

Trusted Connectivity Alliance Recommended 5G SIM: A Definition

February 2021

Copyright © 2021 Trusted Connectivity Alliance Ltd.

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. What is a 5G SIM?.....	4
2. Types of 5G SIM.....	4
3. Recommended 5G SIM Use Cases.....	5
3.1 Recommended 5G SIM – Impact Overview	6
3.2 Recommended 5G SIM – Use Case Overview	7
3.3 Recommended 5G SIM versus Rel 15 5G SIM.....	12
4. Conclusion.....	13

1. What is a 5G SIM?

A SIM (also known as a Universal Integrated Circuit Card or UICC) is the only platform which can be used to secure access to a 3GPP Release 15, 16 or 17 network core (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, NB-IoT, 5G New Radio or other supported non-3GPP radio bearers, such as Wi-Fi.

In November 2018, the Trusted Connectivity Alliance (TCA, formerly known as SIMalliance) 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.

In the same way as the network core architecture is evolving, the SIM is evolving to meet new challenges and opportunities introduced by 5G.

Considering the evolution of 3GPP standards in 2020 with Release 16 for 5G Phase 2, key new use cases including “Network Slicing”, “Enhanced Steering of Roaming”, “Private Networks”, “Enhanced Subscriber Privacy”, “Non-3GPP Network Access” and “Vehicle-to-Everything (V2X) Communication” introduce valuable 5G SIM features in addition to the existing Release 15 functionality.

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

2. 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 (Rel 16):** The Recommended 5G SIM is an evolution of the Release 15 5G SIM and incorporates new technical requirements to support the latest Release 16 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 3.2, shall be supported.

3. Recommended 5G SIM Use Cases

In the first release of this document, TCA identified use cases from 3GPP Release 15 that are supported by a 5G UICC platform. The Recommended 5G SIM has now been enhanced to include new use cases introduced in Release 16.

Table 3.1 lists the Release 16 use cases and highlights which actors are impacted:

- **SIM** – the Secure Element hosting the USIM application.
- **Device Endpoint** – the mobile equipment hosting the SIM.
- **Non-Standalone Network** – a 5G network that still uses control plane of an existing 4G LTE network for control functions, while 5G NR is exclusively focused on the user plane.
- **Standalone Network** – a pure 5G network using 5G technology for both signalling and information transfer.
- **Private Network** – a non-public network able to use 5G core network to deploy services.

Table 3.2 then provides a guide on the changes made to the SIM operating system and the configurations to be completed in the USIM to support 5G network services, specified in Release 16. Table 3.3 then provides a comparison between the features of the Release 15 5G SIM and the enhanced Recommended 5G SIM.

3.1 Recommended 5G SIM – Impact Overview

	SIM	Device Endpoint	Non-Standalone	Standalone	Private
Network Slicing support: Pre-configuration of Mobile device (URSP)	X	X			
Network Slicing support: Toolkit evolutions	X	X		X	
Enhanced Steering of roaming service: Secure messaging over NAS	X	X (already in Rel 15)		X	X
5G Private Networks: Support for SNPN	X	X		X	X
5G Private Networks: Support for PNI-NPN	X	X		X	X
5G Private Networks: 5G NAI SUPI Type	X	X		X	X
5G Private Networks: Wireless / Wireline Convergence	X	X		X	X
Enhanced Subscriber Privacy: NAI SUPI concealment	X	X		X	X
Non-3GPP Network Access	X	X		X	X
V2X in 5G Network	X	X	X	X	
Ensuring Good Quality of Experience: Multi-Device and Multi-Identity	X	X	X	X	X

