TRUSTED
CONNECTIVITY
ALLIANCE

Trusted Connectivity Alliance Recommended 5G SIM for 3GPP Release 17

December 2022

The information contained in this document may be used, disclosed and reproduced without the prior written authorization of Trusted Connectivity Alliance. Readers are advised that Trusted Connectivity Alliance reserves the right to amend and update this document without prior notice. Updated versions will be published on the Trusted Connectivity Alliance website at http://www.trustedconnectivityalliance.org

Intellectual Property Rights (IPR) Disclaimer

Attention is drawn to the possibility that some of the elements of any material available for download from the specification pages on Trusted Connectivity Alliance's website may be the subject of Intellectual Property Rights (IPR) of third parties, some, but not all, of which are identified below. Trusted Connectivity Alliance shall not be held responsible for identifying any or all such IPR, and has made no inquiry into the possible existence of any such IPR. TRUSTED CONNECTIVITY ALLIANCE SPECIFICATIONS ARE OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NON- INFRINGEMENT IS EXPRESSLY DISCLAIMED. ANY IMPLEMENTATION OF ANY TRUSTED CONNECTIVITY ALLIANCE SPECIFICATION SHALL BE MADE ENTIRELY AT THE IMPLEMENTER'S OWN RISK, AND NEITHER TRUSTED CONNECTIVITY ALLIANCE, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY IMPLEMENTER OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER DIRECTLY OR INDIRECTLY ARISING FROM THE IMPLEMENTATION OF ANY TRUSTED CONNECTIVITY ALLIANCE SPECIFICATION.

Contents

1. Executive Summary

In a major milestone for 5G, 3GPP finalised the USIM Release 17 Specifications in September 2022. This is the third set of specifications for 5G New Radio (NR) technology, following the publication of Phase 1 (Release 15) and Phase 2 (Release 16). 3GPP Release 17 marks the conclusion of the 5G NR Phase 2 and the evolution towards '5G-Advanced', with Release 18 expected in the coming years.

3GPP Release 17 includes new features and enhancements to improve network security and profitability through improved Steering of Roaming (SoR), value-added services enablement, and support for non-terrestrial networks. It also introduced a new spectrum, further enhancing the Radio Access Technology (RAN) with a particular focus on industrial IoT, proximity and automotive services.

Trusted Connectivity Alliance (TCA) Recommended 5G SIM

SIMs (also known as a Universal Integrated Circuit Cards or UICCs) and eSIMs (also known as a embedded Universal Integrated Circuit Cards or eUICCs) are the only platforms which can be used to secure access to 3GPP networks, whether it be a 3G, 4G Long Term Evolution (4G-LTE) network, or a 5G network in Release 15, 16 or 17 (commonly referred to in this document as a 5G network). The radio technology used to communicate with the network core can be LTE, LTE CAT-M, Narrowband IoT (NB-IoT), 5G New Radio or other supported non-3GPP radio bearers, such as Wi-Fi.

TCA first defined the Recommended 5G SIM in December 2018 to outline which technical features of SIM/eSIM technology address the challenges mobile operators face, beyond network access, when migrating from 4G to 5G. Subsequently, TCA enhanced the Recommended 5G SIM to align with new use cases introduced by 3GPP's Release 16 for Phase 2 5G deployments. The Recommended 5G SIM has now been updated to align with new features defined in 3GPP Release 17.

The high-performance networks enabled by Release 17, however, requires security to scale new heights. This document explains how the **TCA Recommended 5G SIM for 3GPP Release 17** is the optimal solution that allows mobile operators to take advantage of the business opportunities offered by the latest specification, while maintaining an adequate level of security.

This document offers:

- An overview of the benefits of full 5G network deployments, known as 5G Stand Alone (5G-SA).
- An explanation of the 5G security considerations and summary of how the Recommended 5G SIM enables the full potential of 5G-SA to be realised, while maintaining an adequate level of security.
- A description of new features and upgrades introduced within 3GPP Release 17, highlighting the most vital benefits brought by the use of the Recommended 5G SIM.
- Full technical details (provided in tabular form) identifying the specification parameters affected for each use-case.

2. Introduction – Momentum Continues for 5G

While 4G-LTE is poised to remain the leading mobile technology in terms of deployments over the next few years, 5G is gaining momentum following the initial rollout in 2020 as service providers continue to switch on 5G and launch commercial services globally.

5G subscriptions grew by 110 million during the third quarter to around 870 million, and that number is expected to have reached 1 billion by the end of 2022. North America and Northeast Asia are expected to have the highest 5G subscription penetration at around 35 percent, followed by the Gulf Cooperation Council countries at 20 percent and Western Europe at 11 percent. In 2028, it is projected that North America will have the highest 5G penetration at 91 percent, followed by Western Europe at 88 percent. By the end of 2028, 5 billion 5G subscriptions are forecast globally, accounting for 55 percent of all mobile subscriptions. (Source: Ericsson Mobility Report, November)

As the deployment of a 5G networks requires significant investment from mobile operators, however, many are choosing to do so gradually. A common scenario is to initially deploy the 5G Radio Access Network, relaying on the LTE Evolved Packet Core (EPC). This is known as 5G-Non Stand Alone (5G-NSA) configuration. The full 5G core architecture deployment, known as a 5G Stand Alone (5G-SA) configuration, is subsequently postponed to a later stage.

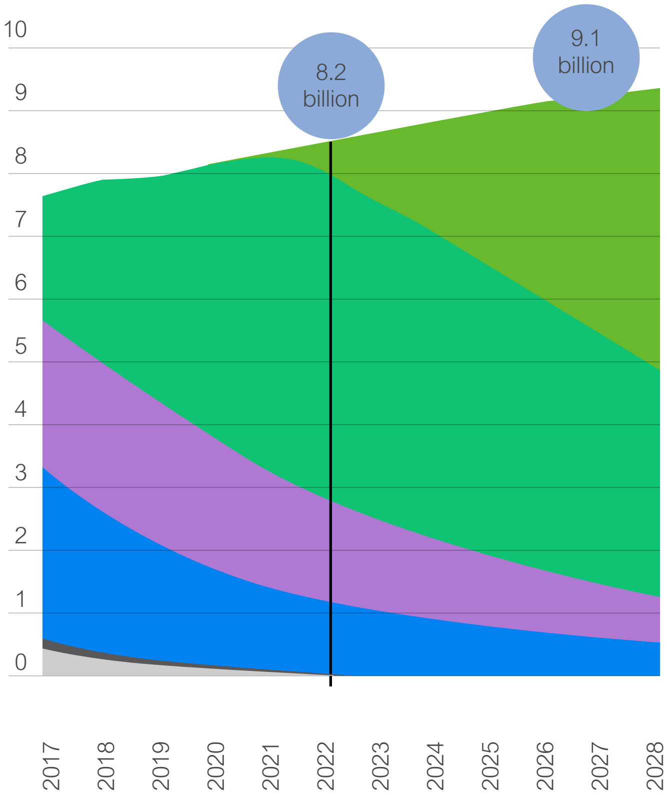
This approach provides an immediate benefit of greater capacity and boosted data rate to users; however it is still bounded to the existing LTE core backbone network for services. This means that with the 5G-NSA configuration, not all 5G features are available. For example, it lacks ultra-low latency reliable communication (URLLC), enhanced broadband, and complete separation of control and data planes.

Consequently, this “intermediate” solution optimises capital expenditure but cannot deliver all the promises of 5G. This is accomplished only when the “full” 5G-SA solution is deployed, as it is the only configuration that implements the full 5G network configuration.

