CBRS Network Services Use Cases and Requirements

CBRSA-TS-1001

V4.1.0 (Rev 5.0 moving to V5.0.0)

18-01-2022

THIS SPECIFICATION IS PROVIDED "AS IS," WITHOUT ANY REPRESENTATION OR WARRANTY OF ANY KIND, EXPRESS, IMPLIED, OR STATUTORY; AND TO THE MAXIMUM EXTENT PERMITTED BY LAW, CBRS ALLIANCE, AS WELL AS ITS MEMBERS AND THEIR AFFILIATES, HEREBY DISCLAIM ANY AND ALL REPRESENTATIONS AND WARRANTIES, INCLUDING WITHOUT LIMITATION ANY WARRANTIES OF MERCHANTABILITY, TITLE, NON-INFRINGEMENT, FITNESS FOR A PARTICULAR PURPOSE, ACCURACY, OR RELIABILITY, OR ARISING OUT OF ANY ALLEGED COURSE OF PERFORMANCE, DEALING OR TRADE USAGE. ANY PERMITTED USER OR IMPLEMENTER OF THIS SPECIFICATION ACCEPTS ALL RISKS ASSOCIATED WITH THE USE OR INABILITY TO USE THIS SPECIFICATION.

THE PROVISION OR OTHER PERMITTED AVAILABILITY OF OR ACCESS TO THIS SPECIFICATION DOES NOT GRANT ANY LICENSE UNDER ANY PATENT OR OTHER INTELLECTUAL PROPERTY RIGHTS ("IPR"). FOR MORE INFORMATION REGARDING IPR THAT MAY APPLY OR POTENTIAL AVAILABILITY OF LICENSES, PLEASE SEE THE CBRS ALLIANCE IPR POLICY. [Include web link if appropriate] CBRS ALLIANCE TAKES NO POSITION ON THE VALIDITY OR SCOPE OF ANY PARTY'S CLAIMED IPR AND IS NOT RESPONSIBLE FOR IDENTIFYING IPR.

TO THE MAXIMUM EXTENT PERMITTED BY LAW, UNDER NO CIRCUMSTANCES WILL CBRS ALLIANCE, OR ANY OF ITS MEMBERS OR THEIR AFFILIATES, BE LIABLE FOR DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, EXEMPLARY, PUNITIVE, OR OTHER FORM OF DAMAGES, EVEN IF SUCH DAMAGES ARE FORESEEABLE OR IT HAS BEEN ADVISED OR HAS CONSTRUCTIVE KNOWLEDGE OF THE POSSIBILITY OF SUCH DAMAGES, ARISING FROM THE USE OR INABILITY TO USE THIS SPECIFICATION, INCLUDING WITHOUT LIMITATION ANY LOSS OF REVENUE, ANTICIPATED PROFITS, OR BUSINESS, REGARDLESS OF WHETHER ANY CLAIM TO SUCH DAMAGES SOUNDS IN CONTRACT, WARRANTY, TORT (INCLUDING NEGLIGENCE AND STRICT LIABILITY), PRODUCT LIABILITY, OR OTHER FORM OF ACTION.

Table of Contents

1. Introduction and Scope 6
1.1 Key Words 6
2. References 6
3. Abbreviations and Definitions 7
3.1 Abbreviations 7
3.2 Definitions 10
4. CBRS Network Services Use Cases, Feature and Functionality Description 13
4.1 Introduction 13
4.2 Use Cases 16
4.2.1 Service Provider Use Case 16
4.2.2 CBRSA NHN Use Case 17
4.2.3 Private Network (LTE & NR) and NR Non-Public Network 18
4.2.3.1 Single Subscription UE Use Case 19
4.2.3.2 Multi-subscription UE Use Case 19
4.2.3.3 LTE Private Network 21
4.2.3.4 NR PRIVATE NETWORK 21
4.2.3.5 NR Non-Public Network 21
4.2.3.5.1 Stand-alone Non-Public Network 21
4.2.3.5.2 Public Network Integrated Non-Public Network 22
4.2.4 Hybrid Network Use Case 22
4.2.5 Fixed Wireless Network Use Case 23
4.2.6 5G NR EN-DC Use Case 25
4.3 Features/Functionalities 28
4.3.1 CBRS UE Profile 28
4.3.1.1 CBRS LTE UE Profile 28
4.3.1.2 CBRS 5G NR UE Profile 30

4.3.2 Traffic LBO (Traffic Local Break Out) 32
4.3.2.1 Traffic LBO - Use Case Mapping 33
4.3.3 Roaming Support 33
4.3.3.1 Roaming Support For Data Only Services 34
4.3.3.2 Roaming Support For IMS-Based Services 34
4.3.3.3 Roaming Support – Use Case Mapping 34
5. Network Service Requirements 35
5.1 Use Case Requirements 35
5.1.1 CBRSA NHN Use Case 35
5.1.1.1 CBRSA NHN RAN Share Requirements 35
5.1.1.2 CBRSA NHN RAN Discovery Requirements 36
5.1.1.3 CBRSA NHN Authentication Requirements 36
5.1.1.4 CBRSA NHN Mobility Requirements 36
5.1.1.5 CBRSA NHN General Security Requirements 37
5.1.1.6 CBRSA NHN Measurement Requirements 37
5.1.2 MSO Use Case 38
5.1.2.1 MSO Specific RAN Requirements 38
5.1.3 Fixed Wireless Network Use Case 38
5.1.3.1 CBRSA Fixed Wireless Network Access Architecture Requirements 38
5.1.3.2 CBRSA Fixed Wireless Network Access Service Requirements 39
5.2 CBRS Network Feature/Functionalities Requirements 39
5.2.1 3GPP-based Access Mode (Non-EPS-AKA) 39
5.2.1.1 General Requirements 39
5.2.1.2 Authentication Requirements 40
5.2.2 UE ReQuirements 40
5.2.2.1 LTE UE Requirements 40
5.2.2.2 UE NR Requirements 42

5.2.2.3 UE Requirements for GeoFENCING 44
5.2.2.4 UE Requirements for TAC COLLISION AVOIDANCE 45
5.2.3 Traffic LBO Requirements 46
5.2.3.1 Traffic LBO Architecture Requirements 46
5.2.4 Roaming Requirements for CBRS Networks 46
5.2.4.1 Roaming Requirements for Data Only Services 46
5.2.4.2 Roaming Requirements for IMS-Based Services 47
5.2.5 NR and 5GC Requirements 47
5.2.5.1 General Requirements 47
5.2.5.2 NR SNPN REQUIREMENTS 47
5.2.5.3 NR PNI-NPN REQUIREMENTS 48
5.2.6 Geofencing Requirements for Private CBRS / Non-Public Networks 48
5.2.6.1 Private CBRS / Non-Public Network deployment requirements 48
5.2.6.2 Geofencing server requirements 49
5.2.7 TAC collision avoidance Private CBRS / Non-Public deployment requirements 49
APPENDICES (Informative) 50
Appendix A: CBRS-Profile V and CBRS-Profile XV Based UE Behavior 50
A.1 CBRS-Profile V Description 50
A.2 CBRS-Profile XV Description 52
Appendix B: SHNI and IMSI Block 56
Appendix C: REQUIREMENTS MAPPING - OLD vs NEW 58
C.1 Requirement Numbering Format 58
C.2 Requirement Mapping 58
Appendix D: UE Dual SIM configurations 61
Appendix E: CHANGE HISTORY 63

LIST OF FIGURES

Figure 4.1-1: Relationship among Roles 15
Figure 4.2.1-1: SP Use Case Example 17
Figure 4.2.2-1: NHN Use Case Example 18
Figure 4.2.3.1-1: Single Subscription UE Use Case Example 19
Figure 4.2.3.2-1: Multi-subscription UE Use Case Example 20
Figure 4.2.3.4.1-1: Stand-alone Architecture 22
Figure 4.2.4-1: Hybrid Network Use Case Example 23
Figure 4.2.5-1: Fixed Wireless Network deployed by SP use case 24
Figure 4.2.5-2: Private CBRS Network providing Fixed Wireless and mobile services. Enterprise UE with MNO subscription serviced through untrusted interface 25
Figure 4.2.6-1: 5G NR NSA Network Architecture 26
Figure 4.2.6-2: 5G NR NSA EN-DC Network Architecture with U-Plane connection from EPC to eNB and gNB 27
Figure A.1-1: Multi-subscription CBRS-Profile V Based UE example (Dual USIM Case) 50
Figure A.1-2: Multi-subscription CBRS-Profile V based UE example (USIM and non-USIM Subscription Case) 51
Figure A.2-1: Multi-subscription CBRS-Profile XV Based UE example (NR CBRS and LTE non-CBRS) 53
Figure A.2-2: Multi-subscription CBRS-Profile XV Based UE example (NR CBRS and NR non-CBRS) 53
Figure A.2-3: Multi-subscription CBRS-Profile XV Based UE example (LTE CBRS and NR non-CBRS) 54
Figure B-1: The SHNI used in CBRS creates a need to route IMSIs to networks; 56
Figure B-2: A flow diagram detailing the IMSI Administrator's role in assigning IBNs for use by CBRS operators who do not possess their own HNI 57

LIST OF TABLES

Table 4.3.1.1-1: CBRS LTE UE Profile Relationship 29
Table 4.3.1.2-1: CBRS NR UE Profile Relationship 32
Table C.2-1: Requirement Mapping 58
Table D-1: CBRS UE Profiles Implemented on Specific GSMA Dual SIM Operational Mode. 61
Table E-1: Change History 63

1. INTRODUCTION AND SCOPE

This document is a Technical Specification that provides requirements for the operation of LTE radio and NR networks in the CBRS band. The requirements shall be the input for the Stage 2 and 3 specification work. Different use cases for providing network services in the CBRS band are also described.

1.1 KEY WORDS

The key words "required", "shall", "shall not", "should", "should not", "recommended", "may", and "optional" in this document are to be interpreted as described in RFC-2119 [8]. In addition, the key word "conditional" shall be interpreted to mean that the definition is an absolute requirement of this specification only if the stated condition is met.

The terminology "it shall be possible" means that the applicable feature or function shall be supported in the stage 2 and stage 3 specifications, but implementation is not mandatory by a vendor.

2. REFERENCES

Note : By default, all references to 3GPP specifications in this section points to latest 3GPP Release unless the release is explicitly mentioned.

[1] Report and Order and Second Further Notice of Proposed Rulemaking, Amendment of the Commission's Rules with Regard to Commercial Operations in the 3550-3650 MHz Band, GN Docket No. 12-354, Federal Communications Commission, 21 April 2015.

[2] Order on Reconsideration and Second Report and Order, Amendment of the Commission's Rules with Regard to Commercial Operations in the 3550-3650 MHz Band, GN Docket No. 12-354, Federal Communications Commission, 2 May 2016.

[3] WINN Forum, WINNF-TS-0016 v1.2.1, "SAS to CBSD Specification", Jan 2018, https://workspace.winnforum.org/higherlogic/ws/public/document?document_id=4441

[4] 3GPP TS 32.450: Key Performance Indicators (KPI) for Evolved Universal Terrestrial Radio Access Network (E-UTRAN): Definitions.

[5] 3GPP TS 32.425: Performance Management (PM); Performance measurements - Evolved Universal Terrestrial Radio Access Network (E-UTRAN).

[6] 3GPP TS 32.455: Key Performance Indicators (KPI) for the Evolved Packet Core (EPC); Definitions.

[7] 3GPP TS 32.426: Performance Management (PM); Performance measurements - Evolved Packet Core (EPC) network.

[8] RFC-2119, "Key words for use in RFCs to Indicate Requirement Levels", March 1997.

[9] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[10] CBRSA-TS-1002-V4.1.0, "CBRS Network Service Stage 2 and 3 Specifications", Note: Document not yet published, but should be published shortly and should be at the following link.

[11] 3GPP TS 33.401: "3GPP System Architecture Evolution (SAE); Security Architecture".

[12] CBRSA-TS-1003-V4.0.0, "CBRSA – Extended Subscriber Authentication Technical Specifications".

[13] 3GPP TS 23.402: "Architecture enhancements for non-3GPP accesses"

[14] 3GPP TS 31.102: "Characteristics of the Universal Subscriber Identity Module (USIM) application"

[15] International Mobile Subscriber Identity (IMSI) Assignment and Management Guidelines for Shared HNI for CBRS Range Version 1.0 May 2018. Document can be found at the following link.

[16] CBRSA-TR-0100-V1.0.0, "CBRS Alliance Identifier Guidelines for Shared HNI", Document can be found at the following link.

[17] GSMA IR.88 V16.0, 05 July 2017, LTE and EPC Roaming Guidelines.

[18] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[19] 3GPP TS 37.340: "3rd Generation Partnership Project, Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA) and NR; Multi-connectivity; Stage 2".

[20] 3GPP TS 23.501: "3rd Generation Partnership Project, Technical Specification Group Services and Systems Aspects; System architecture for the 5G Systems (5GS)"

[21] 3GPP TS 23.502: "3rd Generation Partnership Project, Technical Specification Group Services and System Aspects; Procedures for the 5G Systems (5GS)".

[22] International Telecommunication Union (ITU), Standardization Bureau (TSB): "Operational Bulletin No. 1156"; http://handle.itu.int/11.1002/pub/810cad63-en (retrieved October 5, 2018).

[23] 3GPP TS 22.261: "3rd Generation Partnership Project, Technical Specification Group Services and Systems Aspects; Service requirements for the 5G system; Stage 1

[24] CBRSA-TR-0101-V1.0.2, CBRS Alliance Administration Guidelines for Shared HNI.

[25] 3GPP TR 21.915: "3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects; Release 15 Description; Summary of Rel-15 Work Items.

[26] 3GPP TS 33.501:" Security architecture and procedures for 5G System"; Release 16.

[27] 3GPP TS 24.502: "Access to the 3GPP 5G Core Network (5GCN) via non-3GPP access networks"; Release 16.

