ETSI

Cybersecurity & 3GPP

Anthony Brand
CMO

anthony.brand@etsi.org

April 2024

Bringing people together at ETSI …

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

©ETSI 2024 – All rights reserved

ETSI in a nutshell

- ETSI members: 895 from 64 countries, including 23% SME/micro-enterprises and 15% universities/research bodies
- Technical groups/working groups: 100+
- Publications issued in 2023: 1 812
- Publications to date: 58 550
- Standards downloads in 2023: 19 975 000
- Plugtests interoperability events: 8
- Partnerships: 108
- ETSI Secretariat: 127 people / 25 nationalities

©ETSI 2024 – All rights reserved

… to work collectively…

- Openly
- Transparently
- Based on Consensus

Collective work

- ETSI standards are the result of the work of, and reviews from, many different ETSI members

©ETSI 2024 – All rights reserved

… in TC CYBER…

Technical Committee on Cybersecurity (TC CYBER)

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

©ETSI 2024 – All rights reserved

… and in many other groups…

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

©ETSI 2024 – All rights reserved

… using a holistic approach…

Threat Analysis / Risk Assessment

Definition of security requirements

Test/assessment specification

©ETSI 2024 – All rights reserved

… and collaborating with others (1)

Radio Equipment Directive
Cybersecurity Act
NIS Directive
GDPR
eIDAS
Cyber Resilience Act

Generic cybersecurity matters
eIDAS
Certification scheme (e.g. 5G)
Security of AI

CEN/CLC/JTC 13
CLC/TC 65x

ISO/IEC JTC 1 SC 27

©ETSI 2024 – All rights reserved

… and collaborating with others (2)

…

©ETSI 2024 – All rights reserved

.. to develop world class standards for …

CROSS-DOMAIN CYBERSECURITY (TC CYBER)

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

SECURING TECHNOLOGIES & SYSTEMS

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

EVOLVING SECURITY TOOLS & TECHNIQUES

- Lawful interception & retained data
- Digital signatures & trust services
- Permissioned distributed ledgers
- Smart cards / secure elements
- Security algorithms
- Quantum key distribution
- Quantum-safe cryptography
- Encrypted Traffic Integration

©ETSI 2024 – All rights reserved

… and in ETSI TC CYBER Key areas of Work

Cybersecurity ecosystem

Consumer IoT and Mobile Security and Privacy

Protection of personal data and communication

Network Security

Cybersecurity for Critical Infrastructures

Enterprise/organization and individual cybersecurity

Forensic activities

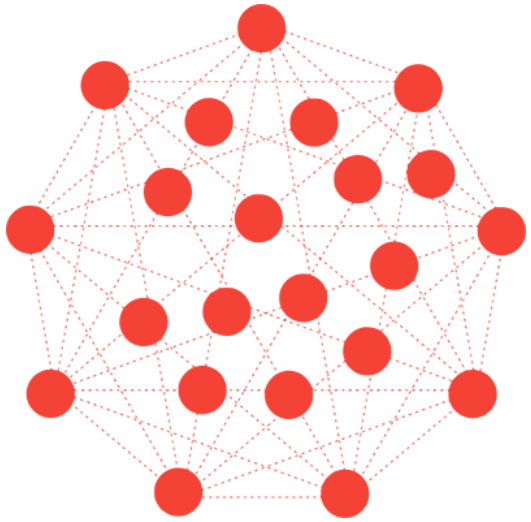
Cybersecurity tools

Direct support to EU legislation

Quantum-Safe Cryptography

©ETSI 2024 – All rights reserved

Consumer Mobile and IoT security and privacy



EN 303 645/TS 103 645 supports a good security baseline for internet-connected consumer products, provisioning a set of 13 provisions, with the top three being:

- no default passwords,
- implement a vulnerability disclosure policy,
- and keep software updated.

This baseline deliverable is complemented with an assessment specification and an implementation guide, all detailed on the Consumer IoT security page.

In addition, TC CYBER has worked on a smart door lock vertical standard, based on ETSI EN 303 645.

TC CYBER has also developed and continues working on a Common Criteria Protection Profile for consumer mobile devices focusing on devices with high computation power and rich user interface such as smart phones and tablets (TS 103 732).

Other IoT work in TC CYBER includes a report on Critical Security Controls (TR 103 305-3), which is applicable to IoT.