To contextualise the current status, as of October 2022, 505 operators in 155 countries and territories have invested in 5G. Of those, 135 operators in 53 countries are investing in 5G-SA networks. 5G is expected to become the dominant mobile access technology by subscriptions in 2027. (Source: GSA)

5G subscriptions are forecast to reach 5 billion in 2028.

5bn



🟢 5G

🟢 LTE (4G)

🟣 WCDMA/HSPA (3G)

🔵 GSM/EDGE - only (2G)

⚫ TD-SCDMA (3G)

⚪ CDMA-only (2G/3G)

Figure 1. Mobile subscriptions by technology (billion)
(Source: Ericsson Mobility Report)

3. Security for 5G

The 5G-SA Architecture, further enhanced by the publication of Rel.17, is a significant departure from 4G-LTE as it is based on a set of independent functions deployed in a cloud infrastructure. The full 5G architecture promises to allow mobile operators and other mobile service providers to build systems that offer innovative services and generate enormous benefits. 5G-SA, with its complex micro-services topology within a cloud environment, is a combination of IT and communications technologies that change the network architecture, enabling the network to flexibly support a variety of application scenarios.

However, these changes raise different security requirements and distinct security configurations for the network, especially for network deployment and operations.

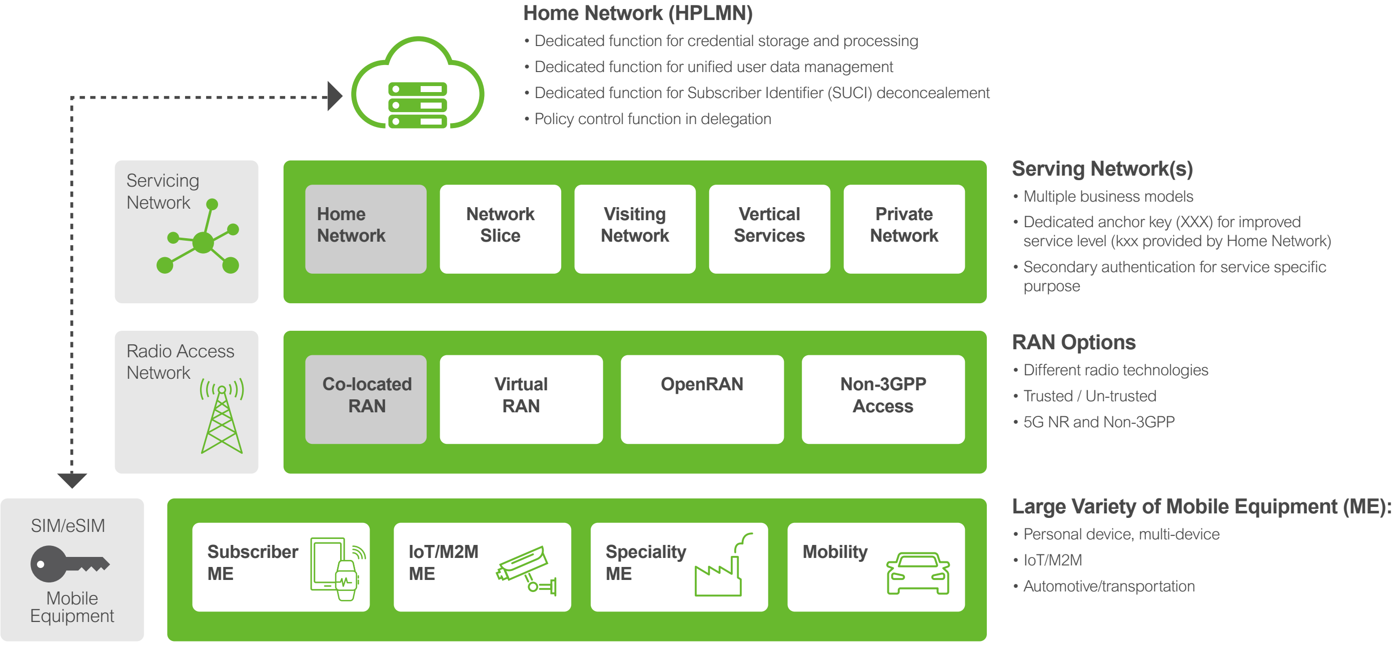
Due to compatibility issues and the need to offer a continuity of service to users, a 4G (or even 3G) SIM can be used in a 5G network. However, only a 5G SIM enables the full potential of 5G-SA to be realised, while maintaining an adequate level of security.

The additional security benefits of 5G-SA beyond 3G and 4G security can be summarised as follows:

- Privacy enhancements.
- Primary authentication for better home network control over authentication.
- Secondary authentication for the enablement of vertical use-cases and value added services.
- Extension of data integrity protection to the data plane, not just the control plane.
- Better roaming signalling protection.
- More flexibility in handling local re-authentications.

In order to explain these concepts in more detail, it is beneficial to summarise the main 5G architecture and the different security options, with a focus on the security aspects relevant for user mobile equipment (ME) functions.

3.1 5G SIM in the 5G Architecture



Home Network (HPLMN)

- Dedicated function for credential storage and processing
- Dedicated function for unified user data management
- Dedicated function for Subscriber Identifier (SUCI) deconcealement
- Policy control function in delegation

Serving Network(s)

- Multiple business models
- Dedicated anchor key (XXX) for improved service level (kxx provided by Home Network)
- Secondary authentication for service specific purpose

RAN Options

- Different radio technologies
- Trusted / Un-trusted
- 5G NR and Non-3GPP

Large Variety of Mobile Equipment (ME):

- Personal device, multi-device
- IoT/M2M
- Automotive/transportation

Figure 2. Four layers 5G architecture.

In sharp contrast with previous mobile generations, 5G is organised as several independent blocks performing a specific function. In other words, a service based architecture (SBA) utilising micro-services. The function points are in a cloud infrastructure, which can also be in a public cloud. This brings an enormous advantage in terms of flexibility and scalability, allowing mobile operators to adapt and scale the network based on their business needs. But along with the huge advantages, come new risks. As the function points can become accessible from a public network, problems that have impacted the ICT industry for many years remain.

The 5G SBA is usually presented highlighting all the main function points. For simplicity and ease of reference, this paper shows the different function units in a logically organised four-layer configuration, as shown in Figure 2 above:

• The Home Network Core

The Home Public Land Mobile Network (HPLMN) identifies the network in which the subscriber's profile is held. All the highest security functions related to the SIM issued by the mobile operator are performed in the HPLMN, including performing the primary authentication that establishes the primary trust relationship between the user equipment and the network. It also contains policy control functions for delegation. Different than in 4G, the ME identity Subscription Permanent Identifier (SUPI) is never sent in clear. It is only sent in its securely encrypted form, known as the Subscription Concealed Identifier (SUCI). The HPLMN maintains subscriber privacy, as the SUCI is only de-crypted in its Unified Data Management (UDM) function point by the so-called Subscription Identifier De-Concealing Function (SIDF). This is the only place in the 5G network where the SUCI is ever decrypted.

• Serving Network

To increase flexibility, in 5G the actual serving network layer is decoupled from the core of the home network. The serving network can be the home network itself, or a visiting network (roaming), a network slice, a dedicated network for a vertical service, or a private network. The security function is performed by a Security Anchor Function (SEAF). In a roaming scenario, the access to the SEAF is performed via an additional Security Endpoint Function (SEPF) that tunnels the exchange of information between the home network and the roaming network (see the next section for an overview of the trust model).