3. ABBREVIATIONS AND DEFINITIONS

3.1 ABBREVIATIONS

- *3GPP* : Third Generation Partnership Project
- *5GC* : 5G Core
- *5GS* : 5G System
- *AAA* : Authentication, Authorization and Accounting

- *AKA* : Authentication and Key Agreement
- *AM* : Assignment Mode
- *AN* : Access Network
- *APN* : Access Point Name
- *APN-NI* : Access Point Name-Network IDentifier
- *CAG* : Closed Access Group
- *CID* : Cell IDentifier
- *CK* : Confidentiality Key
- *CPE* : Customer Premise Equipment
- *CBRS* : Citizens Broadband Radio Service
- *CBRSA* : CBRS Alliance
- DC : Dual Connectivity
- *DNS* : Domain Name Server
- *DSC* : DIAMETER Signalling Controller
- *DHCP* : Dynamic Host Configuration Protocol
- *DSCP* : Differentiated Services Code Point
- *EAP-TLS* : Extensible Authentication Protocol-Transport Layer Security
- *EAP-TTLS* : Extensible Authentication Protocol-Tunneled Transport Layer Security
- *ECGI* : E-UTRAN Cell Global Identifier
- *EMM* : EPS Mobility Management
- *EN-DC* : EUTRAN NR Dual Connectivity
- *EPC* : Evolved Packet Core
- *EPS* : Evolved Packet System
- *EUI* : Extended Unique Identifier
- *ePDG* : Evolved Packet Data Gateway
- *ESM* : EPS Session Management
- *FCC* : Federal Communications Commission
- *GAA* : General Authorized Access
- *GUMMEI* : Global Unique MME Identifier
- *GUTI* : Globally Unique Temporary Identifier
- *HNI* : Home Network Identity
- *hPCRF* : home PCRF
- *HPLMN* : Home PLMN
- *IBN* : IMSI Block Number
- *IK* : Integrity Key
- *IOC* : IMSI Oversight Council
- *IoT* : Internet of Things
- *IIoT* : Industrial Internet of Things
- *IMS* : IP Multimedia Subsystem
- *IMSI* : International Mobile Subscriber Identity

- *IPx* : Internet Packet Exchange
- *ISP* : Internet Service Provider
- *KPI* : Key Performance Indicator
- K_{ASME} : Key Access Security Management Entries
- *LBO* : Local Break Out
- *LTE* : Long-Term Evolution
- *MCC* : Mobile Country Code
- *MCG* : Master Cell Group
- *MDT* : Minimization of Drive Test
- *MMEGI* : MME Group Identifier
- *MMEI* : MME Identifier
- *MNC* : Mobile Network Code
- *MNO* : Mobile Network Operator
- *MS* : Mobile Station
- *MSO* : Multiple-System Operator
- *MVNO* : Mobile Virtual Network Operator
- *N3IWF* : Non-3GPP Inter Working Function
- *NG RAN* : Next Generation Radio Access Network
- *NH* : Neutral Host
- *NHN* : Neutral Host Network
- *NID* : Network Identifier
- *NPN* : Non Public Network
- *NR* : New Radio
- *NR SA* : New Radio Stand-alone
- *OUI* : Organizationally Unique Identifier
- *NW* : Network
- *OTA* : Over The Air
- *OTT* : Over The Top
- *PCC* : Policy and Charging Control
- *PDN* : Packet Data Network
- *PLMN* : Public Land Mobile Network
- *PNI-NPN* : Public Network Integrated Non-Public Network
- PSP : Participating Service Provider
- *QOS* : Quality Of Service
- *R&O* : Rule and Order
- *RRC* : Radio Resource Control
- *SA* : Stand Alone
- *SAE* : System Architecture Evolution
- *SCG* : Secondary Cell Group
- *SHNI* : Shared HNI (Home Network Identifier)

- *SIB* : System Information Block
- *SLA* : Service Level Agreement
- *SP* : Service Provider
- *SNPN* : Stand-alone Non-Public Network
- *TAC* : Tracking Area Code
- *TAU* : Tracking Area Update
- *UE* : User Equipment
- *UICC* : Universal Integrated Circuit Card
- *UIN* : User Identity Number
- *UPF* : User Plane Function
- *USIM* : Universal Subscriber Identity Module
- *VLAN* : Virtual Local Area Network
- *VoLTE* : Voice over LTE
- *vPCRF* : visited PCRF
- *VPLMN* : Visited PLMN

3.2 DEFINITIONS

3GPP Access Mode	:	Operational mode between the UE and the network whereby communication is based on the 3GPP EPS architecture, functions and procedures as described in section 5.5.3 of CBRSA-TS-1002 [10] and for 5GS, functions and procedures are defined in 3GPP TS 23.501 [20].
3GPP Access Mode (EPS-AKA)	:	An operational mode supported by a UE supporting the functions and procedures specified by 3GPP using E-UTRAN EPS-AKA authentication as defined in 3GPP TS 33.401 [11]. That is, 3GPP Access Mode (EPS-AKA) is the normal UE operation per 3GPP E-UTRAN specifications, including the use of EPS-AKA for authentication.
3GPP-based Access Mode (non-EPS-AKA)	:	An operational mode supported by a UE that performs authentication without the use of EPS-AKA, and that in all other aspects supports the functions and procedures specified by 3GPP. That is, 3GPP-based Access Mode (non-EPS-AKA) is the UE operation per 3GPP E-UTRAN specifications, except that a non-EPS-AKA method is used for authentication which includes EAP-TLS, EAP-TTLS. This allows the authentication of the UE without a USIM.
5G-non-SIM-Credential	:	5G-non-SIM-Credential refers to the 5G authentication methodology which is neither 5G-AKA nor EAP-AKA'.
CBRS Network	:	One or more CBSDs, along with their related network elements, operated in compliance with 47 CFR Part 96, all other relevant FCC regulations, and all relevant technical and operational recommendations of the CBRS Alliance.

CBRSA NHN	:	NHN adapted from the MulteFire Alliance (MFA) Release 1.0 specifications for neutral host deployment as described in section 5.5.2 of CBRSA-TS-1002 [10].
EPS-AKA	:	3GPP LTE Authentication and Key Agreement (AKA) defined in 3GPP TS 33.401 [11]. In this method, mutual authentication is achieved between a user and a network by a challenge and response protocol based on a shared cryptographic key K, which is only available to USIM an user's home EPC network. In addition to authentication, it also defines a process of establishing encryption and integrity keying materials to be used by the user equipment (UE) and the network to protect subsequent communication.
ISP (Internet Service Provider)	:	An entity which offers Internet Access and (possibly) other related services.
Mobility Management Entity' (MME')	:	The MME' is a 3GPP LTE MME that is extended to support an interface to a AAA for EAP authentication methods.
Mobile Network Operator (MNO)	:	A Mobile Network Operator, also known as a wireless service provider, wireless carrier, cellular company, or mobile network carrier, is a provider of wireless communications services that owns or controls all the elements necessary to sell and deliver services to an end user including radio spectrum allocation, wireless network infrastructure, backhaul infrastructure, billing, customer care, provisioning computer systems and marketing and repair organizations.
MSO (Multiple System Operator)	:	A company which owns multiple fixed access systems and offer services such as (but not limited to) Internet Access, Video, Voice, etc. to residences and enterprises. A MSO may also own or control the elements necessary to deliver wireless services, in which case it would also be considered a MNO.
NG-RAN	:	A radio access network that supports one or more of the following options with the common characteristics that it connects to 5GC as defined in 3GPP TS 23.501 [20]. 1. Standalone New Radio. 2. New Radio is the anchor with E-UTRA extensions. 3. Standalone E-UTRA. 4. E-UTRA is the anchor with New Radio extensions. Note: E-UTRA extension refers to EN-DC, and New Radio extension refers to NE-DC.
NHN (Neutral Host Network)	:	A Neutral Host Network is a network deployed and operated by an NHN operator, who may also be an independent entity, a MNO, or MSO, where the network resources are being shared by multiple services providers.

NHN Access Mode	:	Operational mode between the UE and the network whereby communication is based on the NHN functions and procedures adapted from the MulteFire Alliance (MFA) Release 1.0 specifications for neutral host deployment as described in section 5.5.2 of CBRSA-TS-1002 [10]. NHN referred in this definition is CBRSA NHN.
NHN Core Network	:	The Core Network part of a NHN.
NHN RAN	:	The RAN part of a NHN deployed in the CBRS band.
Non-EPS-AKA	:	Non-EPS-AKA refers to extended authentication methods as defined in TS-1003. Further, Non-EPS-AKA also refers to an authentication method that does not mandate the use of USIM for protecting authentication credentials.
Non-Public Network	:	A network that is intended for non-public use (Refer 3GPP TS 22.261 [23]).
NR	:	New Radio Access Technology meant for 5G Cellular Networks (Refer 3GPP TS 22.261 [23]).
Non-USIM Authentication	:	Non-USIM Authentication refers to any authentication method that does not mandate the use of USIM for protecting authentication credentials. Extended authentication methods defined in CBRSA TS-1003 do not mandate the use of USIM. Thus, Non-USIM is often used to refer to CBRSA authentication methods, and it is also used interchangeably with Non-EPS-AKA. Depending on the context, the terminology of Non-SIM, non-USIM, Non-USIM authentication, Non-EPS-AKA authentication, Non-USIM credentials, or Non-USIM subscription may also be used. Note that CBRSA does not mandate the use of USIM or prevent USIM from being used for credential storage.
OTA	:	Over The Air is a mechanism to communicate with wireless device to provision, update and manage.
OTT Video	:	Streaming video distribution to consumers over the internet.
Participating Service Provider (PSP)	:	A PSP is a Service Provider (SP) offering services to its subscribers via a CBRSA NHN.
Private CBRS Network	:	A Private CBRS Network provides services to subscribers or connected devices authorized by the provider of the network. Services could be provided exclusively to the network's own subscribers, and the network may be isolated from other networks.
PSP Core Network (PSP CN)	:	A core network operated by a PSP.

PSP RAN	:	A 3GPP RAN network operated by a PSP. Only a PSP which is an MNO is expected to have a RAN.
Public Network Integrated Non-Public Network (PNI NPN)	:	A non-public network deployed with the support of a PLMN. Refer 3GPP TS 23.501 [20].
Radio Footprint	:	Radio signal characteristics of one or more Cell-IDs from the MNO, MSO, or MVNO networks that may also be associated with the signal strength ranges (e.g. using RSRP), which when detected by the UE is used to search for specific Private CBRS / Non-Public Network.
Service Provider (SP)	:	An entity such as an MNO, MVNO, MSO, or ISP that provides services to its Subscribers and can authenticate and authorize its Subscribers. Any entity that has a service agreement with Subscribers can act as a SP.
Stand-alone Non-public Network (SA-NPN)	:	A non-public network not relying on network functions provided by PLMN. Refer 3GPP TS 23.501[20].
SWu	:	The interface from a UE through an untrusted IP access to an operators ePDG (Evolved Packed Data Gateway). The SWu interface allows for establishing or disconnecting a tunnel between the UE and ePDG.
USIM	:	Universal SIM is defined in 3GPP TS 31.102 [14] as a software application resided in UICC that can store sensitive data including, but not limited to, shared secrets, IMSI, and keying materials used by 3GPP authentication and key agreement.
USIM Authentication	:	USIM Authentication refers to any authentication method that mandates the use of USIM for protecting authentication credentials. Since EPS-AKA is the only authentication method in 3GPP LTE which also mandates the use of USIM, USIM authentication is often used interchangeably with EPS-AKA in CBRSA specifications.

4. CBRS NETWORK SERVICES USE CASES, FEATURE AND FUNCTIONALITY DESCRIPTION

4.1 INTRODUCTION

This section describes the different use cases that can be enabled via the CBRS band and features/functionalities that can be supported across multiple use cases. The use cases define the roles involved in providing service and describe how specific entities fulfill the roles in each use case. It is important to recognize the difference between role and entity, and to recognize that a single entity may fulfill more than one role in a given use case.

The following text from the FCC Report & Order [1] [ref. 1, Pg. 107, Para. 8] outlines some use cases anticipated for the CBRS band.

> *As a result of the Commission's actions in the R&O and Second Order and Order on Reconsideration, small business will have access to spectrum that is currently unavailable to them. The potential uses for this spectrum are vast. For example, wireless carriers can deploy small cells on a GAA basis where they need additional capacity. Real estate owners can deploy neutral host systems in high-traffic venues, allowing for cost-effective network sharing among multiple wireless providers and their customers. Manufacturers, utilities, and other large economic sectors can construct private wireless broadband networks to automate industrial processes that require some measure of interference protection and yet are not appropriately outsourced to a commercial cellular network. All of these applications can potentially share common wireless technologies, providing economies of scale and facilitating intensive use of the spectrum.*

There are three roles involved in CBRS service use cases; Service Provider, CBRS Network Operator, and Subscriber.

A Service Provider (SP) authenticates and authorizes its subscribers and provides services to them. Any entity that has a service agreement with Subscribers can act as an SP. For example, entities like traditional communications providers including MNOs, MSOs, MVNOs and ISPs are SPs that provide services to their customers. An entity like an enterprise plays a SP role in providing services to its employees, customers, or other related parties. A Service Provider must have the technical ability to provide suitable Authentication and Authorization of its Subscribers; it may or may not have other components of a traditional EPC. Services offered by SPs include, e.g., VoLTE, Internet access, IoT, etc. A Participating Service Provider (PSP) is an SP having a business agreement with NHN Operator to offer services via the specific Neutral Host.

A CBRS Network Operator deploys a CBRS network with an intention to provide connectivity and/or enable services to Subscribers of Participating Service Provider(s). A CBRS network may be deployed in a variety of locations, including public venues (malls, airports, city squares) and enterprises (offices, hotels, etc.). Any entity that deploys a CBRS Network plays a role of a CBRS Network Operator. For example, when an SP deploys its own CBRS network, the SP also plays a role of CBRS Network Operator.

A Subscriber is authenticated and authorized by one or more Service Providers it has service agreement with, and upon successful authentication and authorization, is provided with services from SPs. For clarity, the term "Subscriber" may refer to a person or a device; it is the device that is subject to authentication and authorization.

Figure 4.1-1 describes the relationships among three different roles.

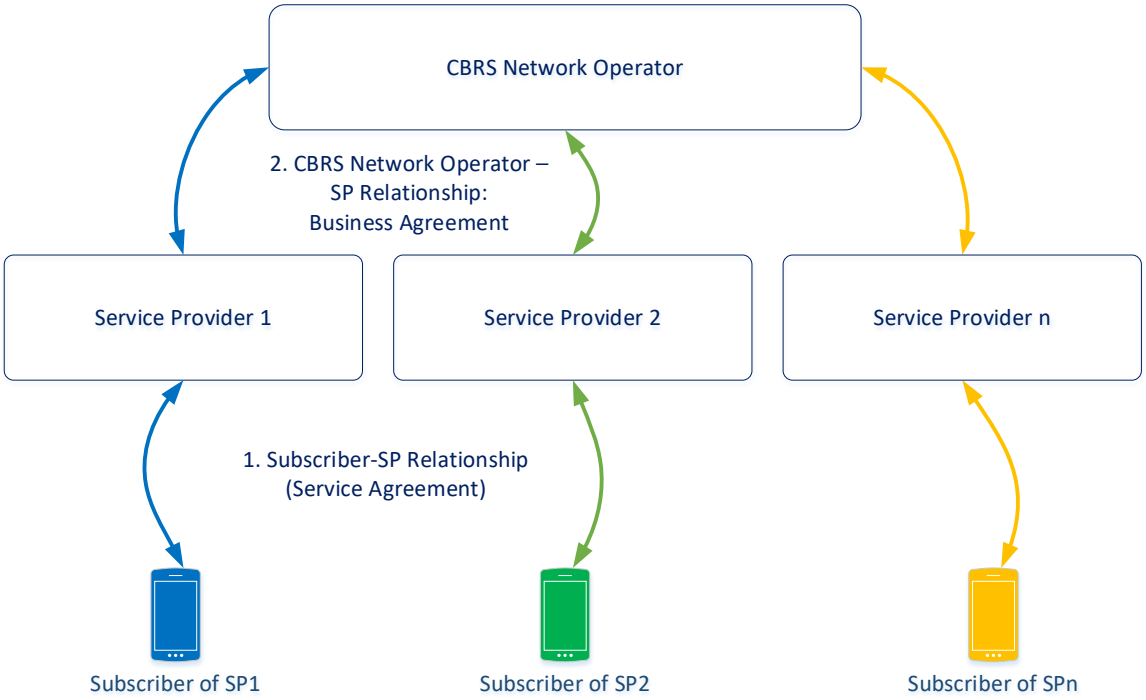

Figure 4.1-1: Relationship among Roles

1. Subscriber – Service provider relationship: A Subscriber has a service agreement with a Service Provider for the services offered by that Service Provider. The Service Provider has all the information about the Subscriber enabling it to provide authentication of the Subscriber, authorization of the services for the Subscriber, and Subscriber management. The service agreement could be, for example, a traditional monthly-billing arrangement, or may take other forms such as on-line sign-up, pre-installed certificates, or vending-machine SIMs. A subscriber may have a service agreement with more than one Service Provider.