3.2 Recommended 5G SIM – Use Case Overview

Use-case	Technical feature 3GPP	Standard reference 3GPP	Additional details
Network Slicing	User Equipment Route Selection Policy (URSP)	<p>Service n°132 Support for URSP by USIM EF_{URSP} 3GPP TS 31.102</p> <p>URSP Rules coding in 3GPP 24.526</p>	<p>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.</p> <p>Pre-configured URSP rules are linked to a PLMN and stored in a BER-TLV format in EF URSP under 5G file system.</p>
	Toolkit Support	<p>Network Slicing information support retrieved in the TERMINAL PROFILE: bit 4 of byte 36.</p> <p>Network Slicing information retrieved by PROVIDE LOCAL INFORMATION toolkit command.</p> <p>3GPP TS 31.111</p>	<p>Network Slicing is the 5G networks 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.</p> <p>Release 16 introduced a modification in the PROVIDE LOCAL INFORMATION toolkit command. 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.</p> <p>An S-NSSAI, as specified in 3GPP, is comprised of:</p> <ul style="list-style-type: none"> • A Slice/Service type (SST) • A Slice Differentiator (SD)
Enhanced Steering of roaming Service	Steering of Roaming (SOR) over control plane.	<p>3GPP TS 31.102 with UST service N°127 "Control plane of steering of roaming over control plane"</p> <p>3GPP TS 23.122 for mechanism description</p>	<p>5G OTA server fully interconnected with 5G core network functions as defined by 3GPP Rel. 16</p> <p>SoR-AF: provides PLMN list. SP-AF: builds secure packet. PLMN list secured packet is sent over signaling (control plane) to UICC by OTA server through the UDM. UDM (5G HLR) directly sends PLMN list to User Equipment.</p>
5G Private Networks	SNPN (Standalone Non-Public Network)	<p>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</p>	<p>A Standalone Non-Public Network (SNPN) is assumed to be operated by an SNPN operator without relying on network functions offered by the PLMN. An SNPN-enabled UE is configured with subscriber identifier (NAI SUPI type, or reserved MCC/MNC) as Subscription Permanent Identifier.</p>
	PNI-NPN (Public Network integrated Non-Public Network)	<p>If IMSI is used as SUPI, regular USIM AID is used.</p> <p>3GPP defined 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</p>	<p>A Public Network integrated Non-Public Network (PNI-NPN) is deployed with the support of a PLMN. In these scenarios, the NPN and the public network share part of the radio access network, while other network functions remain segregated. Public Network Integrated NPNs are NPNs made available via PLMNs. When a PNI-NPN is made available via a PLMN, then the UE shall have a subscription for the PLMN to access PNI-NPN. IMSI or NAI are used as subscriber identifier.</p>

	<p>NAI SUPI Type Dedicated SUPI Type for private Network Access Identifier in 5G Network</p>	<p>Service n°130 Support for SUPI of type NSI or GLI or GCI EF_{SUPI_NAI} 3GPP defined a specific AID for a 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</p>	<p>If service n°130 is available EF SUPI_NAI file shall be present, containing coding of possible NAIs today defined by 3GPP. 3GPP TS 31.102 Coding of SUPI NAI type 3GPP TS 24.501</p>
	<p>5GWWC</p>	<p>3GPP specific NAI SUPI Type GCI (Global Cable Identifier) GLI (Global Line Identifier) 3GPP TS 31.102 Coding of GCI and GLI is specified in 3GPP TS 23.003</p>	<p>5G Wireless Wireline 3GPP Release 16 finalized convergence of core networks supporting wireline and wireless access. Advantages are for both parties, customers and network operators. 5G authentication is performed with dedicated NAI SUPI Type.</p>
<p>Enhanced Subscriber Privacy</p>	<p>Enhancement of Release 15 GET IDENTITY COMMAND</p>	<p>GET IDENTITY command 3GPP TS 31.102 and ETSI 102.221</p>	<p>In Release 16 an enhancement of the GET IDENTITY COMMAND has been introduced to support concealment of a SUPI NAI Type.</p>
<p>Non-3GPP Network Access</p>	<p>Trusted non-3GPP network access</p>	<p>Service n°135 Support for Trusted non-3GPP access networks by USIM If service n°135 is available EF_{TN3GPPSNN} (Trusted non-3GPP Serving network names list) shall be present.</p>	<p>3GPP specified support of multiple access technologies and also the handover between these accesses. The idea is to improve 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 were not specified in the 3GPP. In Release 16 has been defined the non-3GPP trusted access: the mobile operator trusts and operates the access points, i.e. 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 EF_{TN3GPPSNN} is specified in TS 23.003</p>
<p>V2X in 5G Network</p>	<p>C-V2X technology in 5G Network</p>	<p>Service n°119 in EF_{UST} has to be set to support V2X parameters configuration. EF_{VST} (V2X Service Table) has been updated to support V2X feature in 5GS. Following services have been added: Service n°2: V2X policy configuration data over PC5 Service n°3: V2X policy configuration data over Uu EF_{V2XP_PC5} (V2X data policy over PC5) file has been defined. If service n°2 is set, this file shall</p>	<p>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:</p> <ul style="list-style-type: none"> • Road Safety • Traffic management & efficiency • Infotainment & Business

