

■ *Ms. Rana Kamill, BT*

Progressive Enhancement of IoT Security in oneM2M Standards



ETSI's Leadership in Unifying Identity Proofing Standards

Dating back to EESSI and then eIDAS, Europe has led the world in prioritising identity and maintaining the integrity of online transactions. That is because, even within the EU, transactions must ensure trust across borders, languages and cultures.

Amidst the COVID-19 pandemic, remote identity vetting moved to the forefront as organizations transitioned to teleworking while still needing to authenticate people for high-assurance purposes ranging from anti-money laundering (AML), know your client (KYC) to Qualified services.

Identity vetting is the process of verifying that the identity attributes of an applicant are accurately gathered, validated and evidenced. While there has been a blossoming of technology alternatives for remote vetting, there has also been debate over how to measure the 'equivalent assurance' to in-person proofing, which may have slowed adoption.

Identity Proofing, both real world and online

To develop an international standard that can increase reliability and auditability of identity proofing across providers and countries, ETSI's ESI Technical Committee assembled a Specialist Task Force (STF 588) to focus on identity proofing both in real life and online.

As a first step, the group analysed close to 50 international standards and their respective approaches related to identity proofing. From this, the committee created a valuable compendium, *ETSI TR 119 460,* which is a must read for those working in the field.

ETSI ESI then moved to create ETSI TS 119 461 (due to be published in mid-2021) laying out policy and security requirements and consistent standards for reliability and risk management across both face-to-face and virtual identification scenarios.

International Applicability

ETSI TS 119 461 will assist in providing consistent regulation of identity proofing by Qualified TSPs across Europe and set an important model for similar schemes worldwide. We believe it will also inspire the development and adoption of new technologies and services for eID by clarifying the rules of the road.

More importantly, it will help democratise access for individuals and businesses to take advantage of high-assurance online services by removing friction in enrolling. With new remote vetting options, people will no longer need to register in-person but can complete identity vetting at a time and place convenient to them.

Relying Parties, regulators, and Conformance Assessment Bodies will also benefit from more consistent understanding of the quality of validation across TSPs and supervisory regimes.

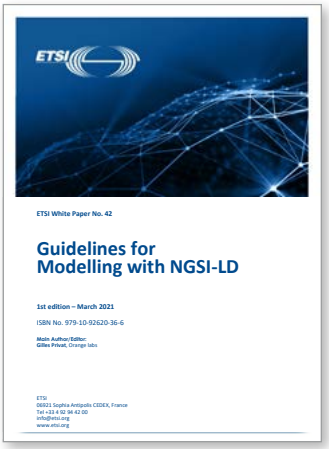
DigiCert is an active participant in ETSI, and we believe ETSI TS 119 461 is a forthright step to acknowledge that new tools and approaches will rapidly evolve for identity proofing, and it lays out a tech-neutral approach to bring them into the fold of trust services requirements.

Remote work will continue well beyond the pandemic and ETSI's work provides standards leadership for identity proofing that the rest of the world can follow.

■ *Stephen Davidson, Governance, Risk and Compliance at DigiCert and Chair of CA/Browser Forum S/MIME Certificate Working Group.*

White Paper:
Modelling with NGSI-LD

This ETSI White Paper is intended to complement the NGSI-LD information model *ETSI GS CIM 006.* It provides a set of practical guidelines on how to model a domain-specific system, process, or environment, how to associate entity instances to types/classes, how to use relationships and properties. These guidelines are based on both the NGSI-LD meta-model and the NGSI-LD cross-domain ontology as a common denominator set of classes cutting across domain-specific ontologies and taxonomies.



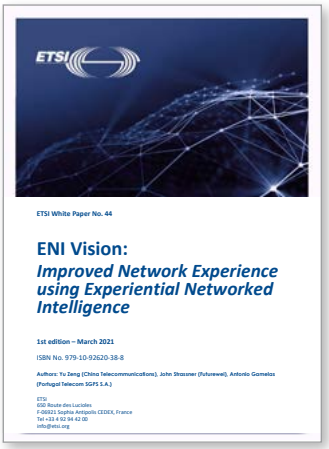
This White Paper is also intended to be complementary to the NGSI-LD Primer described in ETSI GR CIM 008, which mainly explains how to use the NGSI-LD API (e.g. creating or updating entity instances, queries, subscriptions, etc.) in a more "hands-on" practical way, especially for the initial use cases considered.