2. Service Provider – CBRS Network Operator relationship: a CBRS Network Operator has a business agreement with one or more Service Providers to provide connectivity and/or enable services on one or more of its CBRS Networks to the Service Providers' Subscribers. The business agreement includes all the aspects for SPs to be able to provide services to their Subscribers on CBRS networks. This business agreement can include, for example, technical arrangements enabling the Service Provider to provide at least authentication and authorization of its Subscribers when they use the CBRS Network.

Note : This relationship diagram only covers the relationship between CBRS roles. The existing business relationship among Service Providers, including traditional roaming agreement, continues to be in place independent of the relationship among CBRS roles. For example, Subscribers of SPs may be able to roam onto the CBRS Network deployed by

other SPs using conventional 3GPP roaming procedures if there is a roaming agreement between those SPs.

Depending on the roles the entities play, different use cases arise. Each use case is described in more detail in subsequent sections.

4.2 USE CASES

4.2.1 SERVICE PROVIDER USE CASE

For the SP use case, an SP deploys the CBRS network itself and, hence, plays the role of a CBRS Network Operator as well as a SP. Subscribers of the SP benefit from improved user experience and/or an extended coverage through CBRS network.

Figure 4.2.1-1 shows an example of SP use case. In this example, SPs could represent traditional MNOs and MSOs, and other traditional types of SPs. MNO1 deploys a CBRS Network itself; hence plays the role of both SP and CBRS Network Operator. Subscribers of MNO1 have access to the CBRS Network deployed by MNO1. Other SPs (MSO1 and MNO2 in this example) have no relationship with the CBRS Network deployed by MNO1; hence the Subscribers of MSO1 or MNO2 do not have access to this CBRS Network.

For the SP use-case when the SP is a MNO, the CBRS Network may use LTE or NR NSA with LTE as an anchor or NR SA. For CBRS LTE and NR NSA network with LTE as an anchor, the 3GPP defined architectures in 3GPP TS 23.401 [9] using S1 can be used. For CBRS NR SA networks, the 3GPP defined architectures in 3GPP TS 23.501 [20] can be used. In this case, if other SPs have traditional roaming agreements with MNO1, then Subscribers of those SPs may be able to roam onto the CBRS Network deployed by MNO1 using conventional 3GPP roaming procedures.

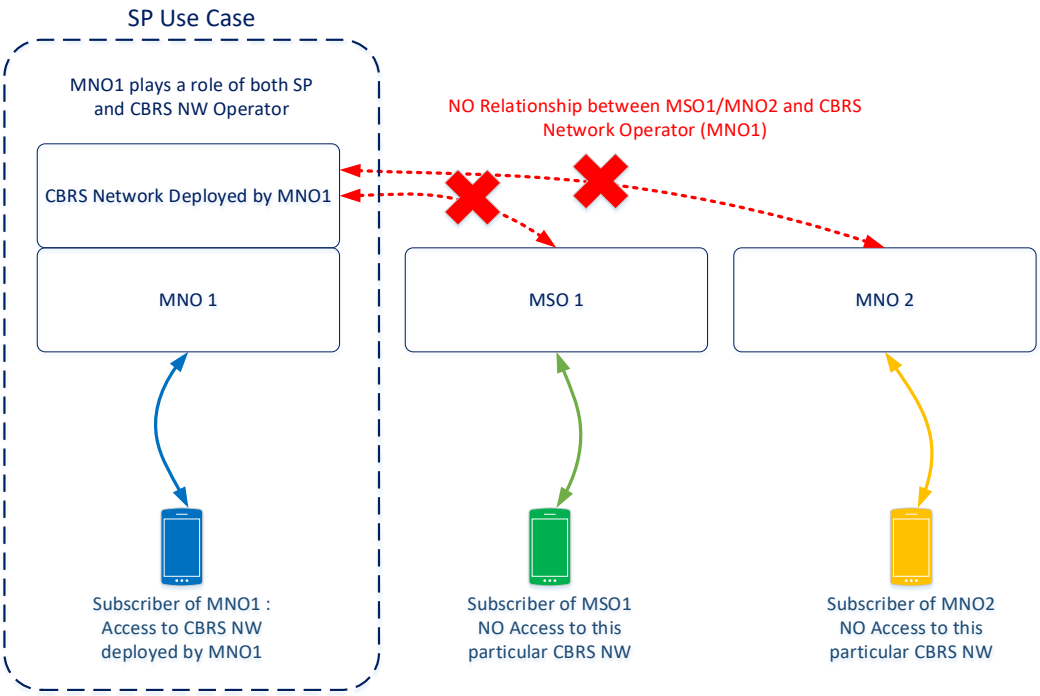

Figure 4.2.1-1: SP Use Case Example

4.2.2 CBRSA NHN USE CASE

The NHN (Neutral Host Network) use case involves the deployment of a CBRS network by a NHN Operator with the intention of providing service to the Subscribers of one or more participating Service Providers through the CBRS Network while the Subscribers are on the CBRS Network. Subscribers have no direct association with the NHN Operator. All subscriber management functions (e.g., billing and payment, customer care, provision of SIMs or certificates) are performed by the SP. The NHN Operator has a business agreement with a SP to provide service to participating SP's subscribers while they are on the CBRS Network. Note that there is no direct service or business relationship between Subscriber and CBRS Network Operator. A CBRS Network Operator simply provides connectivity and/or enables services to the Subscribers of participating SPs.

Figure 4.2.2-1 shows an example of NHN use case. In this example, SP entities MNO1 and MSO1 have business agreements with a NHN Operator which is a CBRS Network Operator. Through these business agreements, MNO1 and MSO1 become Participating Service Providers (PSPs) for this CBRS Network and the Subscribers of MNO1 and MSO1 have access to the CBRS Network deployed by the NHN Operator. MNO2 does not have a relationship with this NHN Operator; hence Subscribers of MNO2 do not have access to this CBRS Network deployed by the NHN Operator.

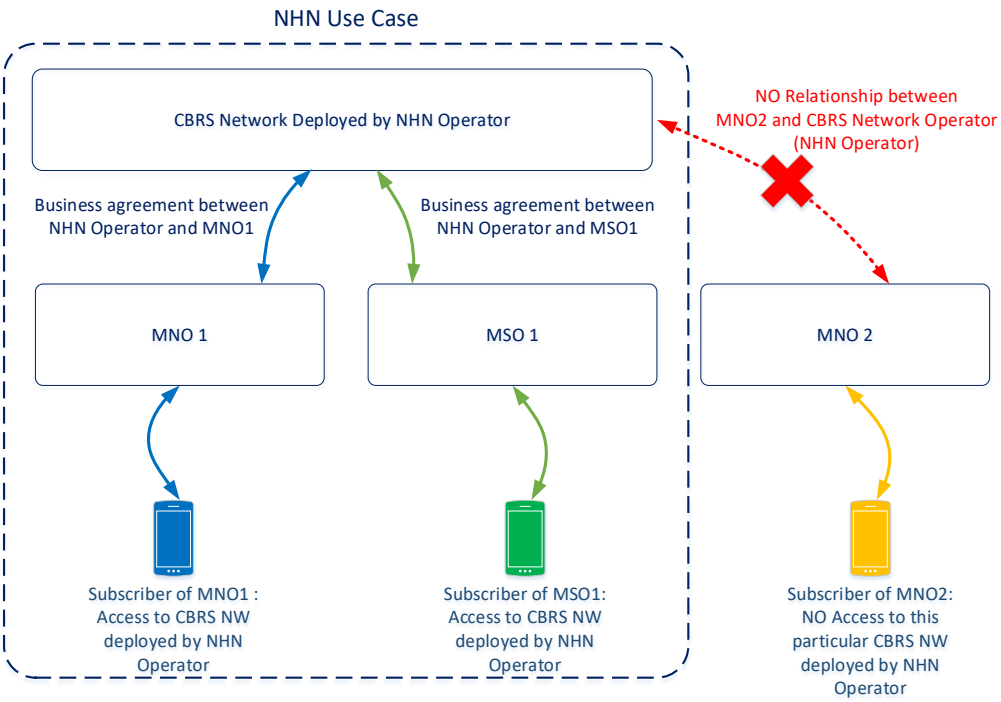

Figure 4.2.2-1: NHN Use Case Example

In the above example, the business relationship between the NHN Operator and SP entities (MSO1 and MNO1) can also be based on 3GPP specification defined roaming relationship wherein the NHN becomes the Visited Network for subscribers belonging to SP entities (MNO1 and MSO1). CBRS Alliance does not exclude any such 3GPP based NHN architecture.

Any impacts to 3GPP defined architecture as a result of IMSI blocks allocated within the PLMN ID allocated for CBRS (CBRS SHNI defined in IMSI Guideline [15]) shall be studied as part of Stage 2 work.

The extension or update of CBRSA NHN to 5G NR is not addressed in this release.

4.2.3 PRIVATE NETWORK (LTE & NR) AND NR NON-PUBLIC NETWORK

A private network is a system that provide services, specifically for a group, or an enterprise(s), e.g., a mall or a school campus. Private networks are typically not accessed by the general public. The terminology private network and non-public networks are referenced in this document, and are used interchangeably in the context of NR.

Note : NR Private Network refers to 3GPP Release 15 and NR Non-Public Network refers to 3GPP Release 16 onwards.

4.2.3.1 SINGLE SUBSCRIPTION UE USE CASE

Private CBRS network is deployed to provide service to employees, machines and other devices as authorized by the Private Network provider. For the LTE Private and NR Non-Public Networks, the network operator plays the roles of both SP (providing services to the authorized users/devices) and CBRS Network Operator (deploying the CBRS network). An LTE private network operator is one that deploys and manages an LTE Core network and an LTE RAN operating in the CBRS band and provides services exclusively for its own Subscribers. The end user devices in a private network shall have a business relationship with the private network operator. NR Private Network a.k.a NR Non-Public Networks can be deployed as Standalone Non-Public Networks or PNI-NPN.

Figure 4.2.3.1-1 shows an example of private network use case. In this example, Enterprise 1 deploys a CBRS Network; hence playing the role of both SP and CBRS Network Operator. Employees or customers of Enterprise 1 are granted a subscription to access the CBRS Network deployed by Enterprise 1. Enterprise 1 does not have any business relationship with MNO1 or MSO1; hence the Subscribers of MNO1 or MSO1 do not have access to the CBRS Network deployed by Enterprise 1.

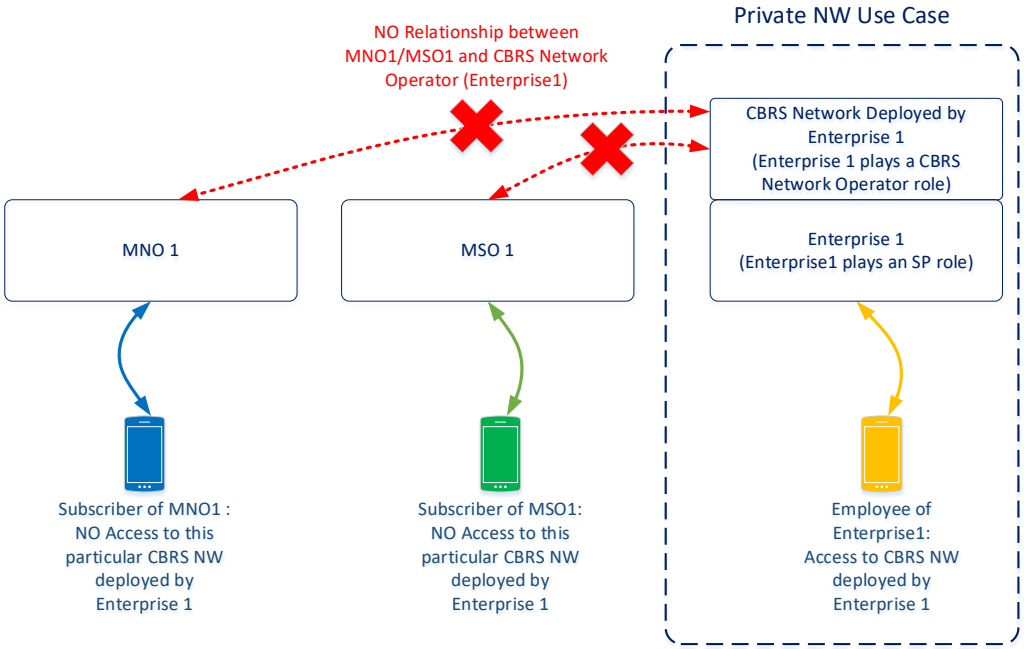

Figure 4.2.3.1-1: Single Subscription UE Use Case Example

4.2.3.2 MULTI-SUBSCRIPTION UE USE CASE

This is a variation of the Private Network use case where a UE used in a Private Network has, in addition to a subscription with the Private Network, a subscription with another SP. The SP subscription can be used to access the SP's network when the Private Network coverage is unsatisfactory or when a Subscriber wants to access SP services. The device uses separate credentials for access to the Private Network and to the SP's network. A Subscriber may use an SP subscription to access SP services using a Private Network as an

untrusted network. In this case, the subscriber can use untrusted non-3GPP access procedures to access SP services. The tunnel is setup using IP connectivity provided by a Private Network after gaining the connectivity by authenticating with the Private Network using Private Network credentials. The Private Network in this use case can be LTE Private Network or NR Non-Public Network (i.e., SNPN or PNI-NPN).

Figure 4.2.3.2-1 shows an example of a Private Network use case with dual subscription. In this example, Enterprise 1 deploys a CBRS Network and provides private services to the authorized users. Enterprise 1 does not have any business relationship with MNO1. An employee of Enterprise 1 also has a subscription to MNO1 with a separate MNO1 credential. This employee can access the private network services through the CBRS network deployed by Enterprise 1. The employee can also access the MNO services with the CBRS network acting as an untrusted non-3GPP access (e.g., the UE can connect to the MNO's ePDG to access MNO's LTE network/services. The UE can connect to the MNO's N3IWF to access MNO's NR network/services.