• Radio Access Physical Network (RAN)

The RAN has a number of configurations to increase access flexibility, and better tailor the performance. The RAN can be:

- Exclusively operated by the 5G-SA mobile operator.

- Co-located with other mobile operators.

- Operated by a third-party, with the mobile operator paying for the service

- Non-3GPP type of networks, most notably but not exclusively IEEE 802.11 Wireless Area Networks (WLAN).

Except for the first case where the RAN is exclusively operated by the 5G-SA, there is no definite trust with the RAN provider. For this reason, 5G defines a further level of security delegated to the radio access (gNodeB) with a set of specific keys. This allows the segregation of security among the different ways of accessing the network

• Wide Variety of Mobile Equipment

The variety of devices that are served by an 5G network has increased significantly, thanks to the different access options. This included Fixed Wireless Access (FWA), vehicle-to-everything (V2X), enhanced mobile broadband, device-to-device (D2D) communication and non-terrestrial networks.

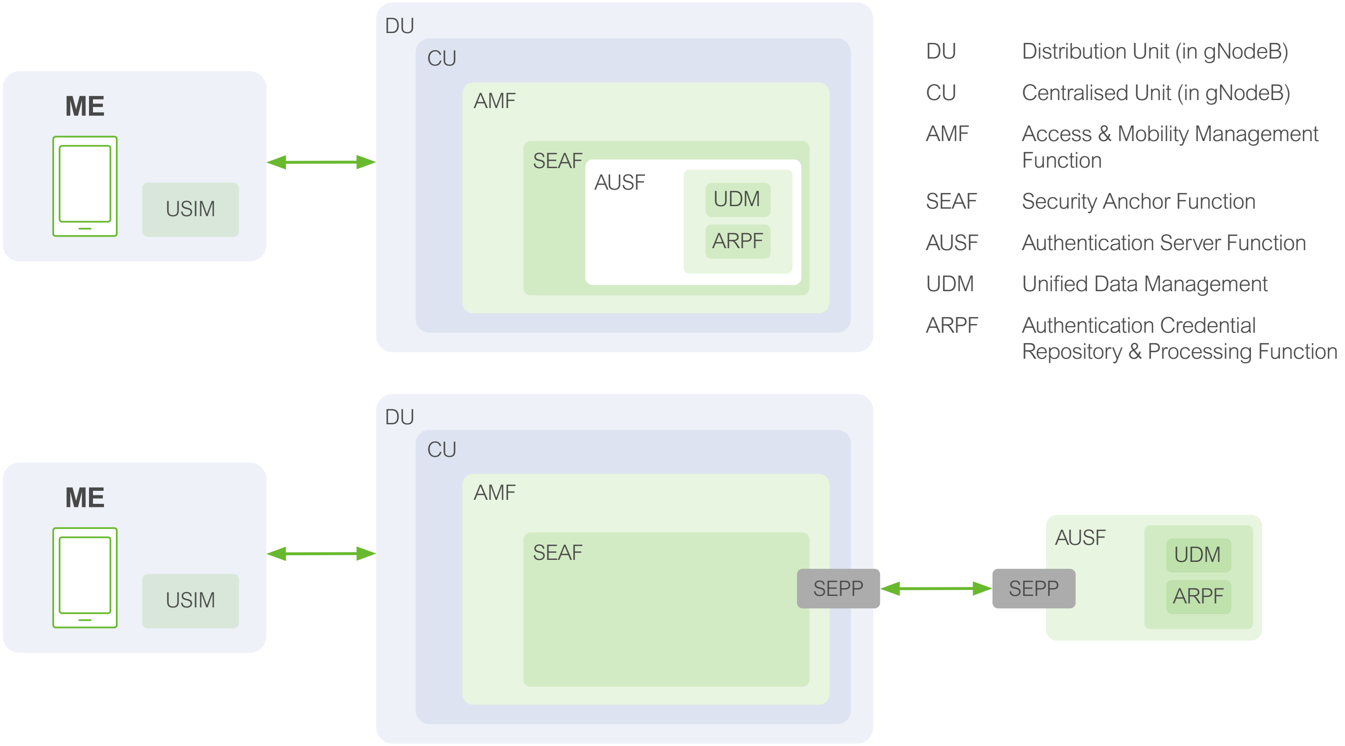
3.2 Trust Model and Key Hierarchy in 5G

The 5G security architecture has been designed to integrate 4G-equivalent security into the 5G system, with the inclusion of additional security mechanisms that defeat new and emerging security threats.

In the 5G system, trust within the network is considered to decrease the further one moves from the core. This is reflected in the 5G key hierarchy.

The trust model in the user equipment (UE) is relatively simple. There are two trust domains; the SIM (based on the tamper-proof UICC) that acts as the trust anchor; and the ME.

[2] In practice, the NR-RAN node, gNodeB, is further divided in two physical entities: Centralised Unit (CU) and Distributed Unit (DU). Only the CU is fully in the physical and logical control of the mobile operator.



DU	Distribution Unit (in gNodeB)
CU	Centralised Unit (in gNodeB)
AMF	Access & Mobility Management Function
SEAF	Security Anchor Function
AUSF	Authentication Server Function
UDM	Unified Data Management
ARPF	Authentication Credential Repository & Processing Function

Figure 3. (a) 5G Trust model and (b) 5G Trust model for roaming scenario

The trust model on the network side has two configurations for non-roaming and roaming cases. The RAN is separated into Distributed Units (DU) and Centralised Units (CU), that together form gNodeB - the 5G base-station.

In the core network, the Access and Mobility Management Function (AMF) serves as termination point for Non-Access Stratum (NAS) security. The Security Anchor Function (SEAF) holds the anchor key for the visited network. The security architecture is defined in a futureproof fashion, having a separation of the security anchor from the mobility function in a future evolution of the system architecture.

In the roaming architecture, the home and the visited network are connected through a Security Protection Proxy (SEPP) for the control plane of the internetwork interconnect.

Authentication Server Function (AUSF) keeps a key for re-use, derived after authentication, in case of simultaneous registration of a ME in different access network technologies (i.e. 3GPP access networks and non-3GPP access networks such as WLAN).

Authentication Credential Repository and Processing Function (ARPF) keeps the authentication credentials. This is mirrored by the USIM on the side of the client (i.e. the UE side). The subscriber information is stored in the Unified Data Repository (UDR). The Unified Data Management (UDM) uses the subscription data stored in UDR and implements the application logic to perform various functions such as authentication credential generation, user identification, service, and session continuity.

3.3 Type of Authentication in 5G

5G allows three types of authentication procedures enabling different use cases and value-added services: 5G Authentication and Key Agreement (5G-AKA), Extensible Authentication Protocol Authentication and Key Agreement (EAP-AKA) and Extensible Authentication Protocol – Transport Layer Security (EAP-TLS). Only 5G-AKA and EAP-AKA are mandatory in 5G.