©ETSI 2024 – All rights reserved

TC ESI – Digital signatures and Trust Services Standards Framework

Trust Services (eIDAS)

Signature-enhanced Services

New Trust Services (eIDAS 2)

- e-Attributes
- e-Ledgers
- e-Archiving

Signature creation & validation formats and procedures

Signing Devices

Crypto Suites

EU Digital Identity Wallet

©ETSI 2024 – All rights reserved

Addressing new technologies

Quantum technologies

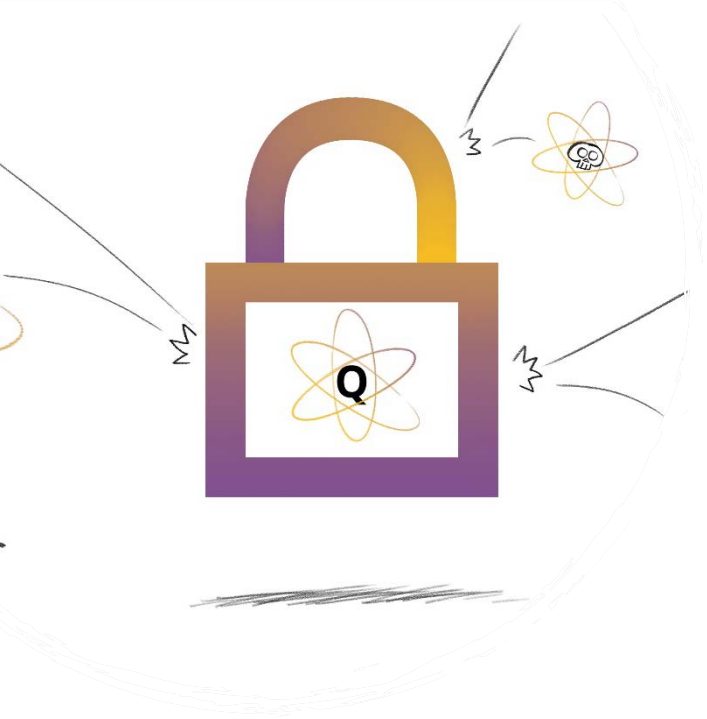
- Quantum Key Distribution (QKD)
- Quantum-Safe Cryptography (QSC)

Artificial Intelligence

- Securing AI from attacks
- Mitigating against AI
- Using AI to enhance security measures against attacks from other things

…

©ETSI 2024 – All rights reserved



Quantum-Safe Cryptography (QSC)

