3GPP R15 5G SIM Card: A Definition

Published by simalliance now Trusted Connectivity Alliance

November 2018

Contents:

1 - What is a 5G SIM?

A Universal Integrated Circuit Card or UICC (better known as a SIM) is the only platform which can be used to secure 5G network access according to the 5G standardisation body (3GPP). In the same way as the network is evolving, the UICC is evolving to meet new challenges introduced by 5G.

The SIMalliance Recommended 5G SIM is a 5G UICC defined as a 3GPP R15 UICC which supports UICC based subscriber privacy at minimum.

2 – Three different types of 5G SIM

While the 5G UICC enables a device to authenticate to the 5G network, it has some additional capabilities, defined for different 5G deployment schemes. SIMalliance has identified three different associated types of 5G UICC:

- *Transitional SIM*: Provides the minimum capabilities to authenticate to the network but does not leverage the benefit of 5G Core Network investment. This is more applicable to early drop for a transition to full 5G deployment where the Recommended 5G SIM is more appropriate.
- *Recommended 5G SIM*: Leverages the full power of 5G phase 1 for enhanced mobile broadband. SIMalliance recommends adopting the Recommended 5G SIM at 5G launch as there is full backward compatibility and it is the most future-proof SIM.
- *Low Power SIM*: Optimised for Low Power IoT use cases for which NB-IoT and LTE-M can be used.

The 3 types of 5G UICC are characterised as follows:

Category	Technical feature 3GPP R15	Standard reference 3GPP R15	Additional details	Transitional SIM	Recommended 5G SIM	Low Power SIM
Ensuring good quality of experience	Call control on PDU Session by USIM	**Service n°128** Call control on PDU Session by USIM 3GPP TS 31.102	The call control on PDU session by USIM forces the ME to first pass the corresponding data to USIM before any PDU session establishment.		X	X
	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.		X	X
	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.		X	X
	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.		X	X
	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.		X	X
	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.		X	X
Subscriber privacy	Encrypted SUPI Subscription Permanent Identifier for 5G	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	MANDATORY: Home Network Public Key has to be stored in the USIM and not in the ME. Step 1: Ephemeral SIM encryption key pair generation (private and public). Step 2: Ephemeral SIM encryption key = f(Home Network's public key, ephemeral SIM encryption private key) Step 3: Encrypted SUPI = f(ephemeral SIM encryption key, SUPI) SUCI = HN ID | HN public key ID | encrypted SUPI SUCI stands for Subscription Concealed Identifier		X	
		Service n°124 Subscription identifier	End user privacy activation. If service n°124 is activated then EF		X	

		privacy support 3GPP TS 31.102	SUCI_Calc_Info shall be present. If service n°124 is deactivated then EF SUCI_Calc_Info shall not be present.			
		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.		X	
		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.		X	
		SUCI registry API 3GPP TS 31.130	Enable to compute encrypted SUCI from a standalone and interoperable Javacard application using standardised APIs.		X	
Extended battery life	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.			X
	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.			X
	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.			X
		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.			X
	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.			X
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.	X	X	X
	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	X	X	

			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…).	X	X	X
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		X	X
		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.		X	X
Security		**Service n°122** 5GS Mobility Management Information: EF 5GS3GPPLOCI, 5GSN3GPPLOCI, EF 5GS3GPPNSC, EF 5GSN3GPPNSC 3GPP TS 31.102	Contains NAS full native security context from 5G Mobility Management Information	X	X	X
		Service n°123 5G Security Parameters EF 5GAUTHKEYS 3GPP TS 31.102	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.	X	X	X

3 – Conclusion

SIMalliance strongly advises that the Recommended 5G SIM is adopted at 5G launch as there is full backward compatibility and it is the most future-proof SIM. The Recommended 5G SIM helps Mobile Network Operators (MNOs) and their customers to make the best use of their 5G investments as detailed below, and in further detail in the '5G SIM: Maximising MNO Investment in 5G Networks' presentation which can be found on the SIMalliance website.

Challenges faced by MNOs	How the Recommended 5G SIM helps
Ensuring a good Quality of Experience	Quality of Experience monitoring
Subscriber privacy	Subscriber ID encrypted
Extended battery life	Features to reduce power consumption
Delivery of all IP services	Authentication to the IMS / SIM can be refreshed through HTTPs
Network resource optimisation	Service prioritisation stored in SIM
Security	5G network access security