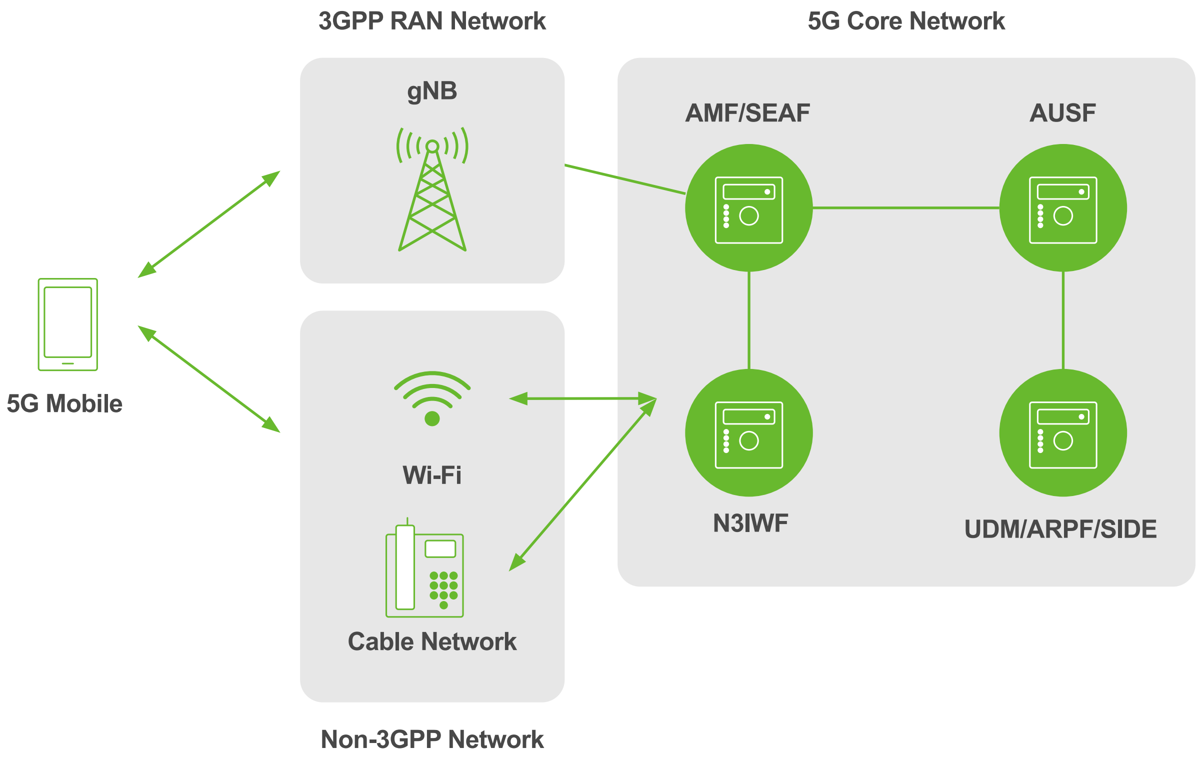
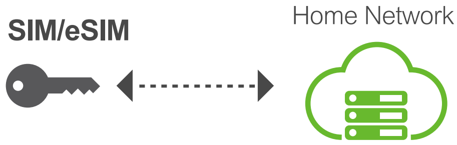


Figure 5. Two ways of accessing a 5G network. AMF (Access and Mobility Management Function), SEAF (Security Anchor Function), AUSF (Authentication Server Function), UDM (Unified Data Management), ARPF (Authentication Credential Repository and Processing Function), SIDF (Subscription Identifier De-concealing Function), N3IWF (Non-3GPP Interworking Function).

5G-AKA

5G-AKA is a mandatory 5G primary authentication method. The 5G Authentication and Key Agreement (AKA) is executed between the network end points: the USIM and the Authentication Credential Repository Function (located in the UDM/ARPF). The USIM provides the concealed identifier (SUCI), and the serving network name from which it is accessing the network.



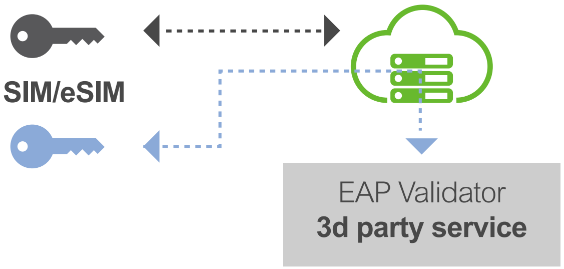
If the access network is authorised, the procedures validate the USIM/ME, and produces confidentiality and integrity keys (CK, IK). From these, a re-usable operational key is derived (KAUSF), from which an "anchor key" (KSEAF) is generated for use by the serving network for subsequent security requests, providing more flexibility and faster response time.

The 5G-AKA is the only procedure used for accessing public mobile networks.

EAP-AKA

EAP-AKA aims to integrate the EAP into the 5G framework. This allows the ME to authenticate to services that have an established relationship with the home network. The procedure is similar in establishing a security "anchor key" (KSEAF), but only after the EAP authentication has been executed.

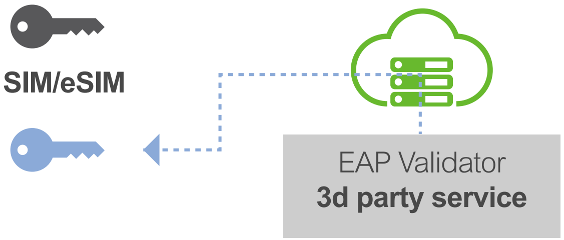
The EAP-AKA allow a seamless connection to a non-3GPP network, using the credentials stored in the 5G SIM



EAP-TLS

The EAP-TLS Authentication and Key Agreement is primarily meant for access to non-3GPP networks. It complements the primary authentication procedure, to authorisation to set-up connections in the user plane. It allows the mobile operator to delegate the authorisation to a third party that provides value-added services. As such, it is categorised as a secondary authentication.

The 5G SIM is not formally involved in the EAP-TLS authentication that is based on PKI infrastructure. However, the 5G SIM can significantly raise the level of security by providing security facilities including certificate storage and validation, and session key establishment. (Source: GSMA)



4. TCA Recommended 5G SIM for 3GPP Release 17

TCA first defined the Recommended 5G SIM in December 2018 to outline which technical features of SIM technology address the challenges mobile operators face, beyond network access, when migrating from 4G to 5G. Subsequently, TCA enhanced the Recommended 5G SIM to align with new use cases introduced by 3GPP's Release 16 for Phase 2 5G deployments. The Recommended 5G SIM has now been updated to align with new features defined in 3GPP Release 17.

4.1 Previous versions

In November 2018, TCA released a set of 3GPP Release 15 technical requirements, including a recommended level of support which mandates the support of SIM-based subscriber privacy at a minimum. Following that, in February 2021, "Trusted Connectivity Alliance Recommended 5G SIM: A Definition" was published. The major introduced improvements were:

- Improved mobile experience – including network slicing and multi-device and multi-identity support.
- Cellular V2X communication – supporting V2X configuration management.
- Enhanced subscriber privacy – addition of SUPI / SUCI support for Network Access Identifier, in addition to the IMSI.
- Private network access – facilitating the same connectivity experience for public and private networks.

4.2 Improvements Introduced by the Release 17 5G SIM

Considering the evolution of 3GPP standards in 2022 with the publication of Release 17 for 5G Phase 2, key new and improved use cases include:

- Improvements in Secure Network Access
- Improvements in roaming services
- Enablement of value-added services and non-3GPP network access
- Enhancement of proximity services
- New Radio Reduced Capability (RedCap) for IoT - NR-Lite
- Enhanced support for standalone private networks.
- Enhanced support for industrial IoT.

In this context, TCA has updated and enhanced its existing technical recommendations to deliver the full benefits of the SIM to 5G Release 17 Phase 2 deployments:

Improvement in Secure Network Access

The access to WLAN has been made more secure and integrated into the 5G framework. When accessing a WLAN network that has a business relation with the issuing mobile operator, a user that has been authenticated to a 5G network using the 5G-AKA, can move from the 3GPP network to a non-3GPP network without having to be reauthenticated.