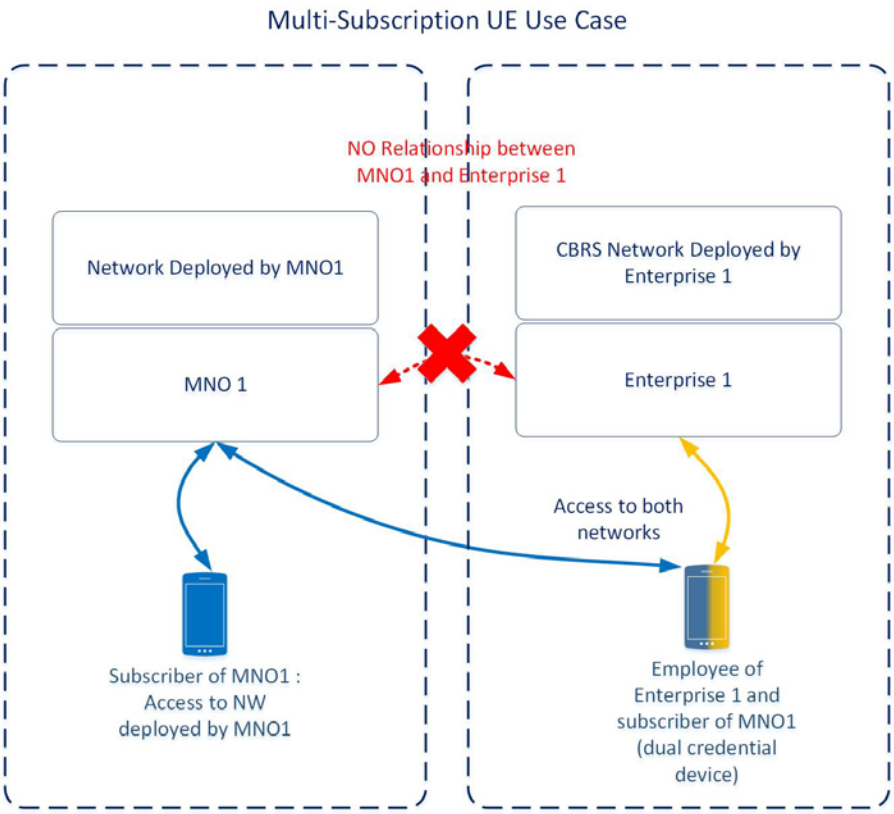

Figure 4.2.3.2-1: Multi-subscription UE Use Case Example

4.2.3.3 LTE PRIVATE NETWORK

A private network operator is one that deploys and manages an LTE Core network and an LTE RAN operating in the CBRS band and provides services exclusively for its own Subscribers. The LTE private network may include the support for NR NSA following the EN-DC architecture as per section 4.2.6.

4.2.3.4 NR PRIVATE NETWORK

NR Private Network is a use case for 3GPP Release 15 based SA mode of operation and deployed by an operator using SHNI to provide services exclusively for its own subscribers. The relevant network identifiers for NR Private Networks may be allocated by OnGo Alliance and can be found in CBRSA-TR-0100 [16].

Note : As of this version of the specification, roaming functionality for NR Private Networks is not supported.

4.2.3.5 NR NON-PUBLIC NETWORK

For 5G NR, 3GPP defines two Non-Public Networks: SNPN and PNI-NPN.

4.2.3.5.1 STAND-ALONE NON-PUBLIC NETWORK

Standalone Non-Public Network (SNPN) is an isolated NR network providing operators the option to deploy their systems as private networks; thus, not depending on network functions provided by a PLMN. 3GPP introduced a new identifier, i.e., NID, which has two assignment modes: self-assigned and coordinated. Self assigned mode (AM=1) is not recommended for use by the CBRS System as the identifiers are not guaranteed to be globally unique. CBRS will support assignment mode 0 (AM=0) and assignment mode 2 (AM=2), both of which are globally unique.

In the SA deployment option, the 5G System (5GS) is composed of the User Equipment, the Access Network (including the "New Radio" or NR) and the Core Network (5GC) (refer 3GPP TR 21.915 [25]). The "Stand-Alone" (SA) architecture, where the NR is connected to the 5G Core is defined illustrated in the following figure:

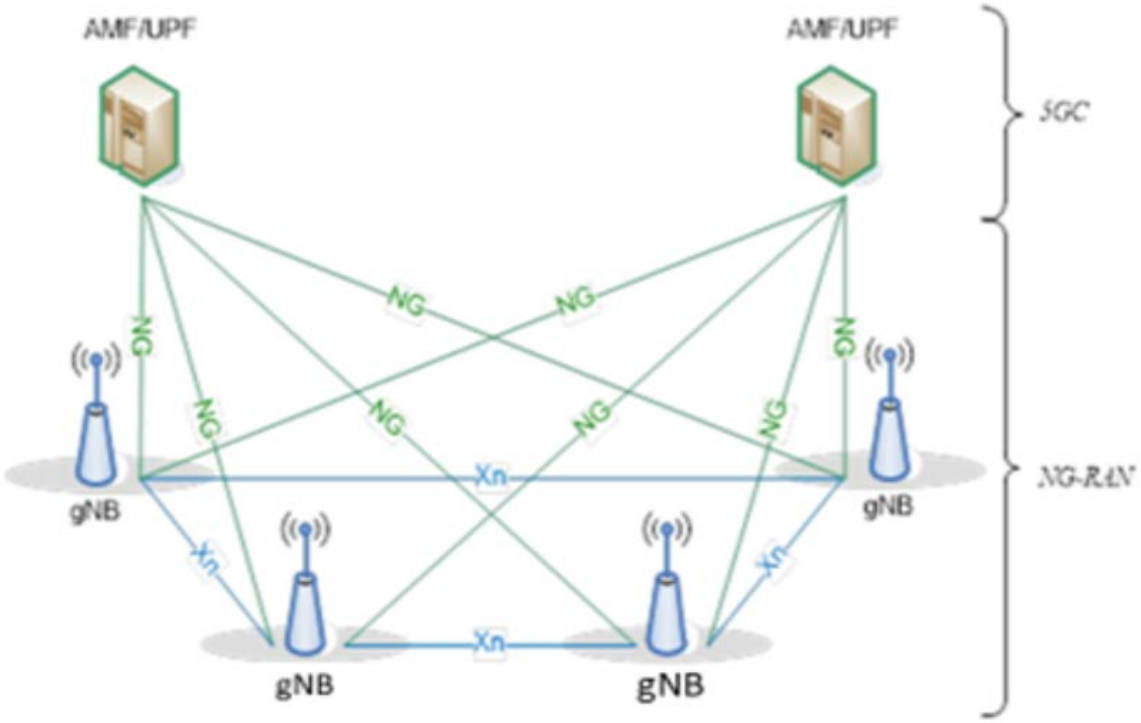

Figure 4.2.3.4.1-1: Stand-alone Architecture

4.2.3.5.2 PUBLIC NETWORK INTEGRATED NON-PUBLIC NETWORK

The support for Public Network Integrated NPN (PNI-NPN) was introduced as part of 3GPP in Release 16. PNI-NPN enables the deployment of standalone non-public networks and requires a PLMN. Within PNI-NPN, a CAG is used as an access control mechanism allowing those authorized UEs to access a system. CBRSA Release 4 does not support the use of SHNI for PNI-NPN and does not allocate CAG-ID. However PNI-NPN is supported without the use of a CBRS SHNI.

4.2.4 HYBRID NETWORK USE CASE

The hybrid use case combines more than one use case described in above sections. Specifically, the hybrid use case combines the CBRSA NHN use case with the other use cases, i.e. SP use case or Private Network use case. In hybrid use case, an SP or Private network operator provides services to its own Subscribers while

simultaneously provides access to the PSP's subscribers. Figure 4.2.4-1 shows an example of a hybrid use case.

SP1 (MNO/MSO/Enterprise) deploys the CBRS network for its own Subscribers and other PSPs' Subscribers. SP1 has a business relationship with MNO1 so that MNO1's Subscriber can access the CBRS network. The Subscriber of SP1 accesses the CBRS network deployed by SP1 to access the SP1 services. The Subscriber of MNO1 accesses the CBRS network deployed by SP1 to access the MNO1 services.

MNO2 does not have a business relationship with SP1 for CBRS access, hence, the Subscriber of MNO2 does not have the access to CBRS network deployed by SP1.

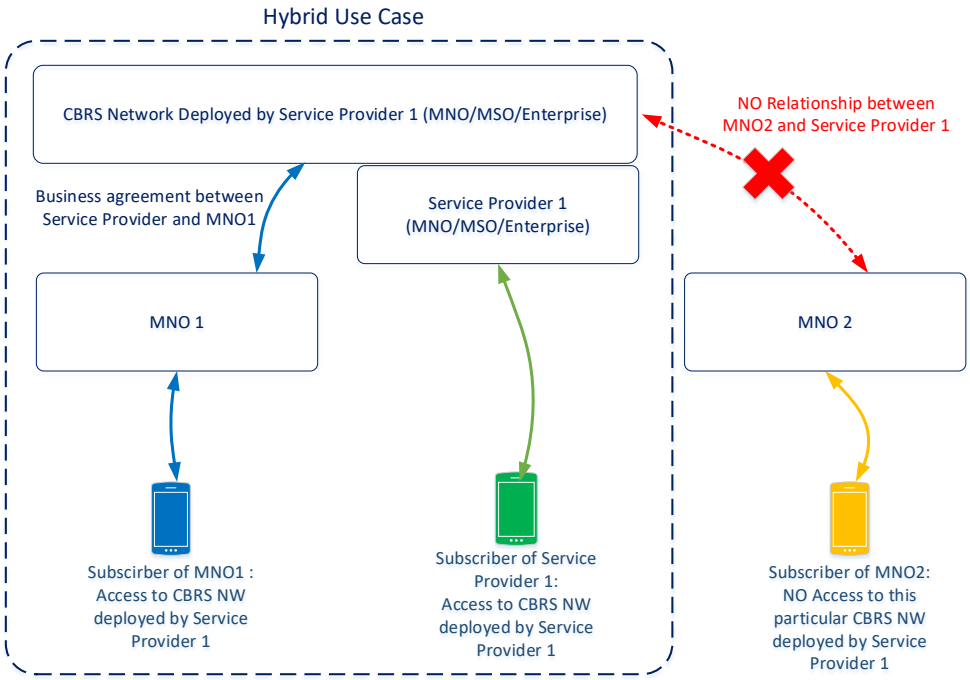

Figure 4.2.4-1: Hybrid Network Use Case Example

4.2.5 FIXED WIRELESS NETWORK USE CASE

In this use case the CBRS Network is deployed by a Fixed Wireless Service Provider to provide data communication services for residential and enterprise customers using Fixed Wireless Access equipment.

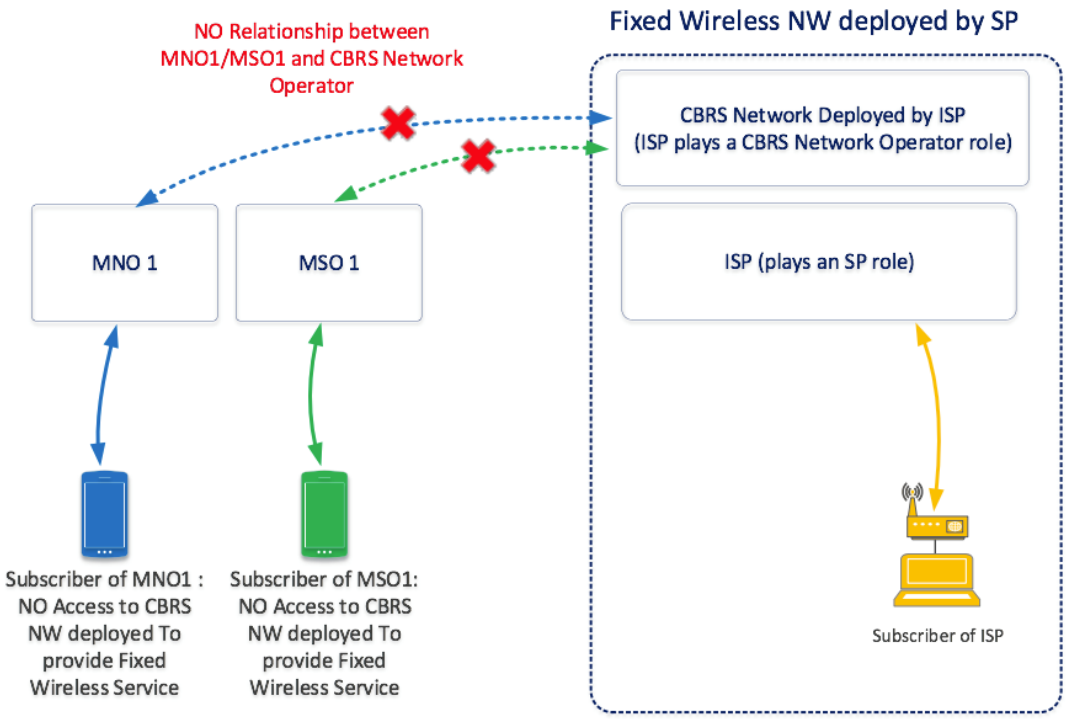

Figure 4.2.5-1: Fixed Wireless Network deployed by SP use case

Residential customers typically require Internet Access, VoIP and OTT video services.

Enterprise customers may require Internet access, corporate (private) data services, corporate VoIP and etc. private applications. Such customers may have one or more locations connected by wireless and/or wireline technologies with multiple computers in each location. In many cases, to serve corporate needs, Enterprise customers require transparent Layer 2 services between their locations from the Fixed Wireless Network Service Provider - plain Ethernet, 802.1q VLANs, etc. with corresponding QOS per service.

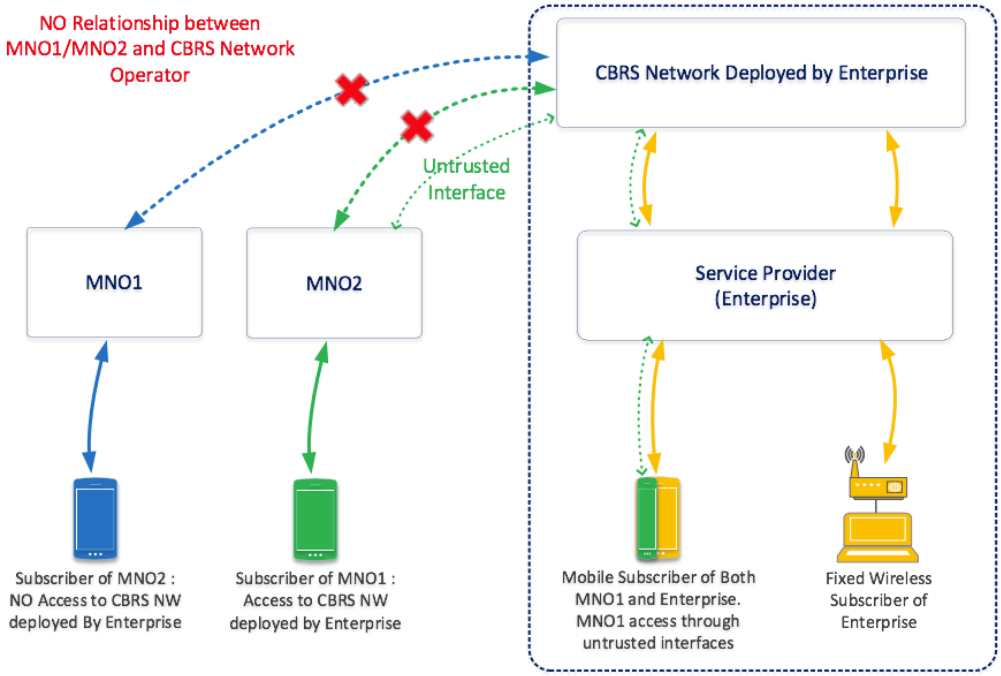

Figure 4.2.5-2: Private CBRS Network providing Fixed Wireless and mobile services. Enterprise UE with MNO subscription serviced through untrusted interface

4.2.6 5G NR EN-DC USE CASE

Figure 4.2.6-1 depicts the network architecture used for 5G NR Non-Standalone (NSA) deployments with LTE as anchor. Private Network deployment with NR Non-Standalone EN-DC can be supported with the use of SHNI. 3GPP EN-DC can be used together with other network architectures and associated Use Cases defined in this document. The EN-DC Use Case supports higher bandwidths, low latency and increased reliability.

Note :

- Currently, 3GPP specifications do not support EN-DC with MeNB broadcasting CSG-ID.
    - The concept of Closed Subscriber Group (CSG) in not supported in 3GPP specifications for NR.
- In 3GPP Release 16, Closed Access Group (CAG) is introduced for NR, which is different than Closed Subscriber Group (CSG) in LTE, as described in 3GPP TS 23.401 [9].
- As on this release, this specification does not support PNI-NPN with SHNI. CBRS Alliance is not planning to allocate and manage CAG-IDs in the current release.

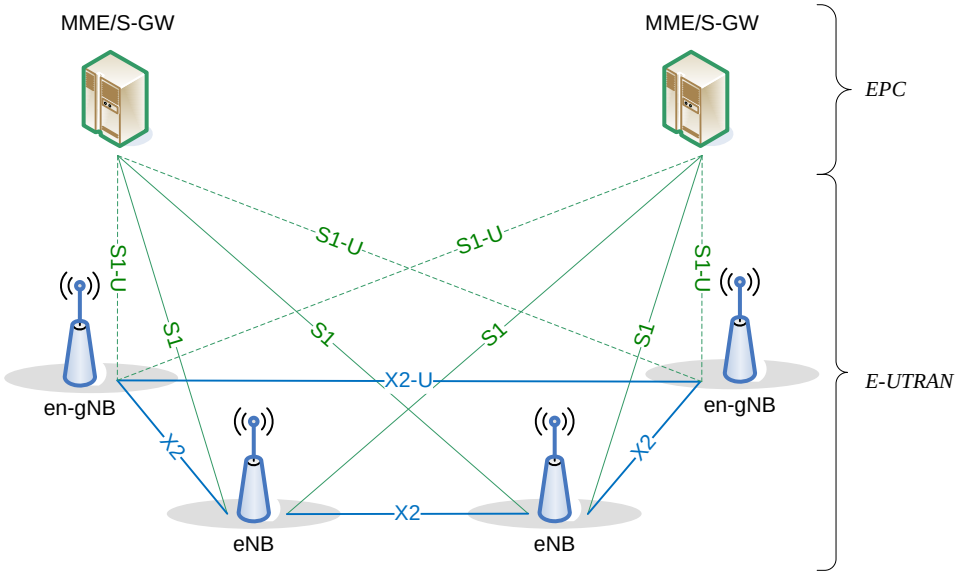

Figure 4.2.6-1: 5G NR NSA Network Architecture

The support of CBRS-A Neutral Host Networks with 5G NR SA architectures or 5G NR NSA architectures may be addressed in future CBRS Alliance releases.

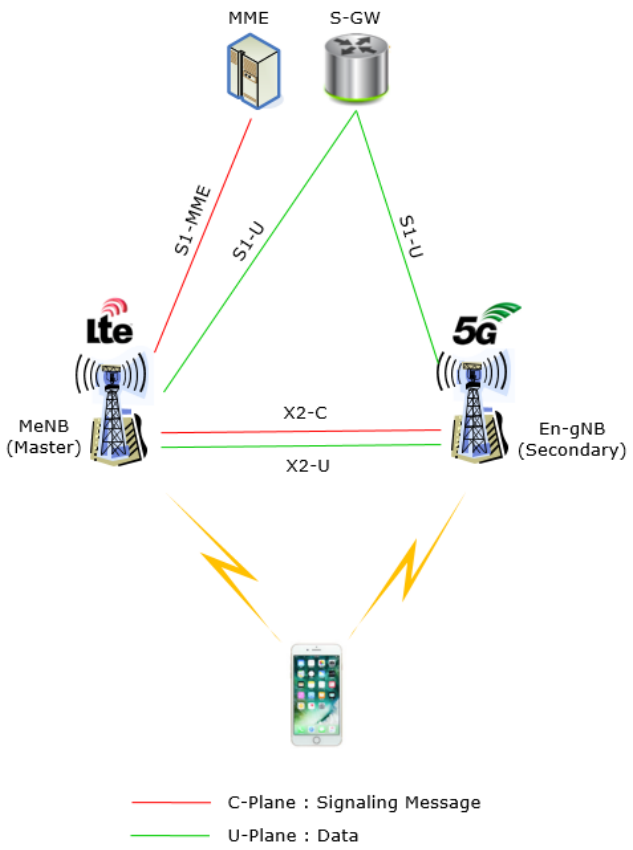

Figure 4.2.6-2: 5G NR NSA EN-DC Network Architecture with U-Plane connection from EPC to eNB and gNB

E-UTRA-NR Dual Connectivity (EN-DC) handles authentication and authorization through the LTE EPC. The 5G NR EN-DC architecture might be deployed in different architecture, depending on whether there is a U-Plane connection from eNB to EPC, or from gNB to EPC. Figure 4.2.6-2 depicts one such architecture of 5G NR NSA EN-DC, wherein, the Secondary Cell Group (SCG) bearer has a U-Plane connection between 5G NR gNB and the core network, as well as another U-Plane connection between the LTE eNB and 5G NR gNB to enable SCG split bearer.

4.3 FEATURES/FUNCTIONALITIES

4.3.1 CBRS UE PROFILE

4.3.1.1 CBRS LTE UE PROFILE

The section defines different capabilities of the LTE UE into CBRS Profiles. A UE can support one or more of these profiles. A CBRS Profile II based UE is the minimum level required for CBRSA NHN support. No assumptions are made about support for other radio technologies such as 3G.

LTE UE refers to a UE with or without EN-DC capability, where:

- EN-DC capability implies support for CBRS inter-band and/or intra-band operation.
- UE supports B48 for LTE-only operation or EN-DC operation with LTE in CBRS band.

UE can also support EN-DC operation with n48 for NR operation in CBRS band. Note: In EN-DC, it is assumed LTE connection is the MCG (Master Cell Group).

1. A CBRS-Profile I is support for 3GPP procedures with CBRS band.
    - A CBRS-Profile I based UE does not have the capability to attach to a CBRSA NHN and does not have the capability to support CBRSA NHN procedures.
    - A CBRS-Profile I based UE supports only 3GPP Access Mode (EPS-AKA) in CBRS band.
2. An extended CBRS-Profile I, also known as a CBRS-Profile I-A is the capability of attaching to 3GPP-based access mode (non-EPS-AKA)
    - A CBRS-Profile I-A based UE does not have the capability to attach to a CBRSA NHN and does not have the capability to support CBRSA NHN procedures.
    - A CBRS-Profile I-A based UE can either attach using 3GPP-based Access Mode (non-EPS-AKA) or using 3GPP Access Mode.
3. A CBRS-Profile II is the capability to support CBRSA NHN selection procedures, mobility procedures, security procedures, and RAN identifiers. A CBRS-Profile II based UE is capable of supporting a single LTE radio access network connection and dual EMM context. A CBRS-Profile II based device can be EMM Registered on at most one access network at a time.
    - For a CBRS-Profile II based UE, all PDN connections are assigned to the same access network (e.g., all on an SP network or all on CBRSA NHN).
    - A device based on CBRS-Profile II supports CBRS-Profile I and optionally supports CBRS-Profile I-A
4. A CBRS-Profile III based UE is capable of supporting a single LTE radio access network connection, dual EMM contexts, and can listen for paging on both EMM contexts, plus search and identify target cells on the non-serving CBRS Network or SP network (possibly at some cost to performance). A CBRS-Profile III based device can be EMM Registered on two access networks simultaneously.

- For a CBRS-Profile III based UE, PDN connections can be assigned to different access networks (e.g., Internet on the CBRSA NHN and VoLTE on the MNO network). Network-originated data for a PDN connection, if needed, triggers a paging procedure on the corresponding access network.

- Since a CBRS-Profile III based UE can connect to a single radio access network connection, it can send/receive data only on one access network at a time. In order for the network to maintain the correct EMM and ESM status of the UE, a CBRS-Profile III based UE may have to perform periodic TAU procedures on the access network where it is in IDLE state.

- A device based on CBRS-Profile III supports CBRS-Profile I and CBRS-Profile II. Such a device optionally supports CBRS-Profile I-A

5. A CBRS-Profile IV based UE is capable of supporting dual LTE radio access network connections simultaneously, dual EMM contexts, and dual ESM contexts.

    - User-plane data can flow over both ESM contexts simultaneously, at the granularity of PDN connections.

    - A device based on CBRS-Profile IV supports CBRS-Profile I and CBRS-Profile II. Such a device optionally supports CBRS-Profile I-A

6. A CBRS-Profile V based UE is capable of supporting a single LTE radio access network connection at a time, has multiple subscriptions and can have the ability to choose the subscription for specific services while using a different subscription for other services including voice. A CBRS-Profile-V based UE is capable of setting up an SWu tunnel via the EMM Registered Access Network to avail services using the other subscription (See Appendix A).

    - A device based on CBRS-Profile V supports CBRS-Profile I. Such a device optionally supports CBRS-Profile I-A and CBRS-Profile II.

The following table shows another view of the UE profiles.

Table 4.3.1.1-1: CBRS LTE UE Profile Relationship

CBRS UE Profile	**Supported Profiles**	**Optional Profile support**
CBRS-Profile I	None	None
CBRS-Profile I-A	CBRS-Profile I	None
CBRS-Profile II	CBRS-Profile I	CBRS-Profile I-A
CBRS-Profile III	CBRS-Profile I, CBRS-Profile II	CBRS-Profile I-A
CBRS-Profile IV	CBRS-Profile I, CBRS-Profile II	CBRS-Profile I-A
CBRS-Profile V	CBRS-Profile I	CBRS-Profile I-A, CBRS-Profile II

4.3.1.2 CBRS 5G NR UE PROFILE

The section defines different capabilities of the 5G NR UE into CBRS Profiles. A 5G NR UE can support one or more of these profiles.

Profile XI captures the capability of a 5G NR UE with single subscription. Profile XI-A is introduced to support 5G-non-SIM-Credential based authentication.

Profile XII is reserved to support 5G NR CBRSA NHN.

Profile XIII captures the capability of a 5G NR UE with multiple subscriptions with only one active Tx radio[1] connection at a time (e.g., DSDS), and Profile XIV captures the capability of a 5G NR UE with multiple subscriptions with more than one Tx radio connection at a time (e.g., DSDA). Similar to Profile III and Profile IV, Profile XIII and Profile XIV can optionally support 5G-non-SIM-Credential based authentication. The support of 5G NR CBRSA NHN is also not included in Profile XIII and Profile XIV and is not addressed in CBRSA Release 4.

NR UE refers to UE with or without NE-DC (dual connectivity with NR as MCG and LTE as SCG) / NN-DC (dual-connectivity with NR for both MCG and SCG) capability with 5GC as the core. The NE-DC / NN-DC capability is applicable to both CBRS inter-band and intra-band operation. At a minimum UE supports B48 or n48.

1. A CBRS-Profile XI supports for 3GPP procedures with CBRS band.
    - A CBRS-Profile XI based UE does not have the capability to attach to a CBRSA NHN and does not have the capability to support CBRSA NHN procedures.
2. An extended CBRS-Profile XI, also known as a CBRS-Profile XI-A is the capability of attaching using 5G-non-SIM-Credential based authentication.
    - Profile XI with the capability to support non-AKA (EAP-TLS and/or EAP-TTLS) based credentials.
    - Non-AKA implies EAP-TLS as defined in 3GPP TS 33.501 [26] and EAP-TTLS as defined in CBRSA-TS-1003 [12].
3. A CBRS-Profile XII is retained as placeholder for CBRSA NHN based UE profiles
4. A CBRS-Profile XIII based UE is capable of supporting a single LTE/NR radio access network connection, dual EMM / 5GMM contexts with at least one as 5GMM, and can listen for paging on both EMM / 5GMM contexts, plus search and identify target cells on the non-serving CBRS Network or SP network (possibly at some cost to performance). A CBRS-Profile XIII based device can be EMM / 5GMM Registered on two access networks simultaneously.

[1] A Tx radio refers to the radio chain associated with the MCG in the case of dual connectivity support.

- For a CBRS-Profile XIII based UE, PDN (EPC) / PDU (5GC) connections can be assigned to different access networks. Network-originated data for a PDN connection, if needed, triggers a paging procedure on the corresponding access network.

- Since a CBRS-Profile XIII based UE can connect to a single radio access network connection, it can send/receive data only on one access network at a time. In order for the network to maintain the correct EMM / 5GMM and ESM (EPC) / 5GSM (5GC) status of the UE, a CBRS-Profile XIII based UE may have to perform periodic TAU procedures (EPC) / periodic Registration Update (5GC) on the access network where it is in IDLE (EPC & 5GC) / INACTIVE (5GC) state.

- A device based on CBRS-Profile XIII supports CBRS-Profile XI. Such a device optionally supports CBRS-Profile XI-A

5. A CBRS-Profile XIV based UE is capable of supporting dual LTE / NR radio access network connections simultaneously, dual EMM / 5GMM contexts with at least one as 5GMM, and dual ESM (EPC) / 5GSM (5GC) contexts.

    - User-plane data can flow over both ESM (EPC) / 5GSM (5GC) contexts simultaneously, at the granularity of PDN (EPC) / PDU (5GC) connections.

    - A device based on CBRS-Profile XIV supports CBRS-Profile XI. Such a device optionally supports CBRS-Profile XI-A

6. A CBRS-Profile XV based UE is capable of supporting a single LTE / NR radio access network connection at a time, has multiple subscriptions and can have the ability to choose the subscription for specific services while using a different subscription for other services including voice. At least one of the subscriptions has to be a 5GC and the other can be either EPC or 5GC. A CBRS-Profile-XV based UE is capable of setting up an SWu as defined in 3GPP TS 23.402 [13] (EPC) / NWu as defined in 3GPP TS 24.502 [27] (5GC) tunnel via the EMM (EPC) / 5GMM (5GC) Registered Access Network to avail services using the other subscription (See Appendix A).