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

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

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

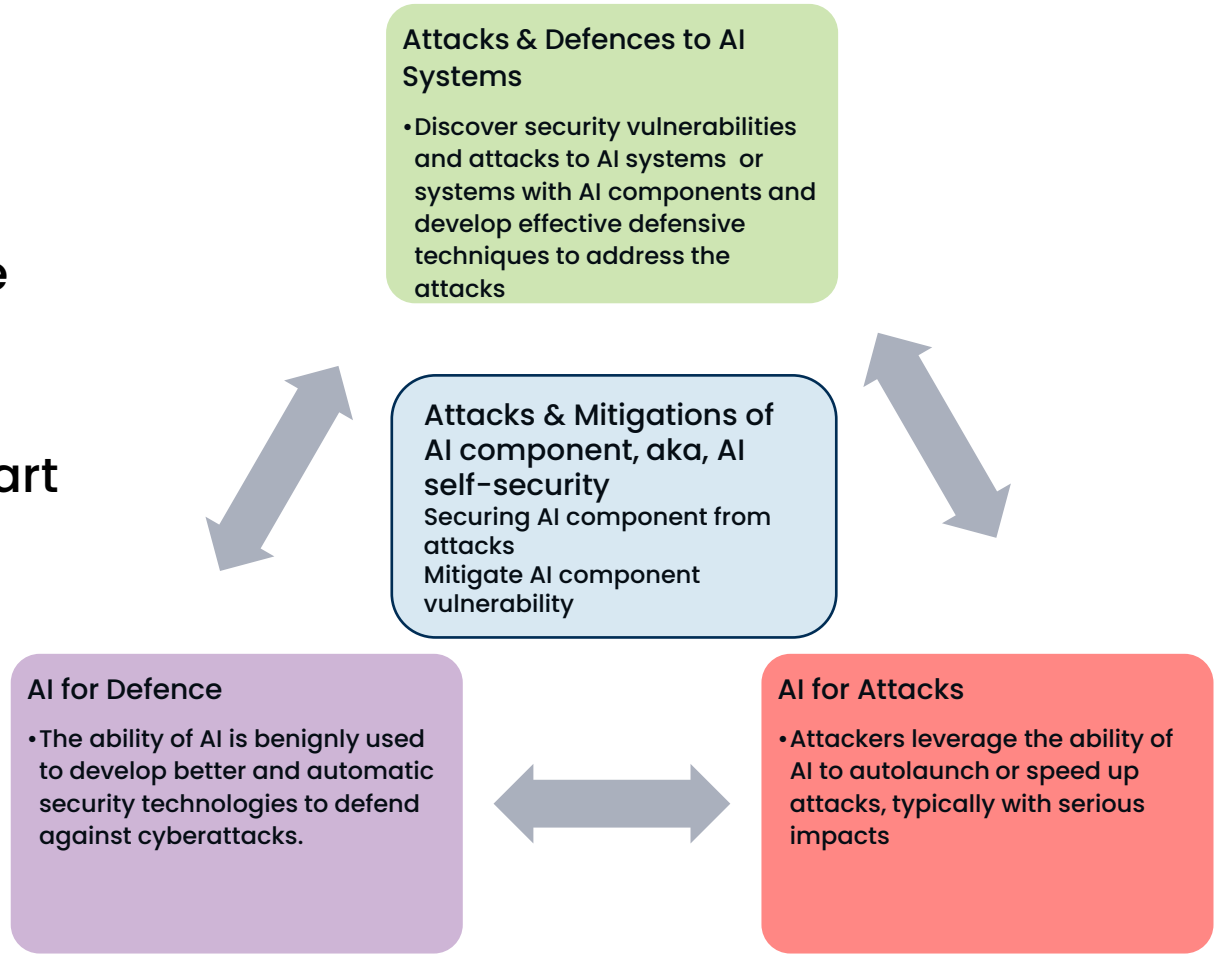
(Does not specify algorithms or key distribution techniques)

Now a working group of TC Cyber

©ETSI 2024 – All rights reserved

ETSI TC SAI Scope

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



©ETSI 2024 – All rights reserved

Supporting new EU policies and legislation

- Cybersecurity Act 5G scheme
- Proposed revised Directive on Security of Network and Information Systems (NIS 2)
- Proposed AI Act
- Proposed Regulation on a framework for a European Digital Identity (eIDAS 2)
- Proposed Cyber Resilience Act

©ETSI 2024 – All rights reserved

ETSI
The Standards People

Introducing 3GPP

What is 3GPP (and what is it not)?

- It is …
  - Comprised of 7 regional and national Standards Development Organizations (SDOs) from around the globe.
- It is populated by …
  - Delegates representing 797 member organizations of those SDOs.
  - Delegates of the SDOs themselves.