Webinar:
ETSI DECT 2020

This webinar introduces the newly released ETSI standard: DECT-2020 NR. It fills a gap currently in the IoT connectivity environment; it addresses industrial applications requiring either or both massive scale (mMTC) and/or ultra-reliable low latency (URLLC), complementing today's 5G technology. The technology enables simple deployment and very cost-efficient operation, demanded by various industries such as logistics and asset tracking, industry 4.0 and building automation as well as condition monitoring. Thanks to its ultra-reliable autonomous and automatic operation, there is no need for network infrastructure nor for a network operator. It can be deployed anywhere by anyone in no time. Listen to the recorded version there: *https://www.brighttalk.com/webcast/12761/453117*

White Paper:
Experiential Networked Intelligence

The Experiential Networked Intelligence Industry Specification Group (ENI ISG) is defining a Cognitive Network Management architecture, using Artificial Intelligence (AI) techniques and context-aware policies to adjust offered services based on changes in user needs, environmental conditions, and business goals. It therefore fully benefits the 5G networks with automated service provision, operation, and assurance, as well as optimized slice management and resource orchestration. ENI has also launched Proof of Concepts (PoCs) aiming to demonstrate how AI techniques can be used to assist network operation including 5G.



This White Paper provides guidance for ENI's future development and overview of the current ENI publications.

Webinar:
OSM Release NINE

This webinar offers an overview of the recently announced Open Source MANO Release NINE, and some of its latest features. OSM Release NINE completes the native adoption of ETSI NFV standardized YANG Data Models (ETSI NFV-SOL006), ensuring a consistent standardized and interoperable way to describe network functions and services, allowing them to be deployed in any Telco Cloud and orchestrated by any SOL006 compliant orchestrator. This release also improves the use of VNF Operations, providing a more efficient and scalable way to manage network functions in Kubernetes, and allowing to distribute the agents managing VNF/CNF operations (Juju Proxy Charms) across different types of clouds; bringing higher resiliency to highly distributed edge deployments.Listen to the recorded version there: *https://www.brighttalk.com/webcast/12761/465808*

Registered Electronic Mail
for modern Electronic Registered Delivery Services

The digital economy in a virtuous and mature digital market requires appropriate measures to address both "interoperability" and "cybercrime-fighting", as learnt from the principles and scope of the eIDAS regulation.

Interoperability is not an easy matter. The standards create the preconditions and constitute the foundation whereby some form of interoperability can be realized.

The set of ETSI standards regarding the *Electronic Registered Delivery Services* (ERDS) arise for such purpose. In particular, *the standard ETSI Registered Electronic Mail (REM) Services* is a specific type of ERDS which builds on the formats, protocols and mechanisms used in ordinary e-mail messaging. ETSI defines the so-called "REM baseline" consisting in the minimum set of technical rules to follow in order to achieve a cross-border interoperability. Both persons and applications, belonging to different and independent organizations and in any country, can easily and rapidly converse in a secure and effective way. The conformity to the REM baseline allows the implementation of a "digital backbone" on top of which the contribution from evolved or collateral services can be added, going forward.

The concept of "evidence" provides proof of sending and receiving the data and protects transmitted data against any unauthorized alterations. Evidence can be seen as a declaration by a trusted party that a specific event related to the delivery process happened at a certain time. Once it is well established, on top of it, several new services can be defined and implemented, on various protocols and obeying different paradigms. The REM baseline represents a great opportunity to achieve this goal.

Broad adhesion to the implementation of the REM baseline and substantial participation in the ETSI REM Plugtests Event - scheduled from 31 May to 18 June 2021 - will provide the final round of the ETSI REM standard and a well-founded starting point for the concretization of new modern ERDS services.

■ *The REM Plugtests team.*

Online tool to assess conformity of Advanced Electronic Signatures

ETSI's Centre for Testing and Interoperability (CTI) provides a free online tool that performs numerous checks in order to verify the conformity of the ETSI Advanced Electronic Signatures. This project was performed in collaboration with UPC (Universitat Politècnica de Catalunya).