    - A device based on CBRS-Profile XV supports CBRS-Profile XI. Such a device optionally supports CBRS-Profile XI-A.

    - With EPC credentials ability to set up an SWu tunnel via the EMM Registered Access Network when the CBRS access connectivity is supported with NR credentials.

    - With 5GC credentials ability to set up an NWu tunnel between the UE and N3IWF of the 5GMM Registered Access Network when the CBRS access connectivity is supported with LTE credentials or NR credentials.

The following table shows another view of the UE profiles.

Table 4.3.1.2-1: CBRS NR UE Profile Relationship

CBRS UE Profile	**Supported Profiles**	**Optional Profile support**
CBRS-Profile XI	None	None
CBRS-Profile XI-A	CBRS-Profile XI	None
CBRS-Profile XII	Reserved	Reserved
CBRS-Profile XIII	CBRS-Profile XI	CBRS-Profile XI-A
CBRS-Profile XIV	CBRS-Profile XI	CBRS-Profile XI-A
CBRS-Profile XV	CBRS-Profile XI	CBRS-Profile XI-A

4.3.2 TRAFFIC LBO (TRAFFIC LOCAL BREAK OUT)

Some service scenarios require the subscribers' data traffic to stay local, that is, to be routed to networks and/or applications in proximity to the RAN elements. The reasons for local routing span from security and privacy constraints, performance improvement (e.g., latency), cost reduction, or other deployment preferences.

Exemplary use cases might be the following.

1. A large enterprise consists of several facilities distributed around geographically scattered sites. Each site may have different service relations with the mobile network infrastructure providers locally available, utilizing more than one of the service models among those described in the following sections. For instance, the enterprise might deploy the Private Network model for the primary site, which is in charge of subscriber authentication, UE IP address assignment and bearer creation for the other connected sites as well. Still, the organization requires to collect part of the user traffic generated from all the sites at the primary site and offload the remaining at each corresponding site. Because users may move from one site to the other, a single default APN is provisioned in all the subscribers' devices, which resolves to a single Packet Data Gateway sitting on the primary site.

2. An MNO services its users localized at a given defined venue, such as a stadium, a theme park, and similar, using the local third party's CBRS network infrastructure. In addition, the facility houses some sort of app-based service to customers for enhanced user experience, like real time video streaming, AR/VR entertainment, video clips and others. Since the information is meant to be produced and consumed on site, the MNO aims at routing the traffic associated to those applications locally, avoiding hauling it to the centralized EPC/5GC.

3. An Industrial IoT (IIoT) deployment enables robots, machinery and other equipment within a factory with cellular connectivity. The equipment might be connected to local servers for the closed control loop as well as to remote servers for data storage and processing.

4. An SP may leverage the public cloud infrastructure to run the EPC/5GC control plane, whereas the data plane is routed through on-premise infrastructure, ensuring traffic isolation so that users belonging to different logical networks can have the traffic breakout to different and separated local network segments.

There is no 3GPP-defined mechanism for an LTE network to enable traffic offload of all or some UE traffic associated to a single PDN connection, as per the use cases listed above. Such enablers essentially embed part of or all the 3GPP EPC gateways' functionalities (and this approach is defined in 5G specifications too) in the LTE Network to enable the Traffic LBO feature described above. Such network element implementing the Traffic LBO enabler may be deployed as part of the CBRS Network and thus belong to the CBRS Network Operator. In this case, the relation between the SP and the CBRS Network Operator should provide means to let the former control and authorize which traffic should be broken out by the latter.

For 5G SA networks, 3GPP has specified non-roaming architecture in section 4.2.3 (Figure 4.2.3-4) of 3GPP TS 23.501 [20] that supports the option of having multiple UPF (User Plane Function), with each UPF handling one/more PDUs within an UE session. All these UPFs can be controlled by one SMF or there can be one SMF controlling one UPF. If the service provider wants to deploy a CBRS based 5G SA network with the intent of supporting Traffic Local Breakout, the service provider may deploy one UPF (along with the control plane entities) centrally in a public cloud and/or in a private cloud infrastructure and another UPF within or near a venue. Subsequently, using pre-provisioned policies (subscription or network level) it is possible to ensure Local Breakout of some/all PDU sessions or even a part of traffic within a PDU, using the UPF that is deployed within/near the venue.

4.3.2.1 TRAFFIC LBO - USE CASE MAPPING

The ability to route traffic to a local network may be a feature of a CBRS-based deployment based on any of the service relations described in section 4.2. However, in the general case, not all the user data traffic needs to be forwarded to a local network, and different filtering granularity may be necessary, often demanding to seamlessly offload part of traffic of the same UE. Thus, SP's alone may authorize and select the traffic to be broken out, regardless if the local network and applications belong to the SP or not.

4.3.3 ROAMING SUPPORT

CBRS based networks can be deployed using the SHNI or any PLMN-ID. Various use cases for CBRS based networks as defined in Section 4.2. Of these use cases, when CBRS based Private and Hybrid networks are deployed using SHNI, the CBRS Service Provider may enter into business agreements with other SPs or CBRS Service Providers. Via such business agreements, the CBRS network operators can enable roaming of their own subscribers into other networks or can allow their own network to serve the subscribers of other networks (as Visited Network).

Two categories of services can be offered by the Visited Network for the in-bound roamers (or subscribers belonging to other operators) – Data only services and/or IMS-Based services. 3GPP TS 23.401 covers the aspects of Home Routing and LBO of PDN services in the Visited Network. All these aspects covered in the 3GPP specifications are based on the underlying premise that all networks are separated using unique PLMN ID. Since all SHNI based networks use the same PLMN ID (SHNI), prevalent procedures for resolving the

Home Operator cannot be used to identify the Home CBRS Operator. The contents of this specification focus on the following aspects –

- Authentication procedure: The procedure by which the subscribers are authenticated and authorized in a Visited Network. In order to complete the Authentication procedure, the Visited Network have to use IBN to locate the Home Network. For example, Locating Home HSS can be done using DSC (based on IBN in the IMSI)
- PDN Service resolution: This includes APN management and resolution since the combination of APN and PLMNID may no longer be universally unique. For resolving APNs, IBN in the IMSI should be considered.

Note :

- This specification does not consider subscribers belonging to non-SHNI based operator network roaming into SHNI based CBRS networks. Since non-SHNI based operators will have a unique PLMN ID, 3GPP TS 23.401 [9] and GSMA IR.88 [17] specification capture the details for such roaming support.
- 3GPP Rel-16 does not support roaming for SNPN; therefore, SNPN does not support roaming scenarios for CBRSA Rel-4. For SNPN, support for roaming is FFS in future 3GPP releases.

4.3.3.1 ROAMING SUPPORT FOR DATA ONLY SERVICES

Data only services involve all the services that do not require an IMS. However, data services may include OTT voice. Data services can be Home Routed or Local Breakout at the Visited Network and such policy decisions are beyond the scope of this specification.

4.3.3.2 ROAMING SUPPORT FOR IMS-BASED SERVICES

The support for IMS-based services, such as VoLTE, SMS over IMS, etc. might be available at CBRS Network operators that use the SHNI. Such services are available to subscribers when they roam out of their home CBRSA network, in which case the Visited Network may be provided by an MNO that does not use the SHNI or a CBRS Network Operator that uses the SHNI.

The use of the SHNI poses some limitations in the ability of legacy network operators to route IMS-based services for visiting subscribers. The CBRSA specifications define methods to support roaming for IMS-based services to subscribers that belong to a CBRS Network Operator that uses the SHNI. Furthermore, IMS-based services roaming is described in the scenario of a Visited Network that operates as a NHN.

4.3.3.3 ROAMING SUPPORT – USE CASE MAPPING

This feature is applicable for all roaming scenarios where either the EPC HPLMN or EPC VPLMN uses SHNI. For all those scenarios where EPC HPLMN and EPC VPLMN use uniquely identifiable PLMN ID, 3GPP TS 23.401 [9] and GSMA IR.88 [17] specification apply. In order to support roaming, a business agreement, also referred as roaming agreement, is essential between the Service Provider of the Home and the Visited PLMN. The roaming support for the use cases described in section 4.2 are as follows:

- CBRS Service Provider Operating a Private network can enter into such roaming agreements with other Service Providers. When such agreements are in place, the private network may serve as Home PLMN or Visited PLMN depending on the roaming scenario.
- A NHN operator does not offer service to subscribers in the NHN. A PSP offers service to subscribers in the NHN. The agreement between NHN Operator and PSP are not considered as roaming agreements. Any PSPs offering a service to subscribers via the CBRS NHN may enter into a roaming agreement with other Service Providers. In such scenario roaming is based on the PLMN ID operated by the PSP.
- In a scenario that a CBRS Service Provider also offer a Neutral Host service, i.e. the network is a Hybrid Network, the CBRS Service Provider and/or PSPs in such a network may enter into a roaming agreement with other Service Providers. In such scenario roaming is based on the PLMN ID operated by the PSP or the PLMN ID used by the CBRS Service Provider (depending on UE policies).

5. NETWORK SERVICE REQUIREMENTS

These requirements support the use cases defined in section 4.

5.1 USE CASE REQUIREMENTS

5.1.1 CBRSA NHN USE CASE

This section includes requirements for sharing LTE radio access and the CBRSA NHN Core network among multiple Participating Service Providers. The support of CBRS-A Neutral Host Networks with 5G NR SA architectures or 5G NR NSA architectures may be addressed in future CBRS Alliance releases.

5.1.1.1 CBRSA NHN RAN SHARE REQUIREMENTS

R1-NHN-RSH-001	It shall be possible to organize a set of LTE CBSDs as a CBRSA Neutral Host Network (NHN) providing LTE radio access to multiple Participating Service Providers (PSPs).
R1-NHN-RSH-002	It shall be possible to organize a set of LTE CBSDs to provide LTE radio access to private network services.
R1-NHN-RSH-003	It shall be possible to configure a CBRSA NHN to provide different portions of available radio resources to each PSP based on business agreements.
R2-NHN-RSH-004	The identity of the CBRS Network is broadcast via System Information SIB1 by the CBRS RAN, and includes a PLMN-ID. The PLMN-ID may be a shared PLMN-ID assigned by the IMSI-Administrator for CBRS operators, or a PLMN-ID used by the operator.
R2-NHN-RSH-005	The Cell identity of the CBRS cell is broadcasted via System Information by the CBRS RAN, and shall be unique within any CBRS shared PLMN-ID.

R2-NHN-RSH-006	It shall be possible for the user to manually select the Participating Service Provider in a CBRS network.
R2-NHN-RSH-007	It shall be possible to authorize local breakout of all or some UE traffic.

5.1.1.2 CBRSA NHN RAN DISCOVERY REQUIREMENTS

R1-NHN-DIS-001	A CBRSA NHN shall broadcast system information that enables discovery of the NHN and associated PSPs.

5.1.1.3 CBRSA NHN AUTHENTICATION REQUIREMENTS

R1-NHN-AUT-001	A CBRSA NHN shall be able to cooperate with the PSP's network to support one or more of the following: - authentication using USIM-based credentials. - authentication using certificate-based credentials, - authentication using Username/Password.
R1-NHN-AUT-002	A CBRSA NHN shall be capable to support one or more of the following: - local authentication with an authentication server dedicated to the network, - authentication using external authentication server(s).
R1-NHN- AUT-003	It shall be possible for a CBRSA NHN UE to support multiple authentication protocols.
R1-NHN- AUT-004	It shall be possible for a CBRSA NHN UE to establish a secure tunnel with a service provider's ePDG using credentials associated with the service provider's subscription.
R1-NHN- AUT-005	A Private Network and a CBRSA NHN that has its own subscribers shall be able to authenticate its own subscribers.

5.1.1.4 CBRSA NHN MOBILITY REQUIREMENTS

R1-NHN-MOB-001	A CBRSA NHN shall support mobility between the cells of the CBRSA NHN RAN per 3GPP specifications (intra-CBRSA NHN mobility).

R1-NHN-MOB-002	A CBRSA NHN shall support the continuity of PDN connections using handover procedures defined in 3GPP specifications from the NHN network to a PSP operator network (e.g., HO from a CBRSA NHN to a MNO with PDN continuity) and also from the PSP operator network into the NHN network.

5.1.1.5 CBRSA NHN GENERAL SECURITY REQUIREMENTS

This section provides requirements regarding the security aspects of a CBRSA NHN.

R1-NHN-SEC-001	A CBRSA NHN shall be capable of cooperating in the authentication of a device by the PSP's core network.
R1-NHN-SEC-002	A CBRSA NHN shall be able to securely provide the KPIs to the PSP as per the mutually agreed security policies.
R1-NHN-SEC-003	A CBRSA NHN shall not disclose KPIs of a PSP to other PSPs.

5.1.1.6 CBRSA NHN MEASUREMENT REQUIREMENTS

The requirements in this section do not apply to Private Network use case.

R1-NHN-MES-001	A CBRSA NHN shall be capable of providing Key Performance Indicators (KPIs) to a PSP regarding the service and resources provided to the PSP.
R1-NHN-MES-002	A CBRSA NHN shall allow a PSP request to fetch KPIs per a mutually agreed SLA.
R1-NHN-MES-003	A CBRSA NHN shall provide individual and aggregated KPIs to the PSP per a mutually agreed SLA.
R1-NHN-MES-004	A CBRSA NHN shall be capable of providing byte counts of user data transmitted between the PSP and the UE in both uplink and downlink directions, within a pre-determined time period via the CBRSA NHN, to the PSP.
R1-NHN-MES-005	A CBRSA NHN shall support a minimum set of KPIs consistent with those specified by 3GPP per a mutually agreed SLA.
R1-NHN-MES-006	A CBRSA NHN shall support, per PSP, the KPI and counters related to Call/Session establishment Success Rate as specified by Accessibility KPI in 3GPP TS 32.450 [4] and by counters to calculate this KPI in 3GPP TS 32.425 [5].

R1-NHN-MES-007	A CBRSA NHN shall support, per PSP, the KPIs and counters as specified by Accessibility EPS Attach Success Rate KPI in 3GPP TS 32.455 [6] and by counters to calculate this KPI in 3GPP TS 32.426 [7].
R1-NHN-MES-008	A CBRSA NHN shall support, per PSP, the KPIs and counters related to Call / Session Drop rate as specified by Retainability KPI in 3GPP TS 32.450 [4] and by counters to calculate this KPI in 3GPP TS 32.425 [5].

5.1.2 MSO USE CASE

5.1.2.1 MSO SPECIFIC RAN REQUIREMENTS

R2-MSO-RAN-001	When a UE with 2 subscriptions – one subscription belonging to an MSO and another subscription belonging to an MNO enters the CBRS operator network deployed by the MSO, the UE shall be able to attach to the CBRS operator's network using the MSO subscription for all non-voice PDN services. For all voice-based services including VoLTE, the UE shall be able to attach to the MNO operator's network using the MNO subscription. The CBRS network architecture shall be able to support such a UE behavior.
R4-MSO-RAN-002	When a NR capable UE with 2 subscriptions with at least one of the subscriptions belonging to an MSO and another subscription belonging to an MNO enters the CBRS operator network deployed by the MSO, and at least one of the subscriptions is a 5GC subscription, the UE shall be able to attach/register to the CBRS operator's network using the MSO subscription for all non-voice PDN services. For all voice-based services including VoLTE / VoNR, the UE shall be able to attach / register to the MNO operator's network using the MNO subscription. The CBRS network architecture shall be able to support such a UE behavior.

5.1.3 FIXED WIRELESS NETWORK USE CASE

5.1.3.1 CBRSA FIXED WIRELESS NETWORK ACCESS ARCHITECTURE REQUIREMENTS

R2-FWN-ARC-001	It shall be possible for a Fixed Wireless Network to enable interworking with another Service Provider's existing non-3GPP AAA for subscription authentication, authorization and accounting.
R2-FWN-ARC-002	A Fixed Wireless Network shall support network (Radio Access and Core Networks) sharing mechanisms for interworking with multiple SP.

R2-FWN-ARC-003	A Fixed Wireless Network shall support delegation of IP address allocation for the subscriber to the corresponding SP, including interworking with SP's AAA or DHCP server.
R2-FWN-ARC-004	A Fixed Wireless Network should be able to support multiple PDNs per UE (e.g., for separation of Internet and VoIP networks), as per 3GPP specifications.

5.1.3.2 CBRSA FIXED WIRELESS NETWORK ACCESS SERVICE REQUIREMENTS

R2-FWN-SVC-001	A Fixed Wireless Network should allow Over-the-Air service and subscription activation based on 3GPP specifications (e.g. 3GPP TS 31.116) or operator specific methods.
R2-FWN-SVC-002	A Fixed Wireless Network should enable Layer 2 data services (native Ethernet or IEEE 802.1q VLAN) to its end-users, including one or more of the following: - Native Ethernet (untagged) user traffic - Single or Multiple Point-to-Point VLAN services for the user - Single or Multiple Point-to-Multipoint VLAN services for the user
R2-FWN-SVC-003	When providing Layer 2 services, A Fixed Wireless Network should provide native wireless infrastructure QOS per user L2 data flow, classified by one or more of the following fields: - 802.1q VLAN Identity - 802.1p priority bits - IP-layer DSCP value

5.2 CBRS NETWORK FEATURE/FUNCTIONALITIES REQUIREMENTS

5.2.1 3GPP-BASED ACCESS MODE (NON-EPS-AKA)

5.2.1.1 GENERAL REQUIREMENTS

R2-XAU-GEN-001	It shall be possible for the service provider to provision an IMSI to the non-EPS-AKA subscription.

R2-XAU-GEN-002	A CBRS Network that supports 3GPP-based Access Mode (non-EPS-AKA) shall support all procedures as defined in 3GPP TS 23.401 with the ability of supporting non-EPS-AKA subscription for attaching the UE.

5.2.1.2 AUTHENTICATION REQUIREMENTS

R2-XAU-AUT-001	A CBRS Network that supports 3GPP-based Access Mode (non-EPS-AKA) shall support multiple non-EPS-AKA authentication mechanisms including EAP-TLS and EAP-TTLS.
R2-XAU-AUT-002	A CBRS Network that supports 3GPP-based Access Mode (non-EPS-AKA) shall be able to identify the UE based on the IMSI provided by the UE during the 3GPP-based Access Mode (Non-EPS-AKA) attach procedure.
R2-XAU-AUT-003	A CBRS Network that supports 3GPP-based Access Mode (non-EPS-AKA) shall be able to allocate GUTI at the end of an IMSI based successful initial attach using a non-EPS-AKA subscription.

5.2.2 UE REQUIREMENTS

5.2.2.1 LTE UE REQUIREMENTS

The UE requirement in this section apply to LTE UEs as defined in section 4.3.

R2-UEP-GEN-001	It shall be possible for a UE that is operating as defined in CBRS-Profile III, CBRS-Profile IV, or CBRS-Profile V to be able to support dual subscriptions – one USIM based subscription and another can be a USIM or certificate-based or username-password subscription (non-EPS-AKA).
R2-UEP-GEN-002	A UE that is operating as defined in CBRS-Profile III shall be able to maintain 2 EMM contexts (with independent PDN connections over active and inactive access network) using a single LTE radio access network connection and may have to perform all requisite session maintenance procedures like TAU even on the access network where it is in IDLE state.
R2-UEP-GEN-003	It shall be possible for the UE to support multiple authentication related mechanisms and protocols based on USIM, certificate, and username-password (e.g., EPS-AKA, EAP-AKA, EAP-AKA', EAP-TLS, EAP-TTLS) and to store the credentials in the USIM or a secure location in the UE.

R2-UEP-GEN-004	It shall be possible for a UE that is operating as defined in CBRS-Profile V to be able to support dual USIM subscriptions or one USIM and one non-USIM subscription.
R2-UEP-GEN-005	A UE that is operating as defined in CBRS-Profile V shall be able to establish SWu as defined in 3GPP TS 23.402 [13] like tunnel for specific PDN services via the LTE network to which it is attached.
R2-UEP-GEN-006	A multi-subscription UE that that is operating as defined in UE-Profile III, UE-Profile IV or UE-Profile V, it shall be possible to provision a preferred operator (subscription and network) to which the UE shall always attach, whenever such operator network is available.
R2-UEP-GEN-007	If a preferred operator network is provisioned in a multi-subscription UE that is operating as defined in CBRS-Profile III, CBRS-Profile IV or CBRS-Profile V, the UE shall always attach to the preferred operator network using the credentials of the preferred operator and shall always use the credentials of the non-preferred operator to attach to the non-preferred operator network.
R2-UEP-GEN-008	In a multi-subscription UE that operates as defined in CBRS-Profile III, CBRS-Profile IV or CBRS-Profile V, it shall be possible to provision a policy such that some specific PDN services are always obtained using one of the subscriptions from the network of the operator pertaining to the subscription.
R2-UEP-GEN-009	When attached to the non-preferred operator network, it shall be possible for the multi-subscription UE that operates as defined in CBRS-Profile III or CBRS-Profile V, to periodically perform background scanning to detect the presence of the preferred operator network.
R2-UEP-GEN-010	When a multi-subscription UE that is operating as defined in CBRS-Profile III, CBRS-Profile IV or CBRS-Profile V is attached to non-preferred operator network and detects the presence of the preferred operator network, it shall be possible for the UE to attach to the preferred operator network using the preferred operator credentials. However, when operating as defined in CBRS-Profile III or CBRS-Profile V such an attach procedure shall be done only when all PDN sessions are in IDLE state.
R2-UEP-GEN-011	When a multi-subscription UE that is operating as defined in CBRS-Profile III is attached to the preferred operator network, it shall be possible for the UE to answer the paging request for itself from non-preferred operator network.
R2-UEP-GEN-012	When a multi-subscription UE that is operating as defined in CBRS-Profile III or CBRS-Profile IV is attached to the preferred operator network, it shall be possible for the UE to attach to the non-preferred operator network in order to obtain the PDN services that are provisioned to use the non-preferred operator network only. In such an event, it shall be possible for the UE to move all other active PDNs to non-preferred operator network.
R2-UEP-GEN-013	When a multi-subscription UE that is operating as defined in CBRS-Profile V is attached to preferred operator network, it shall be possible for the UE to establish an SWu like tunnel with the non-preferred operator network in order to obtain the PDN services that are provisioned to use the non-preferred operator network only.

R2-UEP-GEN-014	When a multi-subscription UE that is operating as defined in CBRS-Profile III, CBRS-Profile IV or CBRS-Profile V is attached to a preferred operator network and moves beyond the coverage area of the preferred operator network, the UE shall attempt to attach to non-preferred operator network (if detected and supported, and not already attached) and it shall be possible to move all active PDN connections to the non-preferred operator network. The attach to non-preferred operator network can happen irrespective of the state of the PDN sessions.
R2-UEP-GEN-015	Whenever the preferred operator network is not available, it shall be possible for a multi-subscription UE that is operating as defined in CBRS-Profile III, CBRS-Profile IV or CBRS-Profile V to attach to a detected and supported non-preferred operator network using the non-preferred operator network subscription and obtain all PDN services from the non-preferred operator network.
R2-UEP-GEN-016	It shall be possible for a UE that is operating as defined in CBRS-Profile III, Profile IV or CBRS-Profile V to remember the network where it had successfully attached along with the respective subscription/credentials that the UE used to attach. A UE shall then use the same subscription for attaching to the same network whenever the subscriber visits the same network in the future. The subscription can be USIM or non-USIM and the credentials can be information related to the network (like PSP ID, NHN ID in case of CBRSA NHN) or information generated during the initial attach procedure (like GUTI).
R2-UEP-GEN-017	For a UE that is capable of supporting 3GPP-based Access Mode (non-EPS-AKA) or NHN Access Mode with non-USIM credentials, it shall be possible to securely store non-USIM credential including IMSI, certificates, username/password, network preferences and mobility policy.
R2-UEP-GEN-018	It shall be possible for a UE that is operating as defined in CBRS-Profile III, CBRS-Profile IV or CBRS-Profile V to support multiple Access Modes.
R2-UEP-GEN-019	A multi-subscription UE that is operating as defined in CBRS-Profile III, Profile IV or CBRS-Profile V shall be able to establish PDN connections using the appropriate access mode [3GPP Access Mode (EPS-AKA), 3GPP-based Access Mode (non-EPS-AKA) or NHN Access Mode (using USIM or non-USIM credential)] based on subscription type.

5.2.2.2 UE NR REQUIREMENTS

The UE requirement in this section apply to NR UEs as defined in section 4.3.

R4-UEN-GEN-001	A UE supporting CBRS-Profile XIII, CBRS-Profile XIV, or CBRS-Profile XV shall support dual subscriptions – one USIM based subscription and another can be a USIM or certificate-based or username-password subscription (5G-non-SIM-Credential).
R4-UEN-GEN-002	A UE supporting CBRS-Profile XIII shall support dual EMM / 5GMM contexts with at least one as 5GMM, (with independent PDN (EPC) / PDU (5GC) connections over active and inactive access network) using a single LTE / NR radio access network connection and may have to perform all requisite session maintenance procedures like TAU (EPC) / periodic Registration Update (5GC) even on the access network where it is in IDLE / INACTIVE state.

R4-UEN-GEN-003	A UE shall support one or more protocols based on USIM, certificate, and username-password (e.g., EPS-AKA, EAP-AKA, 5G-AKA, EAP-AKA', EAP-TLS, EAP-TTLS) and to store the credentials in the USIM or a secure location in the UE.
R4-UEN-GEN-004	A UE supporting CBRS-Profile XV shall support dual USIM subscriptions or one USIM and one non-USIM subscription.
R4-UEN-GEN-005	A UE supporting CBRS-Profile XV shall support establishing NWu (defined in 3GPP TS 23.502 [21]) / SWu (defined in 3GPP TS 23.402 [13]) like tunnel for specific PDN / PDU services via the LTE/5G network to which it is attached/registered.
R4-UEN-GEN-006	A UE supporting CBRS-Profile XIII, CBRS-Profile XIV or CBRS-Profile XV shall support provisioning a preferred operator (subscription and network) to which the UE shall always attach/register whenever such operator network is available.
R4-UEN-GEN-007	If a preferred operator network is provisioned in a multi-subscription UE that is operating as defined in CBRS-Profile XIII, CBRS-Profile XIV or CBRS-Profile XV, the UE shall always attach/register to the preferred operator network using the credentials of the preferred operator and shall always use the credentials of the non-preferred operator to attach/register to the non-preferred operator network.
R4-UEN-GEN-008	A multi-subscription UE supporting CBRS-Profile XIII, CBRS-Profile XIV or CBRS-Profile XV shall provision a policy such that some specific PDN / PDU services are always obtained using one of the subscriptions from the network of the operator pertaining to the subscription.
R4-UEN-GEN-009	When attached/registered to the non-preferred operator network, a multi-subscription UE supporting CBRS-Profile XIII or CBRS-Profile XV shall periodically perform background scanning to detect the presence of the preferred operator network.
R4-UEN-GEN-010	When a multi-subscription UE supporting CBRS-Profile XIII, CBRS-Profile XIV or CBRS-Profile XV is attached/registered to non-preferred operator network and detects the presence of the preferred operator network, the UE shall attach/register to the preferred operator network using the preferred operator credentials. However, when operating as defined in CBRS-Profile XIII or CBRS-Profile XV such an attachment/registration procedure shall be done only when all PDN / PDU sessions are in IDLE / INACTIVE state.
R4-UEN-GEN-011	When a multi-subscription UE supporting CBRS-Profile XIII is attached/registered to the preferred operator network, it shall be possible for the UE to answer the paging request for itself from non-preferred operator network, subject to the RRC connected state on the preferred network, and the service priority on the paging service received on the non-preferred network.
R4-UEN-GEN-012	When a multi-subscription UE supporting CBRS-Profile XIII or CBRS-Profile XIV is attached/registered to the preferred operator network, it shall be possible for the UE to attach/register to the non-preferred operator network in order to obtain the PDN / PDU services that are provisioned to use the non-preferred operator network only. In such an event, the UE may move any other active PDNs / PDUs to non-preferred operator network.

R4-UEN-GEN-013	When a multi-subscription UE suppotting CBRS-Profile XV is attached/registered to preferred operator network, it shall be possible for the UE to establish an NWu / SWu like tunnel with the non-preferred operator network in order to obtain the PDN / PDU services that are provisioned to use the non-preferred operator network only.
R4-UEN-GEN-014	When a multi-subscription UE suppotting CBRS-Profile XIII, CBRS-Profile XIV or CBRS-Profile XV is attached/registered to a preferred operator network and moves beyond the coverage area of the preferred operator network, the UE should attempt to attach/register to non-preferred operator network (if detected and supported, and not already attached/registered) and it shall be possible to move all active PDN /PDU connections to the non-preferred operator network that are provisioned to use the non-preferred operator network. The attachment/registration to non-preferred operator network can happen irrespective of the state of the PDN / PDU sessions.
R4-UEN-GEN-015	Whenever the preferred operator network is not available, it shall be possible for a multi-subscription UE supporting CBRS-Profile XIII, CBRS-Profile XIV or CBRS-Profile XV to attach/register to a detected and supported non-preferred operator network using the non-preferred operator network subscription and obtain all PDN / PDU services from the non-preferred operator network.
R4-UEN-GEN-016	A UE supporting CBRS-Profile XIII, Profile XIV or CBRS-Profile XV shall remember the network where it had successfully attached/registered along with the respective subscription/credentials that the UE used to attach/register. The UE shall then use the same subscription for attaching/registering to the same network whenever the subscriber visits the same network in the future. The subscription can be USIM or non-USIM and the credentials can be information related to the network (like 5G-NID) or information generated during the initial attachment/registration procedure (like 5G-GUTI / GUTI).
R4-UEN-GEN-017	A UE supporting 5G-non-SIM-Credential shall securely store non-USIM credential including IMSI, certificates, username/password, network preferences and mobility policy.
R4-UEN-GEN-018	A UE supporting CBRS-Profile XIII, CBRS-Profile XIV or CBRS-Profile XV may support multiple Access Modes.
R4-UEN-GEN-019	A multi-subscription UE supporting CBRS-Profile XIII, Profile XIV or CBRS-Profile XV shall be able to establish PDN / PDU connections using the appropriate access mode [3GPP Access Mode (EPS-AKA), 3GPP-based Access Mode, NHN Access Mode applicable to LTE subscription, and 5G NR access using 5G-AKA or 5G-non-SIM-Credential (using USIM or non-USIM credential)] based on subscription type.