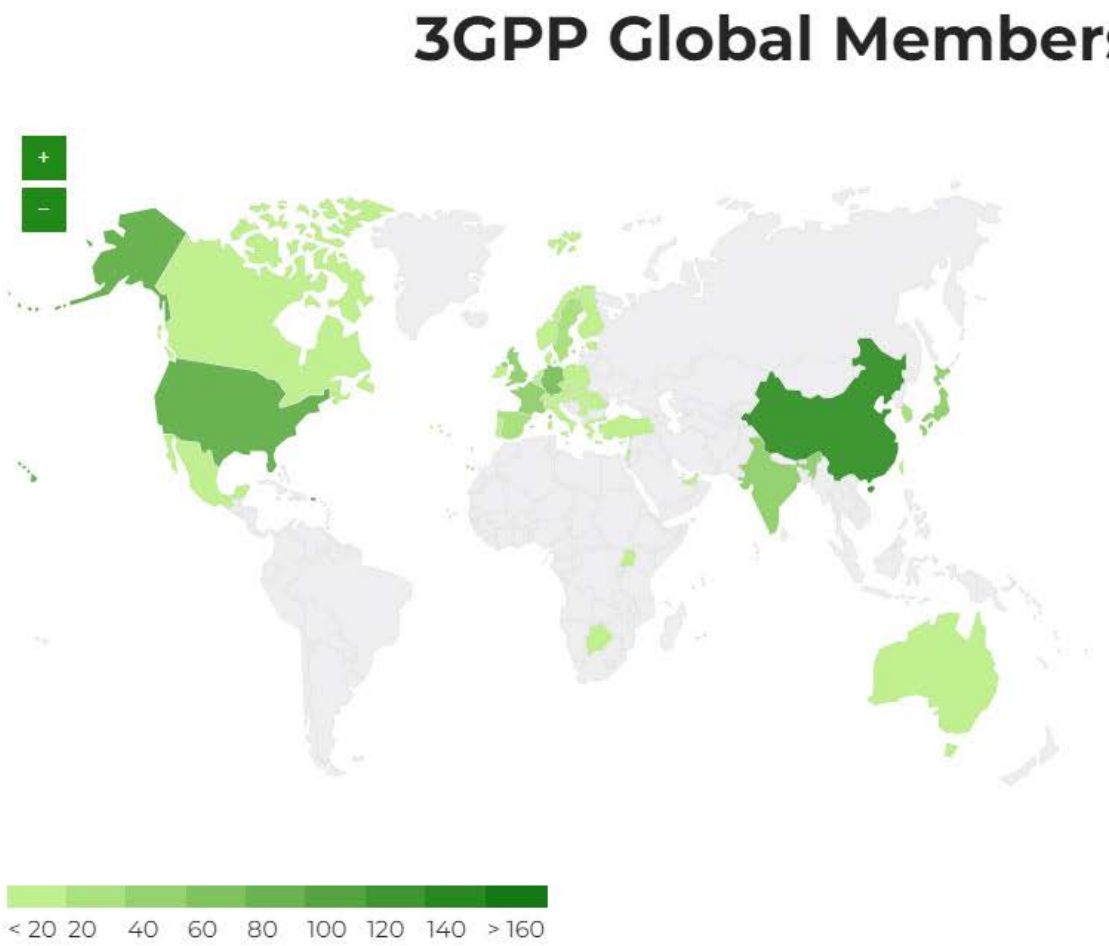
©ETSI 2024 – All rights reserved

What is 3GPP (and what is it not)?

- It is **not** …
  - A government agency
  - A regulatory body
  - An arm of the ITU or the United Nations
  - An arm of the EU or of CEPT
  - A certification body
  - A frequency-allocation body
  - A legally constituted entity

©ETSI 2024 – All rights reserved

3GPP Membership



41

Countries

797

Organizational Partner Members

6723

Number delegates at meetings this year

116

3GPP Meetings per year

4242

3GPP Specifications

ARIB

atis

CCSA

ETSI

tsdsi
India's Telecom SDO

TTA

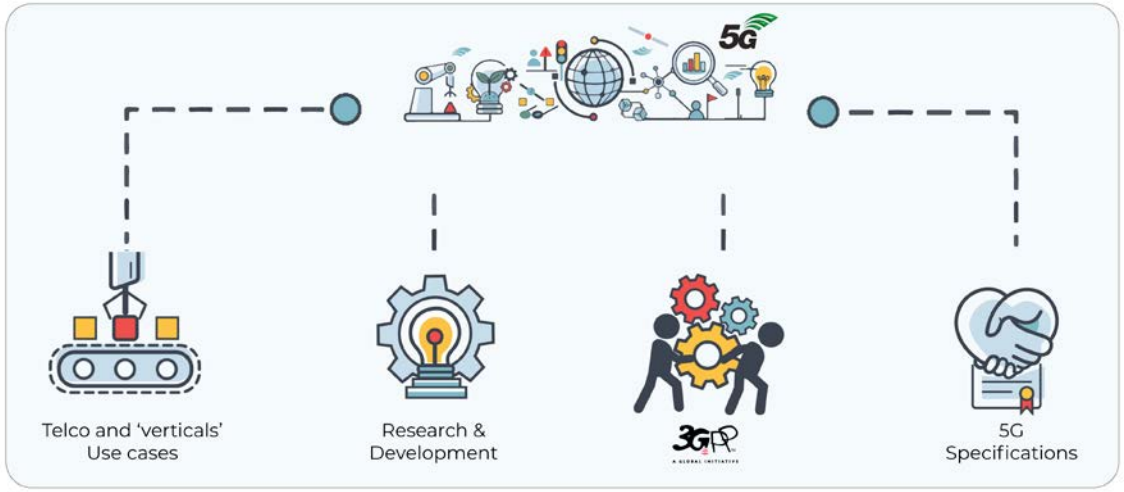
TTC Telecommunication Technology Committee