The tool performs conformance tests on:

- XAdES (XML Advanced Electronic Signature *ETSI 101 903, TS 103 171* and *EN 319 132-1&2*)
- CAdES (CMS Advanced Electronic Signature *ETSI TS 101 733* and *EN 319 122-1&2*)
- ASiC (Associated Signature Container *ETSI TS 102 918* and *EN 319 162-1&2*)
- PAdES (PDF Advanced Electronic Signature *ETSI TS 102 778* and *EN 319 142-1&2*)

It is worth noting that this is not a signature validation tool. It checks the structure of the AdES signature versus the ETSI Specifications. Furthermore, it cryptographically verifies the digital signature value, but it does not validate the certificate chain. This tool aims to help organizations that develop signing or validating tools.

Launched in 2015, the ETSI signature checker became more and more popular with 2100 registered participants. It was also a precious help in support of several Interoperability ETSI Plugtests on Digital signatures.

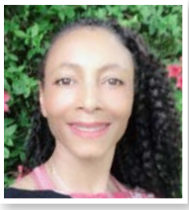
The success of this tool resulted in it officially being referenced as the signature conformance checker of the eSignature Building block of the CEF Digital program of the European Commission

https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eSignature

If you wish to get an account for the tool, see details on the portal *http://signatures-conformance-checker.etsi.org/*

■ *Laurent Velez, Technical Expert at ETSI's Centre for Testing and Interoperability.*

Welcome to our new staff member



Carolyn Taylor
Technical Officer, Mobile Competence

From the US to the UK, via Covid-19 and Brexit, it took 1 year for Carolyn to join ETSI since her first hiring interview. Saying she was motivated is an understatement. Born in Chicago, Carolyn is a seasoned standardization professional. Her first experience dates back to 1999 when she was expatriated from Motorola as a Technical Expert in ETSI. Back to Motorola US, where she stayed for nearly 7 years, she became the Vice Chair of 3GPP RAN5 and continued her career representing ZTE handset and Network divisions for 11 years in several 3GPP RAN WGs then a brief moment with Samsung UK. During her Electrical Engineering undergraduate studies, she was part of an internship programme in Motorola, obtained a NASA scholarship and was trained as an Army Reserve Officer, where she went to several countries including Korea and Germany. She obtained Senior Membership of the IEEE and acquired her PhD through an adult programme while at ZTE and got the opportunity to travel to different ZTE businesses within China. She received a Chinese Language Certificate along the way. Positive thinking is her way of life, she will no doubt be a real asset to ETSI.

Join us at upcoming virtual events that are either organized or supported by ETSI.

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

April 2021

Layer123 Europe, 360° Network Automation Congress

13-14 April, Virtual Event

ETSI, in partnership with Layer123, is delighted to bring an 'ETSI Perspective Day' to *virtual attendees on 12 April.* Several ETSI groups, namely ZSM (Zero touch network and Service Management), NFV (Network Function Virtualization), Multi-Access Edge Computing (MEC), as well as INT (Core Network and Interoperability Testing) will provide a status update of their activities focusing on a network automation perspective. The 'ETSI Perspective Day' will conclude with a joint group wrap-up panel. All presentations will be given live and allow for audience questions.

Fortinet 5G Security Digital Summit

20-21 April, Virtual Event

ETSI's CTO, Adrian Scrase, will bring an ETSI perspective to Fortinet's 5G Security Digital Summit, focusing on enabling industrial adoption. He will participate as a panellist in the general session's discussion panel, touching upon high level, strategic topics around 5G for enterprises/industry verticals and the role of security within this ecosystem.

FutureNet World 2021

20-21 April, Virtual Event

ETSI is pleased to endorse and actively contribute to *FutureNet World 2021,* showcasing some of the most innovative technology solutions in an ever expanding and complex ecosystem. The virtual event provides a unique opportunity to meet and build relationships with industry pioneers, from start-ups to technology giants.