Separate authentication counter have been introduced for different services while roaming. This allows a more secure and more fine graded control of roaming charges.

Roaming Services

Release 17 introduces several new features for the Steering of Roaming. A specific Steering of Roaming procedure has been introduced for satellite network. This is necessary to cope the specificity of this type of networks, that cover very large areas in some cases spanning more than one country, and non-fix location for satellites based on LEO station.

Disaster roaming has been extended to this type of network with specific parameters.

It is also possible to perform different Steering of Roaming for different services (voice, data, etc) to promote cost optimisation.

Value Added Services and Non-3GPP Access

Authentication and Key Management for Applications (AKMA) is an important security feature introduced to facilitate the adoption of 5G technology in a number of vertical markets. AKMA leverages the Generic Bootstrapping Architecture (GBA) specified in earlier generations, leveraging an operator authentication infrastructure in order to secure the communication between the ME and an Application Function (AF) related to the corresponding vertical market. The migration has also taken into account the requirements of battery constrained devices – Battery Efficient Security for very low Throughput Machine (BEST) – to specify lightweight communication security and key agreement protocols.

The GBA authentication and authorisation procedure of the 5G SIM can be immediately used for GBA/AKMA procedures.

Proximity Services

Proximity Service (ProSe) allow direct communication of two devices. This has been available since LTE Release 12, but Release 17 has further enhanced the support of ProSe in 5G for direct discovery, direct communication, and usage information reporting. In case a device is out of network coverage, another device can act as a relay between the out of coverage device and the network. This is an extremely useful feature for the public safety use-case, and for users owning multiple devices.

The 5G SIM provides a secure and reliable storage of ProSe configuration parameters, authorisation policy, discovery and radio parameters, network relay, all managed by the Network Policy Control Function. 5G SIM offers also secure parameter provision, and usage information reporting.

Reduced Capability Devices

The New Radio for Reduced Capability Devices (RedCap) was previously known as NR-Lite. It addresses the low tier devices, such as industrial wireless sensor networks, video monitoring, low-end wearables and other simple IoT Devices. These devices are usually power constrained.

The 5G SIM in eSIM and integrated SIM form factor is an ideal fit for such class of applications due to their power saving features.

It should also be noted that the privacy-preserving features of 5G is a key factor for objects located in critical infrastructure.

Standalone Private Networks

The support for Private network has been significantly improved for IoT use-cases. The 5G SIM can act as secure credential holder to securely authenticate to a third party using secondary authentication. This can favourably facilitate the deployment of standalone private networks, completely decoupled from public networks.

Industrial IoT

The Release 17 has introduced the uplink connectivity. Thanks to the URLLC, this feature allows device-to-device connectivity in a Time Sensitive Network (TSN) . This is a strong enabler for a wide range of industrial IoT applications requiring low latency, with sensitive time stamping features. The use of a 5G SIM is the only means to guarantee the safety and security normally required in such kind of applications: device identity, device integrity, root of trust, and application specific authentications.

5. Types of 5G SIM

While the 5G SIM enables a device to authenticate to the 5G network, it has additional capabilities defined for different 5G deployment schemes. Trusted Connectivity Alliance has identified two different associated types of 5G SIM:

- **Recommended 5G SIM for Rel. 17:**
  The Recommended 5G SIM is an evolution of the Release 15 and Release 16 5G SIM and incorporates new technical requirements to support the latest Release 17 features, while maintaining full backwards compatibility, to maximise the benefits of 5G Phase 2 deployments.
- **Low Power SIM:**
  A TCA Recommended 5G SIM optimised for Low Power IoT use cases for which NB-IoT may be used. All the features that support extended battery life, as listed in Section 6, shall be supported.

6. Recommended Release 17 5G SIM Use Cases Overview

TCA first defined the Recommended 5G SIM in December 2018 to outline which technical features of SIM technology address the challenges mobile operators face, beyond network access, when migrating from 4G to 5G. Subsequently, TCA enhanced the Recommended 5G SIM to align with new use cases introduced by 3GPP's Release 16 for Phase 2 5G deployments. The Recommended 5G SIM has now been updated to align with new features defined in 3GPP Release 17.

Items shadowed in blue were introduced with Release 17.

Use-case	Technical feature 3GPP	Standard reference 3GPP	Additional details
Network Slicing	User Equipment Route Selection Policy (URSP)	User Equipment Route Selection Policy (URSP) Service n°132 Support for URSP by USIM EFURSP in 3GPP TS 31.102 URSP Rules coding 3GPP 24.526	User Equipment Route Selection Policy (URSP) is used by the UE to determine how to route outgoing traffic depending on capabilities expected by an application. Pre-configured URSP rules are linked to a PLMN and stored in a BER-TLV format in EFURSP under 5G file system.
	Toolkit Support	Network Slicing information support retrieved in the TERMINAL PROFILE: bit 4 of byte 36. Network Slicing information retrieved by PROVIDE LOCAL INFORMATION toolkit command. 3GPP TS 31.111	Network Slicing is the 5G network's ability to guarantee management of broadband and latency connections. Each particular type of application should "see" a network configured in the best way to manage its traffic. Release 16 introduced a modification in the PROVIDE LOCAL INFORMATION toolkit command response. If the terminal supports the service slice information, (bit 4 of byte 36 of TERMINAL PROFILE), the TERMINAL RESPONSE related to a PROVIDE LOCAL INFORMATION USIM request has to contain the Serving PLMN Single Network Slice Selection Assistance Information (S-NSSAI) list. An S-NSSAI, as specified in 3GPP, is comprised of: • A Slice/Service type (SST) • A Slice Differentiator (SD)
	Closed Access Group	CAG information retrieved by PROVIDE LOCAL INFORMATION toolkit command. 3GPP TS 31.111	In Rel.17, the Closed Access Group (CAG) information has been added in the response to the to toolkit command response. The toolkit command returns the CAG ID and the corresponding human readable network name of the detected cell.