		<p>be present and contains parameters dedicated to PC5 interface.</p> <p>EF_{V2XP_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.</p> <p>Specific contents of the above files is defined in 3GPP TS 24.588</p>	
Ensuring Good Quality of Experience	Multi-device and Multi-identity	<p>Service n°2 1 MuD and Mul configuration data 3GPP TS 31.103</p> <p>EF_{MuDMIDConfigData} (MuD and MiD Configuration Data) 3GPP TS 24.175</p>	<p>The Multi-Device (MuD) enables a user to use different UEs that are registered under the same public user identity.</p> <p>The Multi-Identity (MiD) enables a user to use different identities. It enables a served user to use any of its identities.</p>
	Call control on PDU Session by USIM	<p>Service n°128 Call control on PDU Session by USIM 3GPP TS 31.102</p>	<p>The call control on PDU session by USIM forces the ME to first pass the corresponding data to USIM before any PDU session establishment.</p>
	Network Rejection Event	<p>Network Rejection event 3GPP TS 31.111</p>	<p>Network Rejection Event 5GS allows the UICC to retrieve the network rejection codes when network issues prevent connection.</p>
	Data Connection Status Change Event for 5GS	<p>Data Connection Status Change event 3GPP TS 31.111</p>	<p>Informs the UICC that the ME has detected a change in 5GS data connection.</p>
	Provide Local information extended to support NG-RAN information	<p>PROVIDE LOCAL INFORMATION proactive command 3GPP TS 31.111</p>	<p>ME provides to UICC information on MNC, MCC, LAC/TAC, Cell ID, NG-RAN cell ID.</p>
	Timing Advance Information	<p>PROVIDE LOCAL INFORMATION proactive command 3GPP TS 31.111</p>	<p>ME provides UICC with NR Primary Timing Advance as defined in 3GPP 38.211.</p>
	Network Measurement Report	<p>PROVIDE LOCAL INFORMATION proactive command 3GPP TS 31.111</p>	<p>ME provides UICC with available Network measurement reports (NMR) related to NR as defined in 3GPP 38.331.</p>
Subscriber Privacy	Encrypted SUPI Subscription Permanent Identifier for 5G	<p>The method to protect end user privacy by encryption of subscriber identifier previously named IMSI (International Mobile Subscriber Identity) is defined in the standard 3GPP TS 33.501</p>	<p>MANDATORY: Home Network Public Key has to be stored in the USIM and not in the ME.</p> <p>Step 1: Ephemeral SIM encryption key pair generation (private and public).</p> <p>Step 2: Ephemeral SIM encryption key = f(Home Network's public key, ephemeral SIM encryption private key)</p> <p>Step 3: Encrypted SUPI = f(ephemeral SIM encryption key, SUPI)</p> <p>SUCI = HN ID HN public key ID encrypted SUPI SUCI stands for Subscription Concealed Identifier</p>
		<p>Service n°124 Subscription identifier privacy support EF_{SUCI_Calc_Info} and EF_{RoutingIndicator} 3GPP TS 31.102</p>	<p>End user privacy activation. If service n°124 is activated then EF SUCI_Calc_Info shall be present and EF RoutingIndicator shall be present. If service n°124 is deactivated then EF SUCI_Calc_Info shall not be present.</p>

		Service n°125 SUCI calculation by the USIM 3GPP TS 31.102	If service 125 SUCI calculation by the USIM is activated then EF SUCI_Calc_Info shall not be present.
		Get IDENTITY command 3GPP TS 31.102 and ETSI TS 102 221	SIM 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.
Extended Battery Life¹	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°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 GP 2.2 Amendment B and ETSI TS 102 226	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		Reaching the SIM to update some data or launch application in an all IP world.
	Access to IMS networks	ISIM ADF and related Efs 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...).
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 n° 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		Service n°122 5GS Mobility Management Information: EF 5GS3GPPLOCI, 5GSN3GPPLOCI, EF 5GS3GPPNSC, EF 5GSN3GPPNSC	Contains NAS full native security context from 5G Mobility Management Information

¹ Note these features only apply to a Recommended 5G SIM optimised for Low Power IoT use -cases.

		<p>Service n°129 5GS Operator PLMN List EF OPL5GS 3GPP TS 31.102</p>	
		<p>Service n°123 5G Security Parameters EF 5GAUTHKEYS 3GPP TS 31.102</p>	<p>Secure temporary keys for 5G but also non 3GPP security context such as WiFi are stored in EF 5GAUTHKEYS: A key called KAUSF derived from CK/IK, left at the AUSF and that home operator can use on its own policy. An anchor key called the KSEAF provided by the AUSF to the SEAF, which can be used for more than one security context. A derived key per security context called KAMF.</p>

3.3 Recommended 5G SIM versus Rel 15 5G SIM

Use-case	Technical feature 3GPP	5G SIM (Rel 15)	Recommended 5G SIM (Rel 16)
Network Slicing	User Equipment Route Selection Policy (URSP)		X
	Toolkit Support		X
Enhanced Steering of Roaming Service	Steering of Roaming (SOR) over control plane.	X	X
5G Private Networks	SNPN (Standalone Non-Public Network)		X
	PNI-NPN (Public Network integrated Non-Public Network)		X
	NAI SUPI Type Dedicated SUPI Type for private Network Access Identifier in 5G Network		X
	5GWWC		X
Enhanced Subscriber Privacy	Enhancement of Release 15 GET IDENTITY COMMAND		X
Non-3GPP Network Access	Trusted non-3GPP network access		X
V2X in 5G Network	C-V2X technology in 5G Network		X
Ensuring Good Quality of experience	Multi-device and Multi-identity		X
	Call control on PDU Session by USIM	X	X
	Network Rejection Event	X	X
	Data Connection Status Change Event for 5GS	X	X
	Provide Local information extended to support NG-RAN information	X	X
	Timing Advance Information	X	X
Subscriber Privacy	Network Measurement Report	X	X
	Encrypted SUPI Subscription Permanent Identifier for 5G	X	X
Extended Battery Life²	Suspend and resume	X	X
	Poll interval negotiation	X	X
	eDRX/PSM	X	X
	EARFCN list for MTC/NB-IoT UEs	X	X
	USAT Pairing	X	X
Deployment of New Services	Remote file and applet management Over The Air	X	X
	Access to IMS networks	X	X
	5G support for the OPEN CHANNEL command	X	X
Network Resource Optimisation	Unified Access Control	X	X
		X	X
Security	Mobility Management Information	X	X
	5G Security Parameters EF 5GAUTHKEYS	X	X

² Note these features only apply to a Recommended 5G SIM optimised for Low Power IoT use -cases.

4. Conclusion

The Release 15 5G SIM originally recommended by TCA included technical features which addressed the many challenges, beyond network access, faced by Mobile Network Operators (MNOs) 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 16, while maintaining full backwards compatibility.