Telecom TV DSP Leaders Summit: Special Report on NFV Evolution – brought to you by ETSI

21 April, Live - Virtual Event

ETSI is proud to bring you an interactive virtual event on the topic of NFV Evolution. In partnership with TelecomTV, as part of their *DSP Leaders Summit Series,* join this Special Report on NFV Evolution, brought to you by ETSI: 'The NFV Journey: the Road Ahead', broadcasting live on 21 April 2021, 3-5pm CET, in virtual format. Prior to the event, on-demand videos of technical presentations will be available online and the audience is invited to leave comments and raise questions on these presentations. The event will feature two panel discussions where distinguished experts will follow-up on these presentations, share their viewpoints and interact with the audience.

April 2021

ETSI IoT Week 2021

26-30 April, Virtual Event

The 2021 edition of the well-established *ETSI IoT Week* will take place in virtual format on 26-30 April 2021. We aim to bring you rich technical content coupled with high interactivity to ensure networking amongst the audience and our speakers. Save the date!

May 2021

OSM 11 Hackfest

31 May - 4 June 2021, Virtual Event

The event will be run remotely, allowing participants to join the hands-on sessions from home. It will offer a great opportunity to share and learn with the OSM community members, users, developers and module leaders, and explore opportunities for synergies and collaboration. The main purpose of this OSM Hackfest event is to allow OSM users to get familiar and discover the latest features in OSM Release NINE while they deploy and test a meaningful use case. In addition, experienced users and developers will have the opportunity to hack into OSM, build complex examples, fine-tune, test and demonstrate experimental features on the OSM Remote Labs network.

REM Plugtests

31 May - 18 June 2021, Virtual Event

ETSI's Centre for Testing and Interoperability is preparing the REM Plugtests (Registered Electronic Mail). This first edition of the Plugtests event will focus on the EN 119 532 series. The format of the event will be remote live testing and REM evidence format remote verification using a dedicated Plugtests portal.

June 2021

ETSI Security Week 2021

14-18 June 2021, Virtual Event

ETSI's flagship annual event is going virtual! As ever, the event will focus on the latest security hot topics - but this new virtual format allows for even more diverse participation from around the globe. ETSI's security groups will deliver 10 virtual sessions spread across five topics: AI security, Network Function Virtualization, IoT security, mobile edge computing and Cyber Security Policy. Save the date now for this unique event!

FRMCS

14-18 June 2021, Virtual Event

ETSI with the support of TCCA (The Critical Communications Association) and the UIC (Union Internationale des Chemins de fer), is organising the first *FRMCS* (Future Railway Mobile Communication System) Plugtests™ remote event. The goal of this event is to validate the interoperability of a variety of implementations using different test scenarios based on the 3GPP Mission Critical services framework with focus on the rail specific features, which will also be used for Mobile Communication System for Railways. Interoperability and Mission Critical service harmonisation are critical challenges for the successful deployment and operation of Mobile Communication System for various sectors, including Railways.

ETSI SNAPSHOT

913 *members* end of March

26% *SMEs*

+100 *technical groups*

543 *standards* Dec-.2020-Feb2021

697 *standards under development*

3.262 *standards' downloads* Dec-.2020-Feb2021

1.441 *eMeetings* Dec-.2020-Feb2021

40.561 *online participants* Dec-.2020-Feb2021

78 *partnerships*

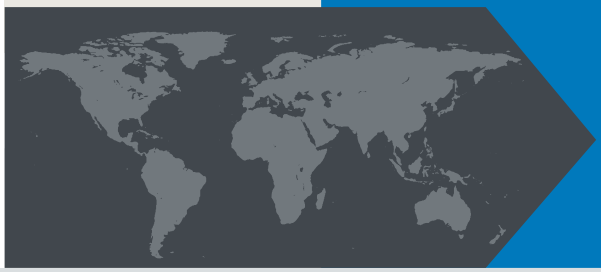
8 *conferences & Plugtests* Dec-.2020-Feb2021

@ETSI Secretariat

127 *people*

16 *nationalities*

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



Members from 62 countries

About ETSI

ETSI provides members with an open and inclusive environment to support the development, ratification and testing of globally applicable standards for ICT systems and services across all sectors of industry and society. We are a not-for-profit body with more than 900 member organizations worldwide, drawn from over 60 countries and five continents. Members comprise a diversified pool of large and small private companies, research entities, academia, government and public organizations. ETSI is 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: