



聽聽3GPP 怎麼說

漫談TS(R) .33

Shin Li

3GPP

3GPP [編輯]

維基百科，自由的百科全書



此條目需要更新。 (2018年6月19日)

請更新本文以反映近況和新增內容。完成修改時，請移除本模板。

第三代合作夥伴計劃（英語：**3rd Generation Partnership Project**，即**3GPP**）是一個成立於1998年12月的標準化機構。目前其成員包括歐洲的ETSI、日本的ARIB和TTC、中國的CCSA、韓國的TTA、北美洲的ATIS和印度的電信標準開發協會。

3GPP的目標是在國際電信聯盟的IMT-2000計劃範圍內製訂和實現全球性的（第三代）行動電話系統規範。它致力於GSM到UMTS（W-CDMA）的演化，雖然GSM到W-CDMA空中介面差別很大，但是其核心網採用了GPRS的框架，因此仍然保持一定的延續性。

3GPP和3GPP2兩者實際上存在一定競爭關係，3GPP2致力於以IS-95（在北美和韓國應用廣泛的CDMA標準，中國電信CDMA與之相容）向IS-2000過渡，和高通公司關係更加緊密。

<https://zh.wikipedia.org/wiki/3GPP>

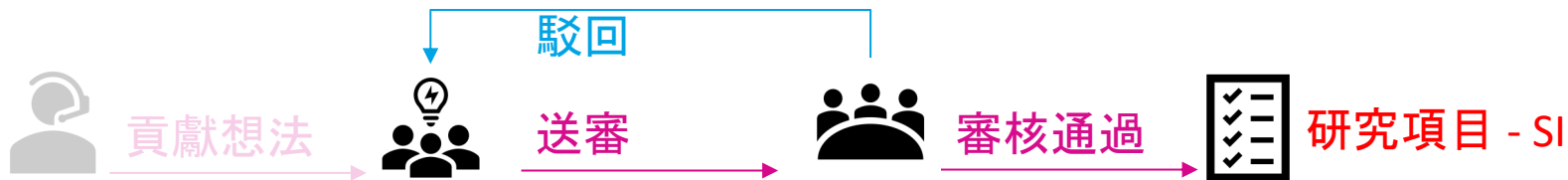


Phase 1 : 早期研發

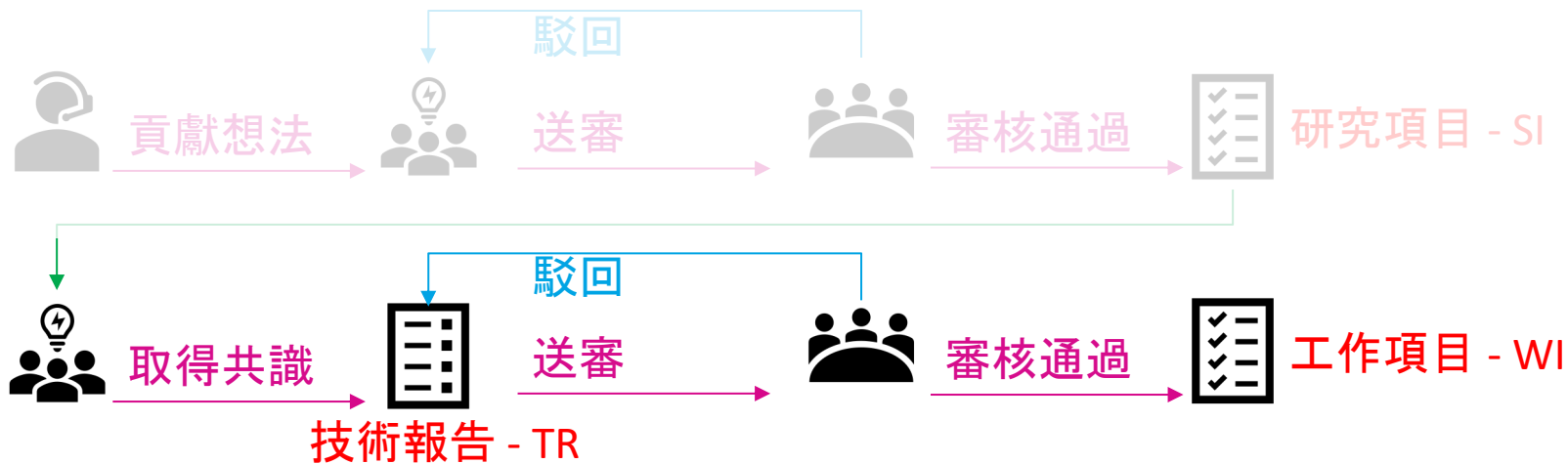


貢獻想法

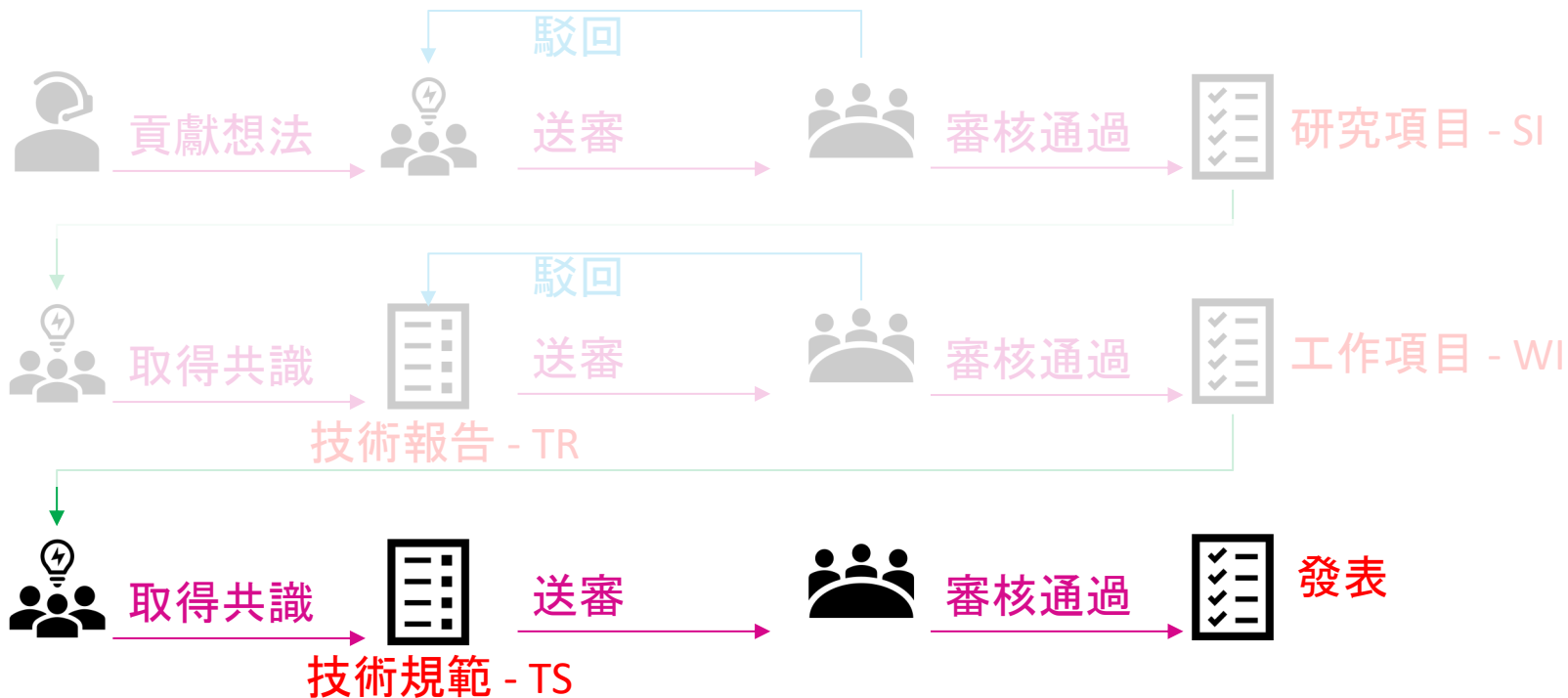
Phase 2 : 提案



Phase 3 : 可行性評估



Phase 4 : 技術規範

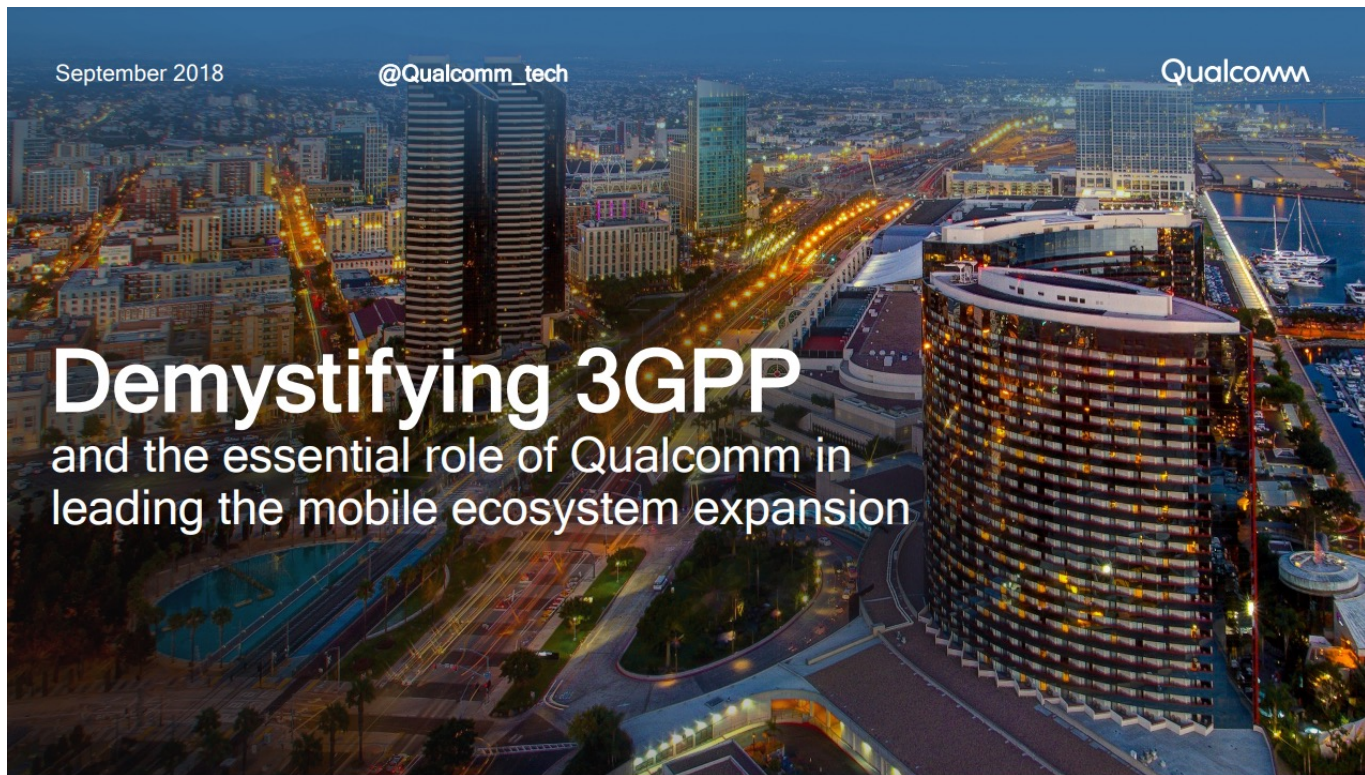




More about 3GPP

Demystifying 3GPP

<https://www.qualcomm.com/documents/demystifying-3gpp>



All specification series in 3GPP

SUBJECT OF SPECIFICATION SERIES	3G AND BEYOND / GSM (R99 AND LATER)	GSM ONLY (REL-4 AND LATER)	GSM ONLY (BEFORE REL-4)
General information (long defunct)	00 series		
Requirements	21 series	41 series	01 series
Service aspects ("stage 1")	22 series	42 series	02 series
Technical realization ("stage 2")	23 series	43 series	03 series
Signalling protocols ("stage 3") – user equipment to network	24 series	44 series	04 series
Radio aspects	25 series	45 series	05 series
CODECs	26 series	46 series	06 series
Data	27 series	47 series (none exists)	07 series
Signaling protocols ("stage 3") –(RSS-CN) and OAM&P and Charging (overflow from 32.- range)	28 series	48 series	08 series