Use-case	Technical feature 3GPP	Standard reference 3GPP	Additional details
Enhanced Steering of Roaming Service	Steering of Roaming (SOR) over control plane.	Service N°127 "Control plane of steering of roaming over control plane" 3GPP TS 31.102 3GPP TS 23.122 for mechanism description	5G OTA server fully interconnected with 5G core network functions as defined by 3GPP Rel. 16 SoR-AF: provides PLMN list. SP-AF: builds secure packet. PLMN list secured packet is sent over signalling (control plane) to UICC by OTA server through the UDM. UDM (5G HLR) directly sends PLMN list to User Equipment.
	SoR-CMCI: Steering of Roaming Connected Mode Control Information	Service N°138 "SoR-CMCI storage in USIM" EFSoR-CMCI Id 4F0E storage of SoR-CMCI parameters as per 3GPP TS 24.501 coding. 3GPP TS 23.122 for mechanism description	SoR-CMCI: Steering of Roaming Connected Mode Control Information SoR Rules storage in EFSoR-CMCI ID=4F0E have to be used by the device when service N°138 is activated in the UST. Rules are composed by Timer and criteria of connection interruption based on DNN, Slice information, Voice Call, Video Call, IMS registration related signaling, SMS over NAS …
	Toolkit Support - Refresh command "SoR-CMCI"	Refresh command "SoR-CMCI" 3GPP TS 31.111 3GPP TS 23.122	The support of the SoR-CMCI is indicated in the b4 of byte 36 of the TERMIINAL PROFILE. If supported, after a Refresh SoR-CMCI command, the UICC informs the device that new steering CMCI rules have to be followed.
5G Private Networks	SNPN (Standalone Non-Public Network)	3GPP defined specific AID for a dedicated SNPN USIM, using a non-IMSI SUPI as subscriber identifier. 3GPP TS 31.102, TS 31.101 AID to be defined in ETSI TS 101 220	In a Standalone Non-Public Network (SNPN) operated by an SNPN operator without relying on network functions offered by the PLMN, a SNPN-enabled UE is configured with subscriber identifier (NAI SUPI type, or reserved MCC/MNC) as Subscription Permanent Identifier.
	PNI-NPN (Public Network integrated Non-Public Network)	If IMSI is used as SUPI, regular USIM AID is used. 3GPP defines a specific AID for a dedicated PNI-NPN USIM, using a non-IMSI SUPI as subscriber identifier. 3GPP TS 31.102, TS 31.101 AID to be defined in ETSI TS 101 220	A Public Network integrated Non-Public Network (PNI-NPN) is deployed with the support of a PLMN. In these scenario, the PNI-NPN and the public network share part of the radio access network, while the other network functions remain segregated. As the PNI-NPN is access via the PLMN, the UE shall have a subscription to the PLMN, to subsequently enable the access to the PNI-NPN. Either IMSI or NAI can used as subscriber identifier.
	5G Wireline and Wireless Convergence	3GPP specific NAI SUPI Type, using NSI, GCI, and GLI 3GPP TS 31.102 Coding of NSI, GCI, and GLI TS 23.003	5G Wireless Wireline 3GPP Release 16 finalised convergence of core networks supporting wireline and wireless access. In addition to the IMSI, the Network Access Identifier (NAI), can assume one of the following identifiers, defined in the TS 23.003 relevant clause: - Network Specific Identifier (NSI), as defined in clause 28.7.2 - Global Line Identifier (GLI), as defined in clause 28.15.2 - Global Cable Identifier, as defined in clause 28.16.2. This is advantageous for both customers and network operators. The 5G authentication is performed with the dedicated NAI SUPI Type.

Use-case	Technical feature 3GPP	Standard reference 3GPP	Additional details
5G Private Networks	NAI SUPI Type Dedicated SUPI Type for private Network Access Identifier (NAI) in 5G Network	Service n°130 Support for SUPI of type NSI or GLI or GCI 3GPP defined a specific AID for a USIM, using a non-IMSI SUPI as subscriber identifier. 3GPP TS 31.102 TS 31.101 TS 23.003 AID to be defined in ETSI TS 101 220	If service n°130 is available, the EFSUPI_NAI file shall be present, as defined in TS 31.102. It contains the Network Access Identifier (NAI), that can be the coding of one of the currently defined values: - Network Specific Identifier (NSI), TS 23.003 - Global Line Identifier (GLI), clause 28.15.2 of TS 23.003 - Global Cable Identifier, clause 28.16.2 of TS 23.003 3GPP TS 31.102 Coding of SUPI NAI type 3GPP TS 24.501
Enhanced Subscriber Privacy	Enhancement of GET IDENTITY COMMAND	GET IDENTITY command in 5G, and 5G NSWO Context. 3GPP TS 31.102 and ETSI 102.221	Release 16 introduced an enhancement of the GET IDENTITY COMMAND to support concealment of a SUPI NAI Type in a SUCI context. In order to perform the SUCI calculation (specified in TS 33.501), the USIM shall have available the following information: - Home Network Identifier (MCC/MNC or domain name, depending on SUPI type) - Routing indicator (EFRouting_Indicator) - Home Network Public Key - Home Network key identifier - Protection scheme identifier - SUPI And Services n°124, and 125 are available. With Release 17, the GET IDENTITY command has been extended. If the SUCI calculation is performed by the USIM, and the 5G NSWO support is activated, the USIM calculates and returns the SUCI. The USIM performs the SUCI calculation under the same condition of SUPI context, and only if the SUPI type is IMSI, and Service n°142 (5G NSWO support) is activated.
Non-3GPP Network Access	Trusted non-3GPP network access	Service n°135 Support for Trusted non-3GPP access networks by USIM If service n°135 is available, then EFTN3GPPSNN (Trusted non-3GPP Serving network names list) shall be present.	3GPP specified support of multiple access technologies and the handover between these accesses. It improves a convergence using a unique core network (5GC) providing services over multiple access technologies also for non-3GPP access technologies. Non-3GPP means that these accesses are not specified in the 3GPP. From Release 16 has been defined the non-3GPP trusted access: the mobile operator trusts and operates the access points, the encryption of the radio link is also controlled by the operator and the credentials are derived from the security context in the UE and the network. EFTN3GPPSNN contains the coding for several Serving networks name configured by operator Coding of EFTN3GPPSNN is specified in TS 23.003

Use-case	Technical feature 3GPP	Standard reference 3GPP	Additional details
V2X in 5G Network	C-V2X technology in 5G Network	Service n°119 in EFUST has to be set to support V2X parameters configuration. If the Service is set, the DFV2X must be present in the DFTELECOM	5G technology improves C-V2X technology thanks to lower latency, greater responsiveness, higher reliability, and wider bandwidths. 3GPP have worked on new specifications providing V2X support in 5GS. Services developed on V2X can be grouped in: • Road safety • Traffic management and efficiency • Infotainment and business
	V2X parameters contained in EFs under the DFV2X	EFVST (V2X Service Table) has been updated to support V2X feature in 5GS. The following services have been added: • Service n°2. V2X policy configuration data over PC5 • Service n°3: V2X policy configuration data over Uu EFV2XP_PC5 (V2X data policy over PC5) file has been defined. If service n°2 is set, this file shall be present and contains parameters dedicated to PC5 interface. EFV2XP_Uu (V2X data policy over Uu) file has been defined. If service n°3 is set, this file shall be present and contains parameters dedicated to Uu interface. Specific contents of the above files are defined in 3GPP TS 24.588	The 5G system architecture supports several operation modes for V2X communication. The V2X communication over the PC5 interface allow 5G orchestrated direct UE-to-UE communication. In Rel.16, a second mode of V2X communication was introduced over the Uu interface both in Uplink and Downlink. The Uu interface allow direct communication of two UEs via NG-RAN). Rel.17 extends the Uu interface communication, allowing broadcast and multicast transmission, improving response for time critical message, such as collision alert messages. The existing V2X data policy over PC5 data file (i.e., EFV2XP_PC5) is updated in order to include PC5 DRX configuration policies for V2X services, and also NR-PC5 unicast security policies for V2X, as defined in TS 24.588