https://www.3gpp.org/about-us/partners

The role of 3GPP

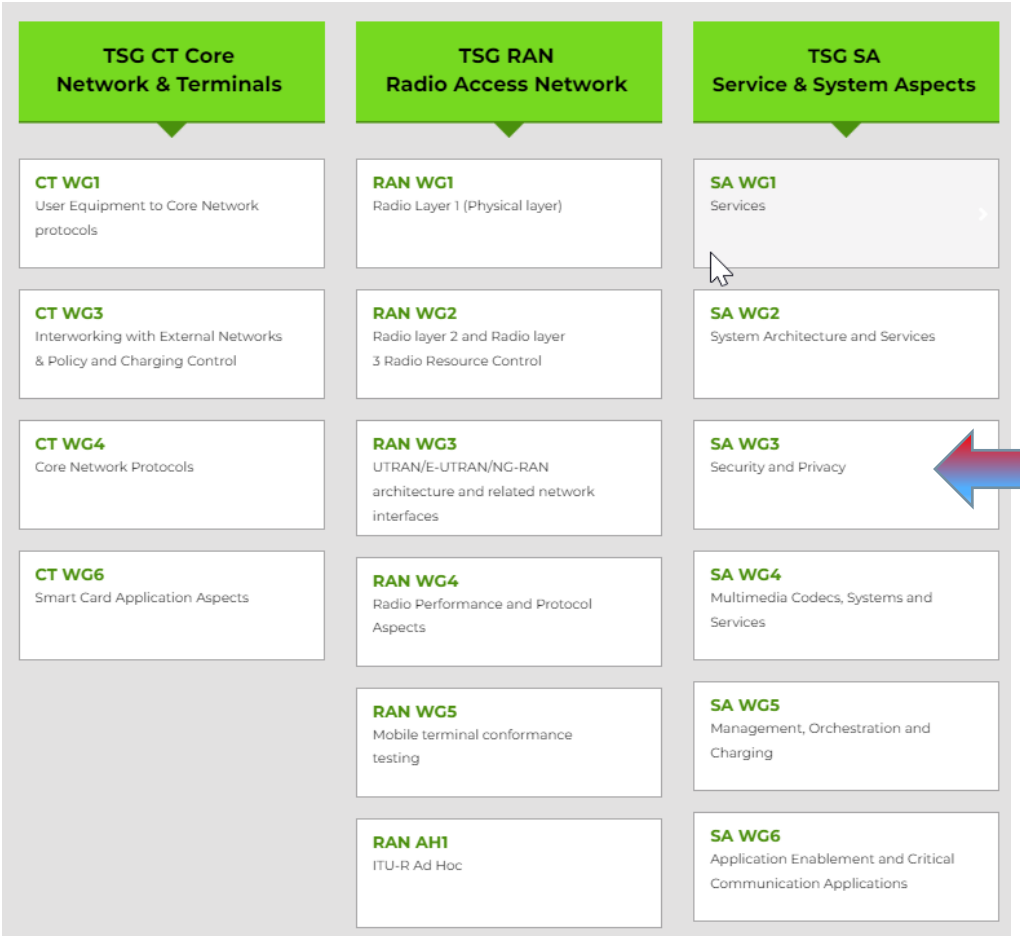
Part of the invention, proof of concept, **standardization**, trials, commercialization …cycle

- Specifications and Studies providing a complete **system description** for mobile telecommunications
- The system description is characterized by a number of **standardized interfaces**. It is **not** a description of a standardized **deployment**
- This standardization effort enables an interoperable, multi-vendor approach to deployment and generates mass market economies of scale, without stifling innovation



Technical Specification Groups

- The TSGs prepare, approve and maintain the 3GPP Technical Specifications and Technical Reports.
- They are responsible for the detailed time frame and management of the work's progress;
  - Management of work items;
  - Technical Co-ordination;
  - Proposal and approval of work items within the agreed scope and terms of reference of the TSG
- The TSG Chair is responsible for the overall management of the technical work within the TSG and its Working Groups.
- The WG Chair is responsible for the overall management of the technical work within the WG and its sub-groups.