Signaling protocols ("stage 3") – intra-fixed-network	29 series	49 series	09 series

All specification series in 3GPP

SUBJECT OF SPECIFICATION SERIES	3G AND BEYOND / GSM (R99 AND LATER)	GSM ONLY (REL-4 AND LATER)	GSM ONLY (BEFORE REL-4)
Program management	30 series	50 series	10 series
Subscriber Identity Module (SIM / USIM), IC Cards. Test specs.	31 series	51 series	11 series
OAM&P and Charging	32 series	52 series	12 series
Access requirements and test specifications	13 series	13 series	
Security aspects	33 series		
UE and (U)SIM test specifications	34 series		11 series
Security algorithms (3)	35 series	55 series	(4)
LTE (Evolved UTRA) and LTE-Advanced radio technology	36 series	—	—
Multiple radio access technology aspects	37 series	—	—

All specification series in 3GPP

SUBJECT OF SPECIFICATION SERIES	3G AND BEYOND / GSM (R99 AND LATER)	GSM ONLY (REL-4 AND LATER)	GSM ONLY (BEFORE REL-4)
Program management	30 series	50 series	10 series
Subscriber Identity Module (SIM / USIM), IC Cards. Test specs.	31 series	51 series	11 series
OAM&P and Charging	32 series	52 series	12 series
Access requirements and test specifications	13 series	13 series	
Security aspects	33 series		
UE and (U)SIM test specifications	34 series		11 series
Security algorithms (3)	35 series	55 series	(4)
LTE (Evolved UTRA) and LTE-Advanced radio technology	36 series	—	—
Multiple radio access technology aspects	37 series	—	—

TS.33

[About 3GPP](#)
[Specifications Groups](#)
[Specifications](#)
[3GPP Calendar](#)
[Technologies](#)
[News & Events](#)
[Home](#)
[Sitemap](#)
[Contact](#)

3GPP Specification series

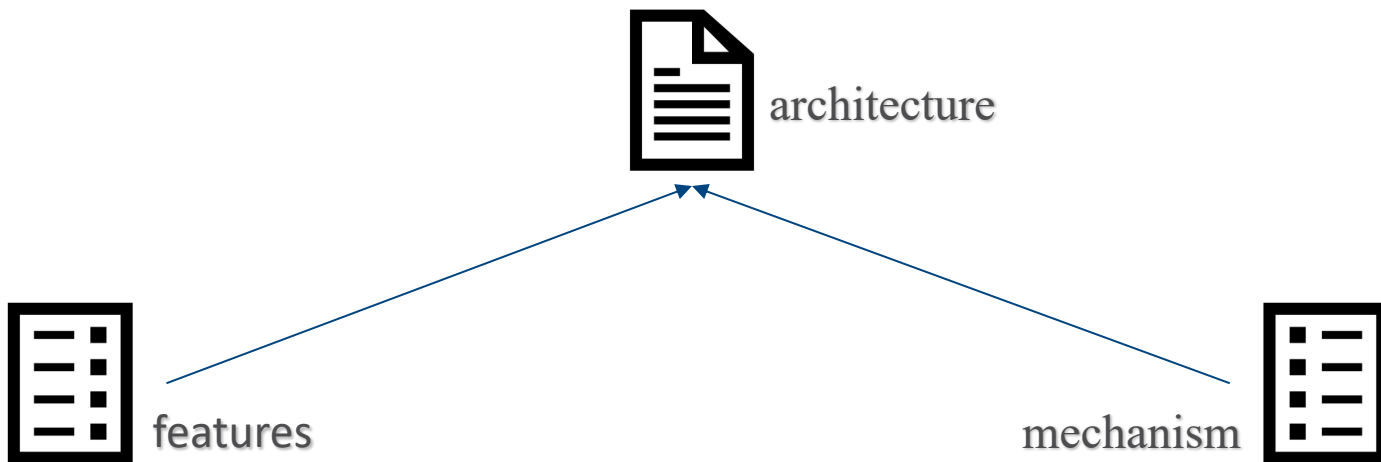
[Go to spec numbering scheme page](#)

Click on spec number for details

spec number	title	notes
TS 33.102	3G security; Security architecture	
TS 33.103	3G security; Integration guidelines	
TS 33.105	3G Security; Cryptographic algorithm requirements	
TS 33.106	3G security; Lawful interception requirements	
TS 33.107	3G security; Lawful interception architecture and functions	
TS 33.108	3G security; Handover interface for Lawful Interception (LI)	
TS 33.109	Bootstrapping of application security using AKA and support for subscriber certificates; System description	SPECIFICATION WITHDRAWN
TS 33.110	Key establishment between a Universal Integrated Circuit Card (UICC) and a terminal	
TS 33.116	Security Assurance Specification (SCAS) for the MME network product class	
TS 33.117	Catalogue of general security assurance requirements	
TS 33.120	Security Objectives and Principles	
TS 33.122	Security aspects of Common API Framework (CAPIF) for 3GPP northbound APIs	
TS 33.126	Lawful Interception requirements	

TS33.102

- This specification defines the security architecture, i.e., the security features and the security mechanisms, for the third generation mobile telecommunication system.





TS33.102

- A security feature is a service capability that meets one or several security requirements. The complete set of security features address the security requirements as they are defined in "3G Security: Threats and Requirements" (TS 21.133 [1]) and implement the security objectives and principles described in TS 33.120 [2].
- A security mechanism is an element that is used to realise a security feature. All security features and security mechanisms taken together form the security architecture.

Network access security (I):

the set of security features that provide users with secure access to 3G services, and which in particular protect against attacks on the (radio) access link;

Network domain security (II):

the set of security features that enable nodes in the provider domain to securely exchange signalling data, and protect against attacks on the wireline network;

User domain security (III):

the set of security features that secure access to mobile stations;

Application domain security (IV):

the set of security features that enable applications in the user and in the provider domain to securely exchange messages;

Visibility and configurability of security (V):

the set of features that enables the user to inform himself whether a security feature is in operation or not and whether the use and provision of services should depend on the security feature.

4 Overview of the security architecture

Figure 1 gives an overview of the complete 3G security architecture.

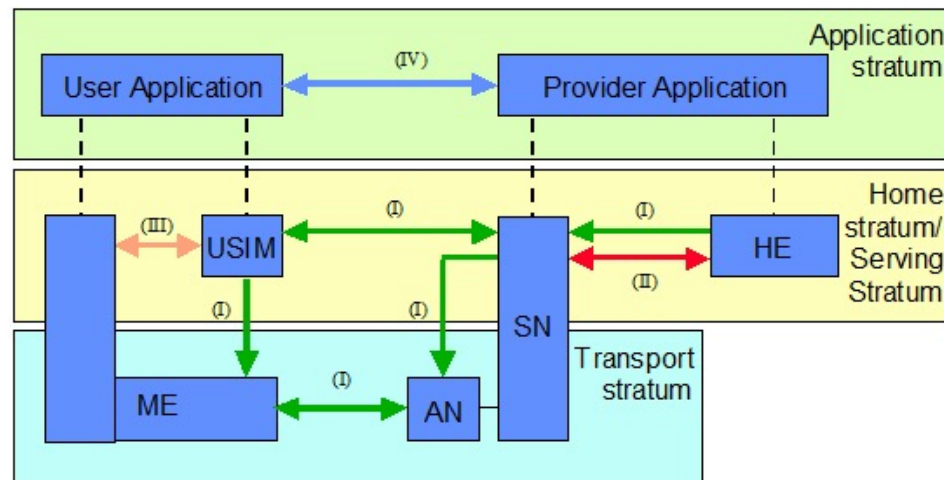
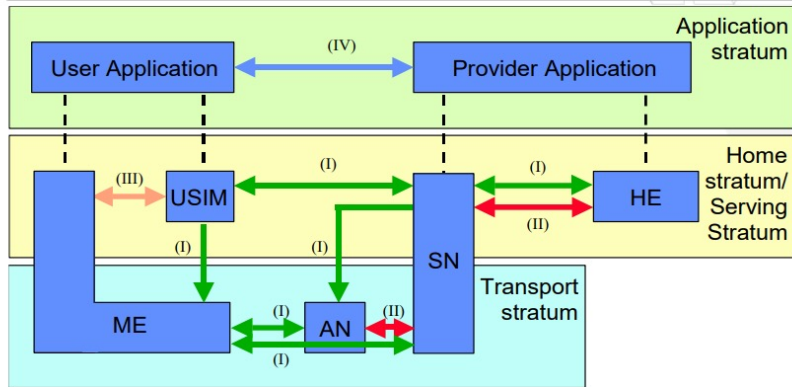


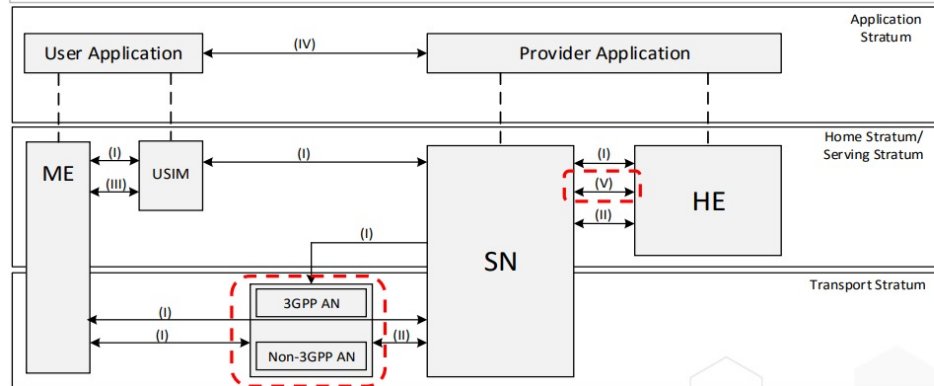
Figure 1: Overview of the security architecture

4G Security Architecture (TS 33.401)



- I. Network access security (I)
- II. Network domain security (II)
- III. User Domain Security (III)
- IV. Application domain security (V)
- V. Visibility and configurability of security (VI)

5G Security Architecture (TS 33.501)



- I. Network access security (I)
- II. Network domain security (II)
- III. User Domain Security(III)
- IV. Application domain security (V)
- V. SBA domain security (V)
- VI. Visibility and configurability of security (VI)

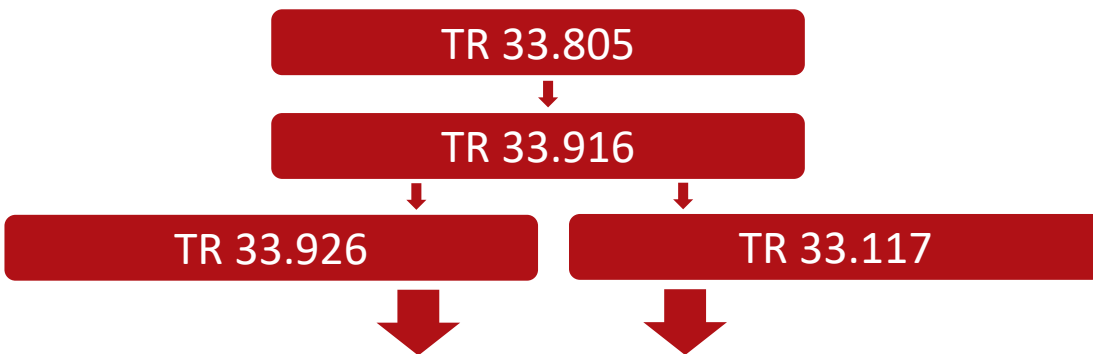
Enhancement

1. AN : 3GPP and non-3GPP access network treated more equally in access network.
2. $SN \leftrightarrow HE(V)$: interface for Service-based Architecture

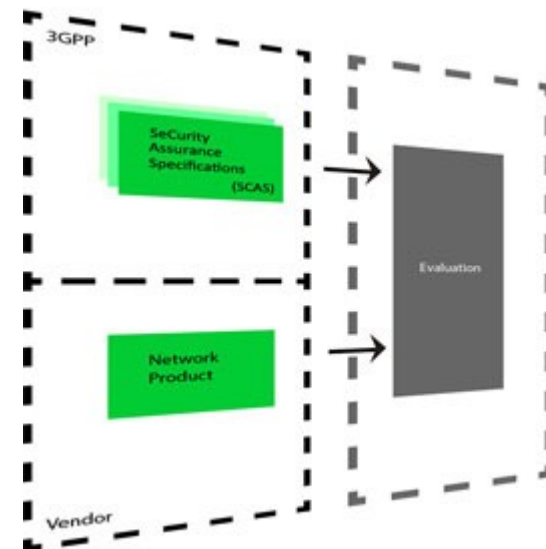
Summary

- The first phase of 5G security standard is approaching its closing stage and technology details are available in TS 33.501. It not only inherits some good security features from previous generations, but also provide some significant new features to make the 5G system more secure and open to meet the new stringent system requirement.
- Comparing to the LTE security standard (TS 33.401), 5G security system provides an open authentication platform with better protection over privacy.
- More advanced security features will be provided in the next phase of 5G standard, including Perfect Forward Secrecy, Credential Remote Provisioning, and possible new authentication and data protection scheme for massive IoT devices.

Security Assurance Methodology (SECAM) for 3GPP Nodes

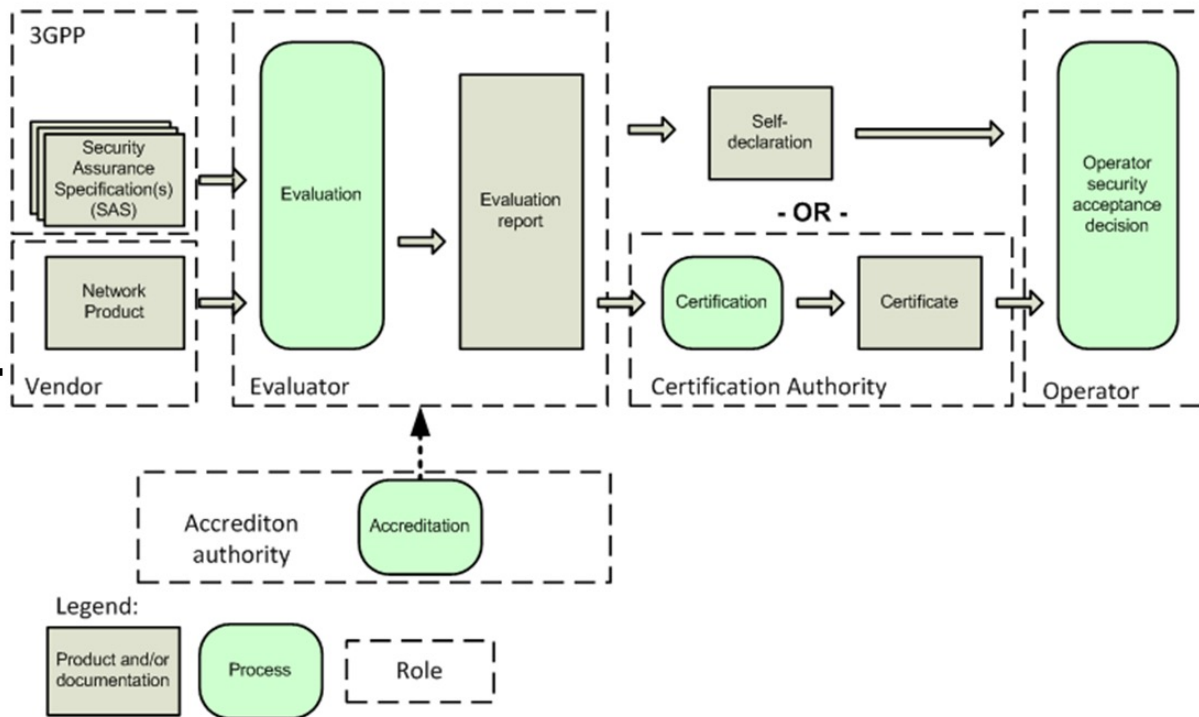


TS 33.511	Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class
TS 33.512	5G Security Assurance Specification (SCAS); Access and Mobility management Function (AMF)
TS 33.513	5G Security Assurance Specification (SCAS); User Plane Function (UPF)
TS 33.514	5G Security Assurance Specification (SCAS) for the Unified Data Management (UDM) network product class
TS 33.515	5G Security Assurance Specification (SCAS) for the Session Management Function (SMF) network product class
TS 33.516	5G Security Assurance Specification (SCAS) for the Authentication Server Function (AUSF) network product class
TS 33.517	5G Security Assurance Specification (SCAS) for the Security Edge Protection Proxy (SEPP) network product class
TS 33.518	5G Security Assurance Specification (SCAS) for the Network Repository Function (NRF) network product class
TS 33.519	5G Security Assurance Specification (SCAS) for the Network Exposure Function (NEF) network product class
TS 33.520	5G Security Assurance Specification (SCAS); Non-3GPP InterWorking Function (N3IWF)
TS 33.521	5G Security Assurance Specification (SCAS); Network Data Analytics Function (NWDAF)
TS 33.522	5G Security Assurance Specification (SCAS); Service Communication Proxy (SECP)



TR 33.805

Study on security assurance methodology for 3GPP network products



TR 33.926

Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes

The critical assets of GNP to be protected are:

- User account data and credentials (e.g. passwords);
- Sufficient processing capacity
- Log data;
- Configuration data.
- Operating System
- GNP Application
- Hardware.

4.3 Generic network product model

4.3.1 Generic network product model overview

Figure 4.3-1 depicts the components of a generic network product model at a high level. These components are further described in the following subclauses.

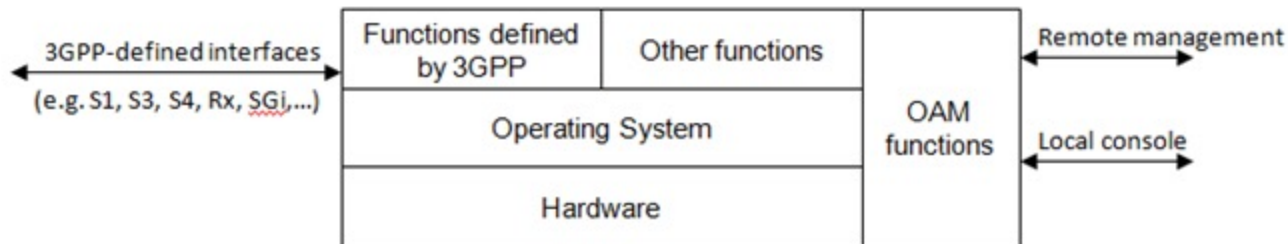


Figure 4.3-1: GNP model



TR 33.926

Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes

- **Spoofing identity.** An example of identity spoofing is illegally accessing and then using another user's authentication information, such as username and password.
- **Tampering with data.** Data tampering involves the malicious modification of data. Examples include unauthorized changes made to persistent data, such as that held in a database, and the alteration of data as it flows between two computers over an open network, such as the Internet.
- **Repudiation.** Repudiation threats are associated with users who deny performing an action without other parties having any way to prove otherwise. For example, a user performs an illegal operation in a system that lacks the ability to trace the prohibited operations. Non-repudiation refers to the ability of a system to counter repudiation threats. For example, a user who purchases an item might have to sign for the item upon receipt. The vendor can then use the signed receipt as evidence that the user did receive the package.
- **Information disclosure.** Information disclosure threats involve the exposure of information to individuals who are not supposed to have access to it. For example, the ability of users to read a file that they were not granted access to, or the ability of an intruder to read data in transit between two computers.
- **Denial of service.** Denial of service (DoS) attacks deny service to valid users-for example, by making a Web server temporarily unavailable or unusable. You need to protect against certain types of DoS threats simply to improve system availability and reliability.
- **Elevation of privilege.** In this type of threat, an unprivileged user gains privileged access and thereby has sufficient access to compromise or destroy the entire system. Elevation of privilege threats include those situations in which an attacker has effectively penetrated all system defenses and become part of the trusted system itself, a dangerous situation indeed.



TR 33.926

Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes

5.3.6 Information disclosure

5.3.6.1 Poor key generation

- *Threat Name:* Poor key generation
- *Threat Category:* Information Disclosure
- *Threat Description:* A poor key generation may help an attacker to discover and disclose the key and then read or modify the encrypted data. Attackers can discover a key, for example, if:
 - It was generated in a non-random fashion (e.g. insecure random generator).
 - It was generated starting from a passphrase containing low entropy.
 - The generated key length is too short so the time to retrieve the key by means of dictionary attacks is short.
- *Threatened Asset:* all critical asset in the GNP as listed in clause 5.2 except hardware assets.



TS 33.117

Catalogue of general security assurance requirements

Contents

Foreword	6
1 Scope	7
2 References	7
3 Definitions and abbreviations	7
3.1 Definitions	7
3.2 Abbreviations	8
4 Catalogue of security requirements and related test cases	8
4.1 Introduction	8
4.1.1 Pre-requisites for testing	8
4.1.2 Use of tools in testing	9
4.1.3 Documentation Requirements	9
4.2 Security functional requirements and related test cases	9
4.2.1 Introduction	9
4.2.2 Security functional requirements deriving from 3GPP specifications and related test cases	10
4.2.2.1 Security functional requirements deriving from 3GPP specifications – general approach	10
4.2.2.2 Security functional requirements derived from 3GPP specifications – general SBA/SBI aspects	10
4.2.2.2.1 Introduction	10
4.2.2.2.2 Protection at the transport layer	10
4.2.2.2.3 Authorization of NF service access	11
4.2.2.2.3.1 Authorization token verification failure handling within one PLMN	11
4.2.2.2.3.2 Authorization token verification failure handling in different PLMNs	13
4.2.3 Technical baseline	14
4.2.3.1 Introduction	14
4.2.3.2 Protecting data and information	14
4.2.3.2.1 Protecting data and information – general	14
4.2.3.2.2 Protecting data and information – Confidential System Internal Data	15
4.2.3.2.3 Protecting data and information in storage	15
4.2.3.2.4 Protecting data and information in transfer	16
4.2.3.2.5 Logging access to personal data	17
4.2.3.3 Protecting availability and integrity	18
4.2.3.3.1 System handling during overload situations	18
4.2.3.3.2 Boot from intended memory devices only	19
4.2.3.3.3 System handling during excessive overload situations	19
4.2.3.3.4 System robustness against unexpected input	21
4.2.3.3.5 Network Product software package integrity	21
4.2.3.4 Authentication and authorization	23
4.2.3.4.1 Authentication policy	23
4.2.3.4.2 Authentication attributes	26
4.2.3.4.2.1 Account protection by at least one authentication attribute	26
4.2.3.4.3 Password policy	29
4.2.3.4.4 Specific Authentication use cases	37
4.2.3.4.5 Policy regarding consecutive failed login attempts	38
4.2.3.4.6 Authorization and access control	39
4.2.3.5 Protecting sessions	40
4.2.3.5.1 Protecting sessions – logout function	40
4.2.3.5.2 Protecting sessions – Inactivity timeout	41
4.2.3.6 Logging	42
4.2.3.6.1 Security event logging	42
4.2.3.6.2 Log transfer to centralized storage	44
4.2.3.6.3 Protection of security event log files	44
4.2.4 Operating systems	45
4.2.4.1 General operating system requirements and related test cases	45
4.2.4.1.1 Availability and Integrity	45
4.2.4.1.2 Authentication and Authorization	50
4.2.4.2 UNIX® specific requirements and related test cases	51

4.2.4.2.1 General	51
4.2.4.2.2 System account identification	51
4.2.5 Web Servers	52
4.2.5.1 HTTPS	52
4.2.5.2 Logging	52
4.2.5.2.1 Webserver logging	52
4.2.5.3 HTTP User sessions	53
4.2.5.4 HTTP input validation	55
4.2.6 Network Devices	55
4.2.6.1 Protection of Data and Information	55
4.2.6.2 Protecting availability and integrity	55
4.2.6.2.1 Packet filtering	55
4.2.6.2.2 Interface robustness requirements	56
4.2.6.2.3 GTP-C Filtering	57
4.2.6.2.4 GTP-U Filtering	59
4.3 Security requirements and related test cases related to hardening	62
4.3.1 Introduction	62
4.3.2 Technical Baseline	62
4.3.2.1 No unnecessary or insecure services / protocols	62
4.3.2.2 Restricted reachability of services	64
4.3.2.3 No unused software	65
4.3.2.4 No unused functions	66
4.3.2.5 No unsupported components	68
4.3.2.6 Remote login restrictions for privileged users	69
4.3.2.7 Filesystem Authorization privileges	70
4.3.3 Operating Systems	70
4.3.3.1 General operating system requirements and test cases	70
4.3.3.1.1 IP-Source address spoofing mitigation	70
4.3.3.1.2 Minimized kernel network functions	73
4.3.3.1.3 No automatic launch of removable media	77
4.3.3.1.4 SYN Flood Prevention	78
4.3.3.1.5 Protection from buffer overflows	79
4.3.3.1.6 External file system mount restrictions	80
4.3.4 Web Servers	81
4.3.4.1 General	81
4.3.4.2 No system privileges for web server	81
4.3.4.3 No unused HTTP methods	82
4.3.4.4 No unused add-ons	83
4.3.4.5 No compiler, interpreter, or shell via CGI or other server-side scripting	85
4.3.4.6 No CGI or other scripting for uploads	85
4.3.4.7 No execution of system commands with SSI	85
4.3.4.8 Access rights for web server configuration	86
4.3.4.9 No default content	86
4.3.4.10 No directory listings	87
4.3.4.11 Web server information in HTTP headers	88
4.3.4.12 Web server information in error pages	89
4.3.4.13 Minimized file type mappings	89
4.3.4.14 Restricted file access	90
4.3.4.15 Execute rights exclusive for CGI/Scripting directory	91
4.3.5 Network Devices	91
4.3.5.1 Traffic Separation	91
4.3.6 Network Functions in service-based architecture	92
4.3.6.1 Introduction	92
4.3.6.2 No code execution or inclusion of external resources by JSON parsers	92
4.3.6.3 Unique key values in IEs	94
4.3.6.4 The valid format and range of values for IEs	94
4.4 Basic vulnerability testing requirements	95
4.4.1 Introduction	95
4.4.2 Port Scanning	95
4.4.3 Vulnerability scanning	97
4.4.4 Robustness and fuzz testing	98

TS 33.117

Catalogue of general security assurance requirements

4.2.2.2.3.2	Authorization token verification failure handling in different PLMMS	4
4.2.3	Technical baseline	4
4.2.3.1	Introduction	4
4.2.3.2	Protecting data and information	4
4.2.3.2.1	Protecting data and information – general	4
4.2.3.2.2	Protecting data and information – Confidential System Internal Data	4
4.2.3.2.3	Protecting data and information in storage	4
4.2.3.2.4	Protecting data and information in transfer	4
4.2.3.2.5	Logging access to personal data	4
4.2.3.3	Protecting availability and integrity	4
4.2.3.3.1	System handling during overload situations	4
4.2.3.3.2	Boot from intended memory devices only	4
4.2.3.3.3	System handling during excessive overload situations	4
4.2.3.3.4	System robustness against unexpected input	4
4.2.3.3.5	Network Product software package integrity	4
4.2.3.4	Authentication and authorization	4
4.2.3.4.1	Authentication policy	4
4.2.3.4.2	Authentication attributes	4
4.2.3.4.2.1	Account protection by at least one authentication attribute	4
4.2.3.4.3	Password policy	4
4.2.3.4.4	Specific Authentication use cases	4
4.2.3.4.5	Policy regarding consecutive failed login attempts	4
4.2.3.4.6	Authorization and access control	4
4.2.3.5	Protecting sessions	4
4.2.3.5.1	Protecting sessions – logout function	4
4.2.3.5.2	Protecting sessions – Inactivity timeout	4
4.2.3.6	Logging	4
4.2.3.6.1	Security event logging	4



TS 33.117

Catalogue of general security assurance requirements

4.2.3.3.4 System robustness against unexpected input.

Requirement Name: System robustness against unexpected input.

Requirement Description: During transmission of data to a system it is necessary to validate input to the network product before processing. This includes all data which is sent to the system. Examples of this are user input, values in arrays and content in protocols. The following typical implementation error shall be avoided:

- No validation on the lengths of transferred data
- Incorrect assumptions about data formats
- No validation that received data complies with the specification
- Insufficient handling of protocol errors in received data
- Insufficient restriction on recursion when parsing complex data formats
- White listing or escaping for inputs outside the values margin

Security Objective references: tba.

Test case:

This requirement will be verified by Robustness and Protocol fuzzing tests as defined in clause 4.4.4 Robustness and fuzz testing.



TS 33.513

5G Security Assurance Specification - UPF

▪ 4.3 UPF-specific adaptations of hardening requirements and related test cases[↵]

▪ 4.3.1 Introduction[↵]

This clause specifies the UPF-specific adaptations of hardening requirements and related test cases. [↵]

▪ 4.3.2 Technical baseline[↵]

There are no UPF-specific additions to clause 4.3.2 in TS 33.117 [3].[↵]

▪ 4.3.3 Operating systems[↵]

There are no UPF-specific additions to clause 4.3.3 in TS 33.117 [3].[↵]

▪ 4.3.4 Web servers[↵]

There are no UPF-specific additions to clause 4.3.4 in TS 33.117 [3].[↵]

▪ 4.3.5 Network devices[↵]

There are no UPF-specific additions to clause 4.3.5 in TS 33.117 [3].[↵]

▪ 4.3.6 Network functions in service-based architecture[↵]

There are no UPF-specific additions to clause 4.3.6 in TS 33.117 [3].[↵]

▪ 4.4 UPF-specific adaptations of basic vulnerability testing requirements and related test cases[↵]

There are no UPF-specific additions to clause 4.4 in TS 33.117 [3].[↵]



TS 33.513

5G Security Assurance Specification - UPF

■ 4.2.2 Security functional requirements on the UPF deriving from 3GPP specifications and related test cases[↵]

■ 4.2.2.0 General [↵]

The general approach in TS 33.117 [3] clause 4.2.2.1 and all the requirements and test cases in TS 33.117 [3] clause 4.2.2.2 related to SBA/SBI aspect apply to the UPF network product class.[↵]

■ 4.2.2.1 Confidentiality protection of user data transported over N3 interface.[↵]

Requirement Name: Confidentiality protection of user data transported over N3 interface.[↵]

Requirement Reference: TS 33.501 [2], Clause 9.3[↵]

Requirement Description: "The transported user data between gNB and UPF shall be confidentiality protected." As specified in TS 33.501 [2], clause 9.3. [↵]

Threat Reference: TR 33.926 [7], Clause L.2.2, "No protection or weak protection for user plane data ".[↵]



TS 33.513

5G Security Assurance Specification - UPF

■ Procedure and execution steps:↵

Pre-Condition: ↵

- UPF network product is connected in simulated/real network environment.↵
- The tunnel mode IPsec ESP and IKE certificate authentication is implemented.↵
- Tester shall have knowledge of the security parameters of tunnel for decrypting the ESP packets.↵
- Tester shall have access to the N3 interface between gNB and UPF. ↵
- Tester shall have knowledge of the confidentiality algorithm and confidentiality protection keys used for encrypting the encapsulated payload.↵

Execution Steps: ↵

The requirement mentioned in this clause is tested in accordance with the procedure mentioned in clause 4.2.3.2.4 of TS 33.117 [3].↵

Expected Results:↵

The user data transported between gNB and UPF is confidentiality protected.↵

Expected format of evidence:↵

Evidence suitable for the interface, e.g., evidence can be presented in the form of screenshot/screen-capture.↵

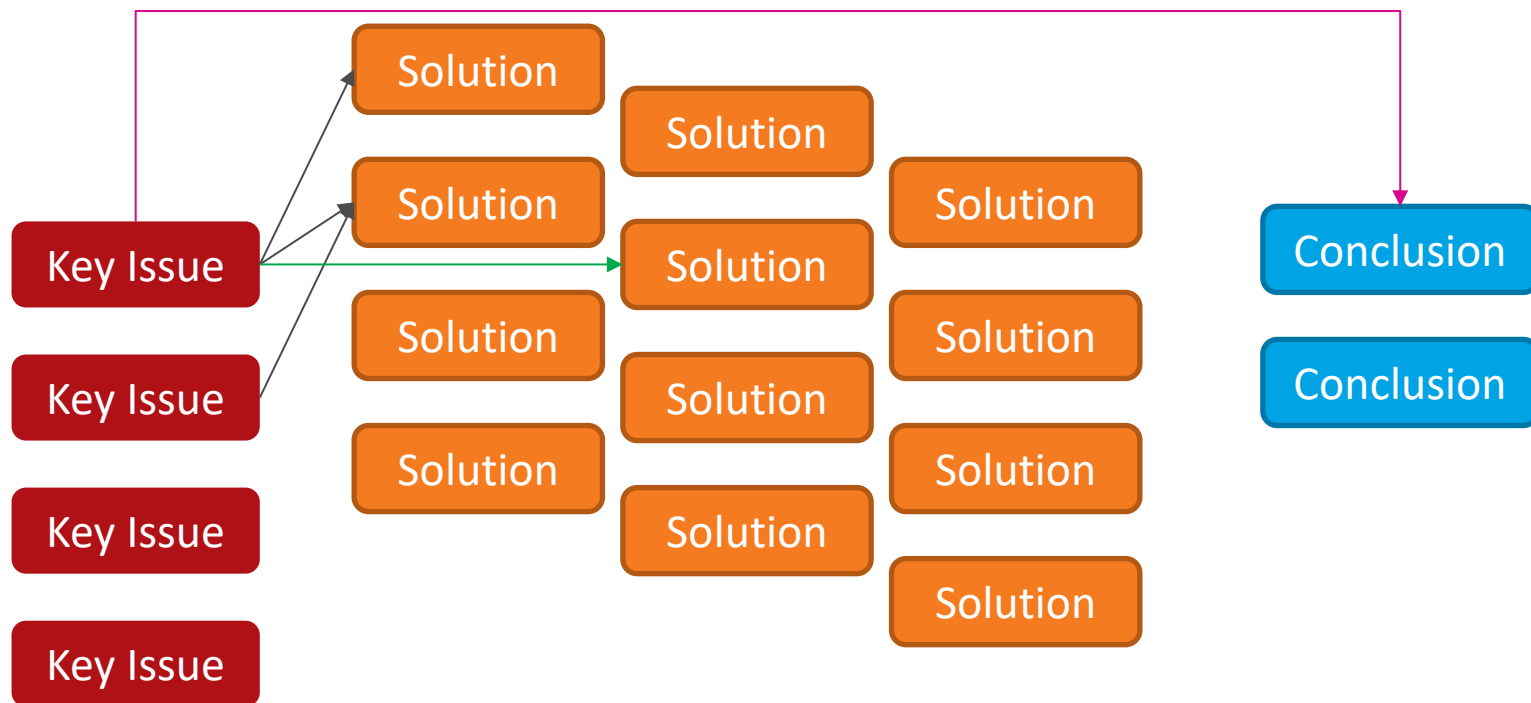


TR 33.8xx

聽聽3gpp
怎麼說

TR 33.854	Study on security aspects of Unmanned Aerial Systems (UAS)
TR 33.855	Study on security aspects of the 5G Service Based Architecture (SBA)
TR 33.856	Study on security aspects of single radio voice continuity from 5G to UTRAN
TR 33.857	Study on enhanced security support for Non-Public Networks (NPN)
TR 33.859	Study on the Introduction of Key Hierarchy in Universal Terrestrial Radio Access Network (UTRAN)
TR 33.860	Study on Enhanced General Packet Radio Service (EGPRS) access security enhancements with relation to cellular Internet of Things (IoT)
TR 33.861	Study on evolution of Cellular Internet of Things (CIoT) security for the 5G System
TR 33.862	Study on security aspects of the Message Service for MIoT over the 5G System (MSGin5G)
TR 33.863	Study on battery efficient security for very low throughput Machine Type Communication (MTC) devices
TR 33.864	Study on the security of Access and Mobility Management Function (AMF) re-allocation
TR 33.865	Security Aspects of WLAN Network Selection for 3GPP Terminals
TR 33.866	Study on security aspects of enablers for Network Automation (eNA) for the 5G system (5GS) Phase 2
TR 33.867	Study on user consent for 3GPP services
TR 33.868	Study on security aspects of Machine-Type Communications (MTC) and other mobile data applications communications enhancements
TR 33.869	Security aspects of Public Warning System (PWS)
TR 33.871	Study on security for Web Real Time Communications (WebRTC) IP Multimedia Subsystem (IMS) client access to IMS
TR 33.872	Study on security enhancements to Web Real Time Communication (WebRTC) access to IP Multimedia Subsystem (IMS)
TR 33.873	Study on the security of the system enablers for devices having Multiple Universal Subscriber Identity Modules (MUSIM)
TR 33.874	Study on enhanced security for Phase 2 network slicing
TR 33.875	Study on enhanced security aspects of the 5G Service Based Architecture (eSBA)
TR 33.878	Security aspects of early IMS
TR 33.879	Study on security enhancements for Mission Critical Push To Talk (MCPTT) over LTE
TR 33.880	Study on mission critical security enhancements
TR 33.885	Study on security aspects for LTE support of Vehicle-to-Everything (V2X) services
TR 33.888	Study on security issues to support Group Communication System Enablers (GCSE) for LTE
TR 33.889	Study on security aspects of Machine-Type Communications (MTC) architecture and feature enhancements
TR 33.895	Study on Security aspects of integration of Single Sign-On (SSO) frameworks with 3GPP operator-controlled resources and mechanisms