Use-case	Technical feature 3GPP	Standard reference 3GPP	Additional details
Ensuring Good Quality of Experience	Multi-Device and Multi-Identity	Service n°134 MuD and MuI configuration data 3GPP TS 31.103 EFMuDMiDConfigData (MuD and MiD Configuration Data) 3GPP TS 24.175	If the Service n°134 is available, the file EFMuDMiDConfigData shall be present. The file contains MuD and MiD configuration data objects as specified in 3GPP TS 24.175. - The Multi-Device (MuD) enables a user to use different UEs that are registered under the same public user identity - The Multi-Identity (MiD) enables a user to use different identities. It enables a served user to use any of its identities. The coding of the file is specified in the 3GPP TS 31.103
	Call control on PDU Session by USIM	Service n°128 Call control on PDU Session by USIM 3GPP TS 31.102 3GPP TS 31.111	The call control on Protocol Data Unit (PDU) session by USIM forces the ME to first pass the corresponding data to USIM before any PDU session establishment.
	Network rejection event	Network Rejection event 3GPP TS 31.111	Network Rejection Event 5GS allows the UICC to retrieve the network rejection codes when network issues prevent connection. In Rel.17 the support for Satellite Network has been added.
	Data connection status Change Event for 5GS	Data Connection Status Change event 3GPP TS 31.111	Informs the UICC that the ME has detected a change in 5GS data connection. In Rel.17 the support for Satellite Network has been added.
	Provide Local information extended to support NG-RAN information	PROVIDE LOCAL INFORMATION proactive command 3GPP TS 31.111	ME provides to UICC information on MNC, MCC, LAC/TAC, Cell ID, NG-RAN cell ID.
	Timing advance information	PROVIDE LOCAL INFORMATION proactive command 3GPP TS 31.111	ME provides UICC with NR primary timing advance as defined in 3GPP 38.211. In Rel.17, the timing advance information for Satellite NG-RAN has been added in the PROVIDE LOCAL INFORMATION toolkit command response.
	Network measurement report	PROVIDE LOCAL INFORMATION proactive command 3GPP TS 31.111	ME provides UICC with available Network measurement reports (NMR) related to NR as defined in 3GPP 38.331.

Use-case	Technical feature 3GPP	Standard reference 3GPP	Additional details
Subscriber Privacy	5GS mobile identity	5G SUPI based on IMSI TS 23.003 5G based on NAI RFC 7542	5G use a globally unique Subscription Permanent Identifier (SUPI). The SUPI can take two forms: - SUPI contains the IMSI, - SUPI is built starting from the Network Access Identifier, as defined in RFC 7542
	Encryption method of SUPI, the Subscription Permanent Identifier for 5G	The SUPI encryption method is defined in 3GPP TS 33.501	The method protects end user privacy by encryption of Subscriber Permanent Identifier (SUPI), previously named IMSI (International Mobile Subscriber Identity), that generates a Subscription Concealed Identifier (SUCI). A mandatory features is that the Home Network Public Key KHN_pu must be stored in the USIM, not in the ME. Outline of the SUCI generation Method: • Step 1: Generation of Ephemeral SIM encryption key pair: EKSIM_pr private and EKSIM_pu public • Step 2: Ephemeral SIM encryption key EEKSIM = F(KHN_pu, EKSIM_pr) • Step 3: Encrypted SUPI = F(EEKSIM, SUPI) • Step 4: SUCI = Home Network ID | KHN_pu | Encrypted SUPI Note that the SUPI is never transmitted in clear, only the SUCI is.
	Services related to the SUPI protection & calculation.	Service n°124 Subscription identifier privacy support EFSUCI_Calc_Info and EFRouting_Indicator Service n°125 SUCI calculation by the USIM 3GPP TS 31.102 3GPP TS 24.501	Two scenarios are possible: If the service n°124 is active, the SUCI calculation is performed by the ME. Then, the following two files must be present which they will used by the ME: • EFSUCI_Calc_Info contains the information needed by the ME to perform the calculations • EFRouting_Indicator it contains the Routing Indicator, a 4 digit code defined by the home network operator, as defined in the 3GPPS TS 24.501 If service n°125 is active (which means is “available” in EFUST), the SUCI calculation is performed by the USIM. In such case the EFSUCI_Calc_Info content should not be made available to the ME.
		Get IDENTITY command 3GPP TS 31.102 and ETSI TS 102 221	ISIM card operating system must support the Get Identity command used by the ME to retrieve the encrypted SUCI computed by the SIM and deliver it to the network each time it is requested.
		SUCI registry API 3GPP TS 31.130	Enable to compute encrypted SUCI from a standalone and interoperable Javacard application using standardised APIs.
	Rel.17, added SUCI 5G NSWO context in GET IDENTITY command	Service n°142 5G NSWO support in SUCI calculation	If service n°142 is activated, then EFSU5GNSWO_CONF file shall be present and the GET IDENTITY command shall be performed in SUCI 5G NSWO context

Use-case	Technical feature 3GPP	Standard reference 3GPP	Additional details
Extended Battery Life[2] for RedCap	Suspend and resume	UICC suspension as defined in 11.1.22 in ETSI TS 102 221	Before switching off, the SIM must store its internal status. When the device resumes the UICC, certain states which were used in a previous card session can be also used in a new card session.
	Poll interval negotiation	Negotiation of Poll Interval as defined in 3GPP TS 31.111	Negotiation between the SIM and the device to find the optimum poll interval that will reduce device activity to save battery while letting the SIM applications contact some servers or the device when required.
	eDRX/PSM	EF AD Administrative Data 3GPP 31.102 & 31.101	The proper personalisation shall be put in the SIM to allow the usage of eDRX to be able to reduce the power consumption of the device.
		Service n° 141 Pre-configured eDRX parameters 3GPP 31.102	If service n°141 is activated, then EF5GSEDRX (5GS eDRX Parameters) shall be present. The content of file specifies: ratType: Radio Access Technology Type; edrxValue: Extended idle mode DRX cycle length. To efficiently support lower complexity IoT devices (e.g., sensors, wearables, video cameras, in general reduced capability devices), Release 17 scales down wideband 5G NR design. This project also enables further energy savings and coexistence with other 5G NR devices. The impact on TS 31.102 is an enhancement of eDRX parametrs
		Service n°121 EARFCN list for MTC/NB-IOT UEs 3GPP 31.102	Contains the geographical areas associated with the EARFCNs for enabling cell search of MTC carrier or NB-IOT carrier.
	USAT Pairing	UE-based procedure with USAT application pairing defined in 3GPP TS 33.187 Security aspects of Machine-Type Communications	The SIM card can be locked to a device or a device type so it would be useless to steal a SIM in a traffic light for example to use it in a smartphone because thanks to this functionality the SIM is locked to a device type: the traffic light. This is especially useful in the IoT context.
Unleashing Deployment of New Services	Remote file and applet management Over The Air	GP 2.2 Amendment B and ETSI TS 102 226	Reaching the SIM to update some data or launch application in an all IP world.
	Access to IMS networks	ISIM ADF and related EF's as defined in 3GPP TS 31.103	Application protocol ISIM application selection IMPI request IMPU request SIP Domain request ISIM service table request P-CSCF address request ISIM session termination
	5G support for the OPEN CHANNEL command	OPEN CHANNEL proactive command 3GPP TS 31.111	Bearer Type NG-RAN must be supported in addition to legacy modes (GPRS, UTRAN, etc…). In Rel.17 the support for Satellite NR-RAN network has been added.

Use-case	Technical feature 3GPP	Standard reference 3GPP	Additional details
Network Resource Optimisation	Unified Access Control	Service n°126 UAC Access Identities support: EF UAC_AIC 3GPP TS 31.102	Prioritisation of multi-media services configured within the SIM
		Service n°127 Steering of UE in VPLMN. 3GPP TS 31.102	If service nº 127 is activated then the device is to receive Steering of Roaming, including the list of preferred networks and access technology combinations, during initial registration in a visited network as specified in 3GPP TS 23.122.
Security	Mobility Management	Service n°122 5GS Mobility Management Information: EF5GS3GPPLOCI, EF5GSN3GPPLOCI, EF5GS3GPPNSC, EF5GSN3GPPNSC Service n°129 5GS Operator PLMN List EFOPL5GS 3GPP TS 31.102	Contains NAS full native security context from 5G Mobility Management Information
	Secondary keys for value added services	Service n°123 5G Security Parameters EF5GAUTHKEYS 3GPP TS 31.102	Several Secure temporary keys are generated for 5G Services, for 3GPP and non-3GPP security context such as WiFi are stored in EF5GAUTHKEYS: - KAUSF is generated by the Authentication Server Function (AUSF) used for authentication in the home network, and for reuse in case of simultaneous registration of a UE in different access network technologies. 3GPP access networks and non-3GPP access networks such as WLAN. - A service network specific anchor key, KSEAF provided by the AUSF to the SEAF as base for authentication in visited networks, which can be used for more than one security context. - The Access and Mobility Function (AMF) derives the key KAMF from the KSEAF. It is used to separate mobility security anchor KAMF. from security anchor KSEAF, and pre-empt any AMF insecure locations.