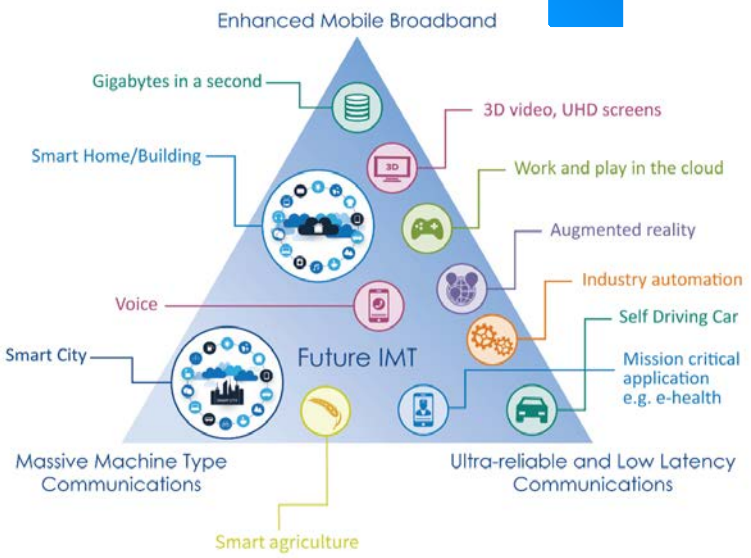
Bringing the work into the groups

Use Case diversity

- High or Low data rates
- Higher user mobility
- Improved coverage

Overall System Goals

- Enable new business
- Greater efficiency
- More flexibility – not one-size-fits-all



3GPP Working Groups

TSG CT Core Network & Terminals	TSG RAN Radio Access Network	TSG SA Service & System Aspects
CT WG1 User Equipment to Core Network protocols	RAN WG1 Radio Layer 1 (Physical layer)	SA WG1 Services
CT WG3 Interworking with External Networks & Policy and Charging Control	RAN WG2 Radio layer 2 and Radio layer 3 Radio Resource Control	SA WG2 System Architecture and Services
CT WG4 Core Network Protocols	RAN WG3 UTRAN/E-UTRAN/NG-RAN architecture and related network interfaces	SA WG3 Security and Privacy
CT WG6 Smart Card Application Aspects	RAN WG4 Radio Performance and Protocol Aspects	SA WG4 Multimedia Codecs, Systems and Services
	RAN WG5 Mobile terminal conformance testing	SA WG5 Management, Orchestration and Charging
	RAN AH1 ITU-R Ad Hoc	SA WG6 Application Enablement and Critical Communication Applications

3GPP Specifications and Reports:	
Requirements	21 series
Service aspects ("stage 1")	22 series
Technical realization ("stage 2")	23 series
Signalling protocols ("stage 3") - user equipment to network	24 series
Radio aspects	25 series
CODECs	26 series
Data	27 series
Signalling protocols ("stage 3") -(RSS-CN) and OAM&P and Charging (overflow from 32.- range)	28 series
Signalling protocols ("stage 3") - intra-fixed-network	29 series
Programme management	30 series
Subscriber Identity Module (SIM / USIM), IC Cards. Test specs.	31 series
OAM&P and Charging	32 series
Security aspects	33 series
UE and (U)SIM test specifications	34 series
Security algorithms	35 series
LTE (Evolved UTRA), LTE-Advanced, LTE-Advanced Pro radio technology	36 series
Multiple radio access technology aspects	37 series
Radio technology beyond LTE	38 series

What is 3GPP SA3 working on?

Security Assurance Specifications (SCAS) for 3GPP network functions

- Test cases for a variety of 3GPP network functionalities.
- They will be an important part of the future 5G Security Certification.

256-Bit encryption algorithms for 5G/6G

- Recently approved, they will make **5G** advanced and **6G** more resilient against future attacks like those based on Quantum Computing mechanisms.

Security of Ambient IoT services

Security of AI/ML (Artificial Intelligence/ Machine Learning)

Security of Energy Serving

Security of 5G Mobile Metaverse services

Security of 5G Satellite access

Mitigation against bidding down attacks

Security of Non-Public networks (NPN)

©ETSI 2024 – All rights reserved

Get involved

- ETSI has 51 Technical areas for activities.
- ETSI membership enables membership of both 3GPP and oneM2M
- ETSI members gain unlimited access and participation in all active Technical Groups and Partnership Projects
- Through ETSI Membership, organisations enhance their reputation, competitiveness and professional network
- Gain valuable information from members, locally and internationally

©ETSI 2024 – All rights reserved

Any further questions?

Contact:

info@etsi.org

Anthony.brand@etsi.org

Claire.desclercs@etsi.org