TR33.8xx Studies reading guide





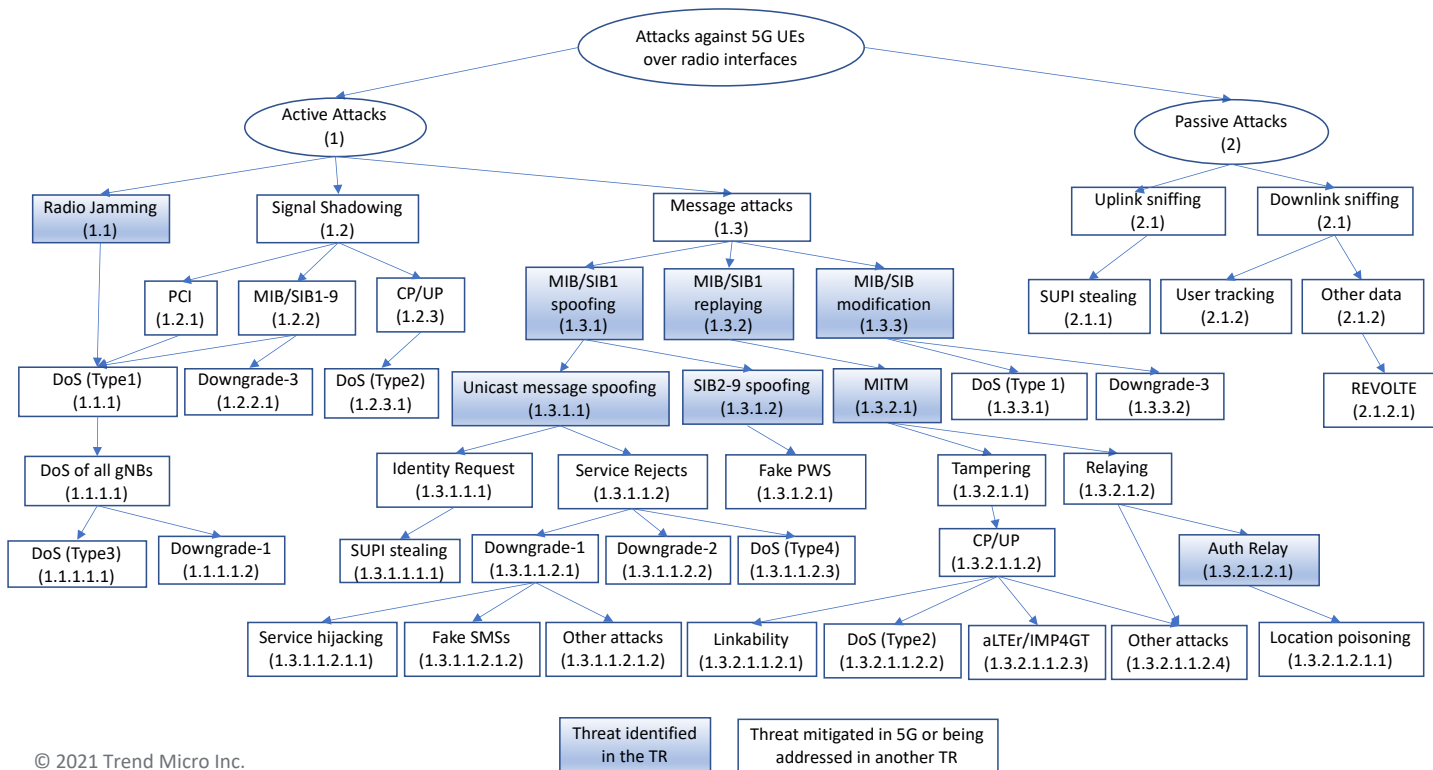
TR 33.809

Study on 5G security enhancements against False Base Stations (FBS)

The key-issues and solutions in the present document should state which of the following security and privacy areas they address:

- **DoS attack on UE:** attempts to hinder the UEs' access to the network.
- **DoS attack on network:** attempts to hinder the network's ability to provide services to the UEs.
- **Rogue services:** attempts to deliver unauthorized or unsolicited services (e.g., SMS and calls) to the UEs.
- **Subscriber privacy attack:** attempts to identify subscriptions or trace the UEs.

Attack Against 5G UEs





Key Issue #1:

Security of unprotected unicast messages

- Both the uplink and downlink unicast message which could be sent unprotected
- An example of unprotected uplink message is RRC UECapabilityInformation.
- Examples of unprotected downlink messages are RRC UE Capability Enquiry, and REJECTs in RRC/NAS layers.



Key Issue #1:

Security of unprotected unicast messages

- Due to optimization need, the gNB in theory could send **UECapabilityEnquiry** to ask for UE's AS capability.



Key Issue #1:

Security of unprotected unicast messages

- Due to optimization need, the gNB in theory could send **UECapabilityEnquiry** to ask for UE's AS capability.
- The false base station could behave as a man-in-the-middle and catch the **UECapabilityInformation** over-the-air. After that, the false base station could modify the value in this message to lower capability level and forward it to the real gNB, causing the UE to only operate with limited radio capability.



Key Issue #1:

Security of unprotected unicast messages

- Due to optimization need, the gNB in theory could send **UECapabilityEnquiry** to ask for UE's AS capability.
- The false base station could behave as a man-in-the-middle and catch the **UECapabilityInformation** over-the-air. After that, the false base station could modify the value in this message to lower capability level and forward it to the real gNB, causing the UE to only operate with limited radio capability.
- Security capabilities are protected from bidding down attack. And it is not certain if the bidding down of radio capabilities cause serious threat



Key Issue #1:

Security of unprotected unicast messages

6.1 Solution #1: Protection for the UE Capability Transfer

6.1.1 Introduction

This solution addresses the security requirement in Key Issue #1 for unicast RRC messages.

6.1.2 Solution details

The two messages exchanged in the UE Capability transfer procedure, namely UECapabilityEnquiry and UECapabilityInformation, needs to be sent after the AS security establishment and activation.

NOTE: According to TS 38.331 [2], it is implementation specific whether the gNB initiates UE Capability Transfer procedure after the AS SMC and AS security context established or before it.



Key Issue #1:

Security of unprotected unicast messages

6.3 Solution #3: Protection of uplink UECapabilityInformation RRC message

6.3.1 Introduction

This solution addresses the following key issues:


- Key issue #1: security of unprotected unicast messages.

The solution provides a mechanism for protection of the uplink RRC UECapabilityInformation message.

6.3.2 Solution details

Current security mechanisms for RRC UECapabilityInformation are listed in Annex B.1 (Protection of RRC messages) of 3GPP TS 38.331, which can be summarized as follows:

- (1) The RRC UECapabilityInformation should not be sent unprotected after AS security activation.
- (2) The RRC UECapabilityInformation may be sent unprotected before AS security activation.



Mechanism #(1) ensures that the RRC UECapabilityInformation cannot be tampered after AS security activation.

For mechanism #(2), which is the root cause of the problem, this solution introduces two recommendations for the system (the network and the UE):

- The network should not send RRC UECapabilityEnquiry to the UE before AS security has been activated.
- When the UE gets an RRC UECapabilityEnquiry message from a gNB, the UE should first verify that the AS security has been activated, i.e., an RRC security mode command procedure has been successfully performed. If the above verification succeeds, the UE should send corresponding RRC UECapabilityInformation message to the gNB as a ciphered and integrity protected message. Else if the above verification fails, i.e., an RRC security mode command procedure has not been performed or has failed, the UE should not send RRC UECapabilityInformation message to the gNB. The UE may send the RRC UECapabilityInformation message to the gNB later, after AS security has been activated.

However, if the system (the network and the UE) has to perform the mechanism #(2), e.g., for early optimization, this solution mandates that the system supports a recovery mechanism from tampered uplink RRC UECapabilityInformation message. It means the followings:

- The network should taint the UE capabilities so that the network (i.e., same gNB/AMF or different gNB/AMF at handovers) can determine whether those UE capabilities were received before or after the AS security activation.
- Once a successful security activation is performed, depending on the security policy, the network may re-enquire the UE capabilities if they were received earlier without security protection. To re-enquire the UE capabilities, the network may send to UE a Boolean flag in AS SMCommand message, or a HASH of locally stored UE capabilities, or a new RRC UECapabilityEnquiry message.



7 Conclusions

Editor's Note: This clause contains the agreed conclusions.

7.1 Conclusions on Key Issue #1

Following conclusions are made on Key Issue #1 "Security of unprotected unicast messages":

- It is concluded that no additional normative work is required for the protection against tampering of RRC UE CapabilityInformation messages.

7.6 Conclusions on Key Issue #6

Following conclusions are made on Key Issue #6 "Resistance to radio jamming":

- It is concluded that there will be no further action for Rel-16 as it is stated in the NOTE in the key issue details.



Bonus : 還能問3GPP什麼？

5GMF 白書

5G ユースケースにおけるセキュリティ

第 1.0 版

2020 年 7 月 29 日



The Fifth Generation Mobile Communications Promotion Forum

https://5gmf.jp/wp/wp-content/uploads/2020/07/5g-whitepaper_1.0.pdf

了解更多關於行動網路安全



Contact us :

contact_telecom@trendmicro.com

Thanks





THE ART OF CYBERSECURITY

Threat detection and response across multiple
attack vectors by Trend Micro. Created with
real data by artist **Brendan Dawes**.