Use-case	Technical feature 3GPP	Standard reference 3GPP	Additional details
ProSe Proximity Services	ProSe Proximity Services in 5G Network	Service n°139 5G ProSe 3GPP TS 31.102	Proximity Service (ProSe) for direct communication of two devices has been available since LTE Rel.12. Release 17 has further enhanced the support in 5G of ProSe for direct discovery, direct communication, UE-to-network relay, remote UE, and usage information reporting. The communication is usually via the NR-RAN. In case a device is out of network coverage, another device can act as a relay between the out of coverage device and the network, an extremely useful feature for the Public Safety use case.
	Provisioning of Configuration information	Service n°139 5G ProSe If the Service is set, the DF5GProSe must be present in the DF5GS	The service 139 specifies the configuration parameter for 5G Proximity Services discovery, affecting: ProSe direct discovery parameters, HPLMN Function, Direct Communication, Discovery, and announcing of radio parameters policy parameters, group counter, Usage Information Reporting configuration, UICC ProSe Direct Communication usage information reporting Group Member Discovery parameters, and Relay parameters If service n°139 is activated, DF5GProSe folder and file EF5G_PROSE_ST shall be present. EF5G_PROSE_ST indicates which 5G ProSe services are available, other files presence depends of EF5G_PROSE_ST content.
	Configuration parameters for 5G ProSe UE-to-network relay	EF5G_PROSE_ST 5G ProSe Service Table 3GPP TS 31.102	The EF5G_PROSE_ST file indicates which ProSe services are available. In Rel.17. Four ProSe services are available: - direct discovery, - direct communication, - UE-to-network relay UE, - remote UE For each service that is present, the corresponding configuration file must exist.
		EF5G_PROSE_DD 3GPP TS 31.102 3GPP TS 24.555	The file contains the 5G ProSe policy for direct discovery, such as validity timer, NG-RAN service, UE ID, default destination layer-2, and group member information.
		EF5G_PROSE_DC 3GPP TS 31.102 3GPP TS 24.555	The file contains the 5G ProSe policy for direct communication, such as validity timer, NG-RAN service, NR-PC5 information.
		EF5G_PROSE_U2NRU 3GPP TS 31.102 3GPP TS 24.555	The file contains the 5G ProSe configuration data for UE-to-network relay.

6.1 Recommended Release 17 5G SIM versus Release 16 5G SIM

Use-cases	3GPP Technical Feature	Present in Rel. 16	Addition / Enhancement in Rel. 17
Network Slicing	User Equipment Route Selection Policy (URSP)	✗	✗
	Toolkit Support	✗	✗
	Closed Access Group		✗
Enhanced Steering of roaming Service	Steering of Roaming (SOR) over control plane.	✗	✗
	SoR-CMCI: Steering of Roaming Connected Mode Control Information	✗	✗
	Toolkit Support - Refresh command “SoR-CMCI”		✗
5G Private Networks	SNPN (Standalone Non-Public Network)	✗	✗
	PNI-NPN (Public Network integrated Non-Public Network)	✗	✗
	5G Wireline and Wireless Convergence	✗	✗
	NAI SUPI Type Dedicated SUPI Type for private Network Access Identifier in 5G Network	✗	
Enhanced Subscriber Privacy	Enhancement of GET IDENTITY COMMAND	✗	✗
Non-3GPP Network Access	Trusted non-3GPP network access	✗	✗
V2X in 5G Network	C-V2X technology in 5G Network	✗	✗
	V2X Parameters contained in EFs under the DFV2X		✗
Ensuring Good Quality of Experience	Multi-device and Multi-identity	✗	
	Call control on PDU Session by USIM	✗	✗
	Network Rejection Event	✗	✗
	Data Connection Status Change Event for 5GS	✗	✗
	Provide Local information extended to support NG-RAN information	✗	✗
	Timing Advance Information	✗	✗
	Network Measurement Report	✗	✗

6.1 Recommended Release 17 5G SIM versus Release 16 5G SIM

Use-cases	3GPP Technical Feature	Present in Rel. 16	Addition / Enhancement in Rel. 17
Subscriber Privacy	5GS mobile identity	✗	✗
	Encryption method of SUPI, the Subscription Permanent Identifier for 5G	✗	
	Services related to the SUPI protection & calculation.	✗	✗
	Rel.17, added SUCI 5G NSWO context in GET IDENTITY command		✗
Extended Battery Life for RedCap	Suspend and resume	✗	✗
	Poll interval negotiation	✗	✗
	eDRX/PSM	✗	✗
	USAT Pairing	✗	✗
Unleashing Deployment of New Services	Remote file and applet management Over The Air	✗	✗
	Access to IMS networks	✗	✗
	5G support for the OPEN CHANNEL command	✗	✗
Network Resource Optimization	Unified Access Control	✗	
Security	Mobility Managment	✗	✗
	Secondary keys for value added services	✗	✗
ProSe Proximity Services	ProSe Proximity Services in 5G Network		✗
	Provisioning of Configuration information		✗
	Configuration parameters for 5G ProSe UE-to-network relay		✗

7. Conclusion

The Release 16 5G SIM recommended by TCA included technical features which addressed the many challenges, beyond network access, faced by mobile operators as they migrated to 5G networks. Now, with momentum for 5G Phase 2 deployments building, TCA strongly recommends the adoption of the enhanced Recommended 5G SIM to fully benefit from the opportunities presented by 3GPP Release 17, while maintaining full backwards compatibility.

For more 5G insights:

Visit TCA's YouTube channel to watch a recording of our webinar
'Recommended 5G SIM: Unlocking the benefits and opportunities of Release 17'.

Subscribe to the TCA newsletter and follow us on Twitter and LinkedIn to stay up to date on the latest news and resources.

Visit the TCA website to read and download TCA educational and technical materials
www.trustedconnectivityalliance.org

8. About Trusted Connectivity Alliance

Trusted Connectivity Alliance (TCA) is a global, non-profit industry association working to enable trust in a connected future. The organisation’s vision is to drive the sustained growth of a connected society through trusted connectivity which protects assets, end user privacy and networks.

TCA members are leaders within the global Tamper Resistant Element (TRE) ecosystem and work collectively to define requirements and provide deliverables of a strategic, technical and marketing nature. This enables all stakeholders in our connected society to benefit from the most stringent secure connectivity solutions that leverage TCA members’ expertise in tamper proof end-to-end-security.

TCA members are:

CARD CENTRIC LIMITED CARD CENTRIC

COMPRION

东信和平 EASTCOMPEACE

Giesecke+Devrient Creating Confidence

IDEMIA

Kigen

Linxens crafting the future of connections

NXP

OASIS Embed. Connect. Activate

Qualcomm

ST life.augmented

THALES

Valid

WORKZ

TIANYU