5.2.2.3 UE REQUIREMENTS FOR GEOFENCING

R5-GEO-UEP-001	The UE shall support the provisioning of Private CBRS / Non-Public Network service provider identifier as part of a Private CBRS / Non-Public Network service provider's subscription.

R5-GEO-UEP-002	The UE shall be capable of reading the Private CBRS / Non-Public Network service provider identifier that may be stored in the subscription.
R5-GEO-UEP-003	The UE shall support storing multiple Private CBRS / Non-Public Network service providers subscription, and each of these subscription may contain Private CBRS / Non-Public Network service provider identifier.
R5-GEO-UEP-004	A given UE subscription that supports access to an Private CBRS / Non-Public Network hosting LTE and/or NR connectivity may be associated with a single Private CBRS / Non-Public Network identifier, if provisioned as part of subscription.
R5-GEO-UEP-005	The UE should support requesting for Private CBRS / Non-Public Network geofencing information for a proviosioned subscription, when such information is not already provisioned at the UE, or such information needs to be updated at the UE.
R5-GEO-UEP-006	The UE shall posses and use valid credentials to access the geofencing provisioning server associated with Private CBRS / Non-Public Network subscription.
R5-GEO-UEP-007	Associated with each subscription, the UE should support receiving the geofencing information of the Private CBRS / Non-Public Network, when provided by the network.
R5-GEO-UEP-008	UE may provide Private CBRS / Non-Public Network identifier(s), or its current geolocation, when it requests for geofencing information
R5-GEO-UEP-009	The UE may use the geofencing information provided to optimize its system camping procedures to find and camp on preferred LTE / 5G NR Private CBRS / Non-Public Networks.
R5-GEO-UEP-010	The UE may use the geofence information to determine the Private CBRS / Non-Public Network subscription to use amongst the stored subscriptions in the device.
R5-GEO-UEP-011	The UE may use the Private CBRS / Non-Public Network specific deployment information to determine its camping preferences for the Private CBRS / Non-Public Network including networks that matches the cell broadcast information specific signature.

5.2.2.4 UE REQUIREMENTS FOR TAC COLLISION AVOIDANCE

R5-TAC-UEP-001	The UE may receive the broadcast message of the Home eNB name and compare it with the Private CBRS / Non-Public identifier associated with the credentials stored in the device prior to camping on the cell.
R5-TAC-UEP-002	The UE may match the provisioned eNB ID ranges with the broadcasted eNB ID associated with an Private CBRS / Non-Public credential prior to camping on a cell.
R5-TAC-UEP-003	The UE may enhance the MDT data collection and reporting procedures to include both the PLMN ID and the Private CBRS / Non-Public ID that is supported as Home eNB name from the Private CBRS / Non-Public networks that it encounters.

5.2.3 TRAFFIC LBO REQUIREMENTS

5.2.3.1 TRAFFIC LBO ARCHITECTURE REQUIREMENTS

R3-TLB-ARC-001	The CBRS Network may support the *Traffic Local Breakout (Traffic LBO)* feature, by which it is possible to authorize and enable forwarding all or some UE traffic associated to a single PDN connection or multiple PDN connections to networks and/or applications in proximity to the RAN elements.
R3-TLB-ARC-002	For the CBRS Network to enable the Traffic LBO feature, the SP and the CBRS Network Operator shall jointly agree on services authorized for Traffic LBO.
R3-TLB-ARC-003	When the CBRS Network supports the Traffic LBO feature, the network element that enables traffic breakout shall support the 3GPP-defined procedures for mobility and session management, charging and lawful intercept.

5.2.4 ROAMING REQUIREMENTS FOR CBRS NETWORKS

5.2.4.1 ROAMING REQUIREMENTS FOR DATA ONLY SERVICES

The requirements in this section is applicable to all use cases where 3GPP Access Mode and 3GPP-based Access Mode (non-EPS-AKA) are used.

R3-ROM-DAT-001	Whenever a Visited LTE Network (CBRS or a non-CBRS Network) is deployed with an intent to provide service to visiting subscribers that belong to other HNI based CBRS Network operators, the LTE network shall interface with an appropriate function (internal or external function) to determine the respective Home Network HSS based on IBN, in order to authenticate and authorize the visiting subscriber.
R3-ROM-DAT-002	When the LTE Network (CBRS or a non-CBRS Network) communicates with an external function to determine the respective Home Network HSS (based on IBN), such interface shall comply with the Security requirements specified in GSMA Guidelines for LTE and EPC Roaming (GSMA IR.88 [17]).
R3-ROM-DAT-003	A visited LTE Network (CBRS or a non-CBRS network) deployed with an intent to provide data services to visiting subscribers belonging to other SHNI based CBRS Network operators may enable Local Break-out of all or some of the visiting subscribers' data traffic.
R3-ROM-DAT-004	A visited LTE Network (CBRS or a non-CBRS network) that provide home routed data services to visiting subscribers of other SHNI based CBRS Network operators shall establish the 3GPP/GSMA specified roaming interfaces

	(e.g. S8 as defined in 3GPP TS 23.401 [9] and N16 as defined in 3GPP TS 23.502 [21]) towards SHNI based CBRS Network.
R3-ROM-DAT-005	A Visited LTE Network (CBRS or a non-CBRS network) admitting subscribers belonging to other SHNI based CBRS network operators may record KPIs and other counters relevant to visited subscribers' data that is offloaded to the visited LTE network. SuchKPIs or counters may be provided to the SHNI based CBRS Network.

5.2.4.2 ROAMING REQUIREMENTS FOR IMS-BASED SERVICES

The requirements in this section is in addition to the requirements in section 5.2.4.1 and are applicable when providing Roaming support for IMS-Based services.

R3-ROM-IMS-001	When a CBRS Network supports IMS-based services, such as VoLTE, it shall follow relevant 3GPP specifications (3GPP TS 23.228 [18]).
R3-ROM-IMS-002	Roaming support for IMS-based services shall be provided by a Visited Network to subscribers that belong to a CBRS Network Operator that uses the SHNI.
R3-ROM-IMS-003	void

5.2.5 NR AND 5GC REQUIREMENTS

5.2.5.1 GENERAL REQUIREMENTS

R4-5GC-GEN-001	As per 3GPP requirements, the network based on 5GC shall support primary authentication methods of 5G-AKA and EAP-AKA' as per 3GPP TS 33.501 [26].
R4-5GC-GEN-002	The Non Public Network (NPN) based on 5GC such as SNPN or PNI-NPN may support primary authentication method of EAP-TLS. If supported, EAP-TLS implementation shall follow Annex B and Annex I of 3GPP TS 33.501 [26].
R4-5GC-GEN-003	The Non Public Network (NPN) based on 5GC such as SNPN or PNI-NPN may support primary authentication method of EAP-TTLS. If supported, EAP-TTLS implementation shall follow CBRSA TS-1003 [12].

5.2.5.2 NR SNPN REQUIREMENTS

R4-SNN-GEN-001	When SNPN is supported, the network shall follow relevant 3GPP Rel-16 specifications.
R4-SNN-GEN-002	The SNPN deployed using SHNI shall only use AM = 0 or AM = 2.

5.2.5.3 NR PNI-NPN REQUIREMENTS

R4-PNN-GEN-001	When PNI-NPN is supported, the network shall follow relevant 3GPP Rel-16 specifications.
R4-PNN-GEN-002	PNI-NPN shall not use SHNI.

5.2.6 GEOFENCING REQUIREMENTS FOR PRIVATE CBRS / NON-PUBLIC NETWORKS

The support of providing the geofencing information, storage and delivery of the geofencing information, and device based optimizations for Private CBRS / Non-Public Network system camping is optional for both the network and the UE.

The requirement in this section targets the Private CBRS / Non-Public Network (Private LTE or 5G NR SNPN) deployed using CBRS-I. UE requirements for geofencing and TAC collision avoidance is covered in section 5.2.2.

5.2.6.1 PRIVATE CBRS / NON-PUBLIC NETWORK DEPLOYMENT REQUIREMENTS

R5-GEO-DPL-001	The Private CBRS / Non-Public Network may provide the geofence information for the different sites associated with the Private CBRS / Non-Public Network.
R5-GEO-DPL-002	The geofence information shall be GPS based and may also include information based on Radio Footprint.
R5-GEO-DPL-003	When the geofence information is provided, the Private CBRS / Non-Public Network at a mimimum provide the GPS coordinates based fencing for the individual sites associated with the Private CBRS / Non-Public Network. Additionally, the Private CBRS / Non-Public Network may also provide geofence information that can be recognized using the Radio Footprint.
R5-GEO-DPL-004	A given Private CBRS / Non-Public Network may be associated with an explicit identifier. This Private CBRS / Non-Public Network identifier is obtained from - OnGo Alliance by applying for CBRS NID (network identifier) and can be used for both LTE and 5G NR networks - IANA by appling for 3GPP NID (network identifier) and can be used for 5G NR networks.
R5-GEO-DPL-005	The Private CBRS / Non-Public Network service provider may provision the Private CBRS / Non-Public Network service provider identifier in the UE.
R5-GEO-DPL-006	If the Private CBRS / Non-Public Network service provider provisions the Private CBRS / Non-Public Network service provider identifier, then it shall be provisioned as part of the subscription information.

5.2.6.2 GEOFENCING SERVER REQUIREMENTS

R5-GEO-SRV-001	The geofencing provisioning server shall store the geofence information of at least one Private CBRS / Non-Public Networks.
R5-GEO-SRV-002	When the geofence information is stored, the network may associate the geofence information with the UE subscription used to connect to the Private CBRS / Non-Public Network.
R5-GEO-SRV-003	The storage of Private CBRS / Non-Public Network geofence information and the delivery of this information to the UE shall be performed in a secure manner.
R5-GEO-SRV-004	The geofencing server shall deliver the Private CBRS / Non-Public Network geofence information only to UEs that have valid subscriptions to access the Private CBRS / Non-Public Network.
R5-GEO-SRV-005	The geofencing server may provide the Private CBRS / Non-Public Network deployment specific cell broadcast information, in addition to the Private CBRS / Non-Public Network geofence information.
R5-GEO-SRV-006	The geofencing server may provide the eNB ID ranges deployed in an Private CBRS / Non-Public network as part of the geofence information

5.2.7 TAC COLLISION AVOIDANCE PRIVATE CBRS / NON-PUBLIC DEPLOYMENT REQUIREMENTS

This section addresses the TAC collision avoidance requirements.

R5-TAC-DPL-001	The Private CBRS / Non-Public deployed eNB may broadcast the Home eNB name and carry in it the Private CBRS / Non-Public identifier as a text.

APPENDICES (INFORMATIVE)

APPENDIX A: CBRS-PROFILE V AND CBRS-PROFILE XV BASED UE BEHAVIOR

A CBRS-Profile V based UE is a multi-subscription UE. In this example, the CBRS-Profile V based UE behavior is explained using subscription from 2 Operators – Operator 1 and Operator 2. The CBRS-Profile V based UE shall always attach to the Operator 1 network using the Operator 1 subscription and shall always attach to the Operator 2 network using the Operator 2 subscription. The UE is provisioned to prefer the Operator 1 network over the Operator 2 network. Policy that is provisioned in the UE will also ensure that some specific PDN services are always obtained using the Operator 2 subscription/network and the remaining PDN services will be obtained from the Operator 1 network whenever the Operator 1 network is available. When the Operator 1 network is not available, the UE will use the Operator 2 network for all PDN services. CBRS-Profile V based UE can come with both USIM subscriptions or one USIM subscription and another non-USIM (e.g., certificate based).

A.1 CBRS-PROFILE V DESCRIPTION

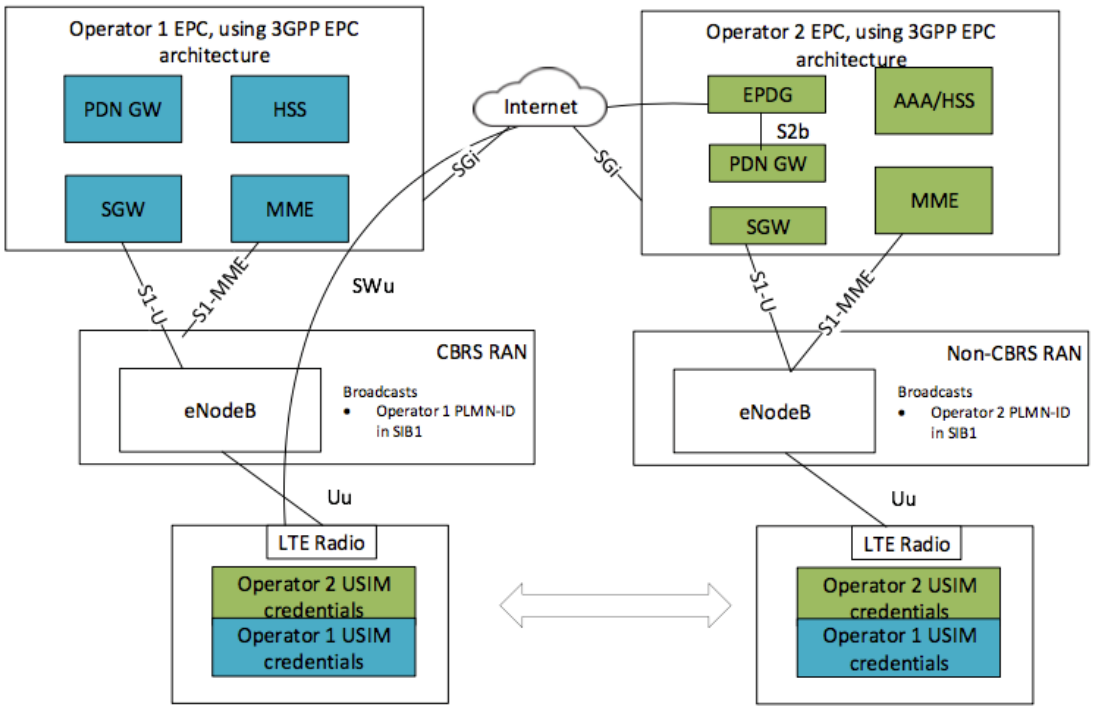

Figure A.1-1: Multi-subscription CBRS-Profile V Based UE example (Dual USIM Case)

In Figure A.1-1 above, the UE has a USIM subscription with Operator 1 and with Operator 2.

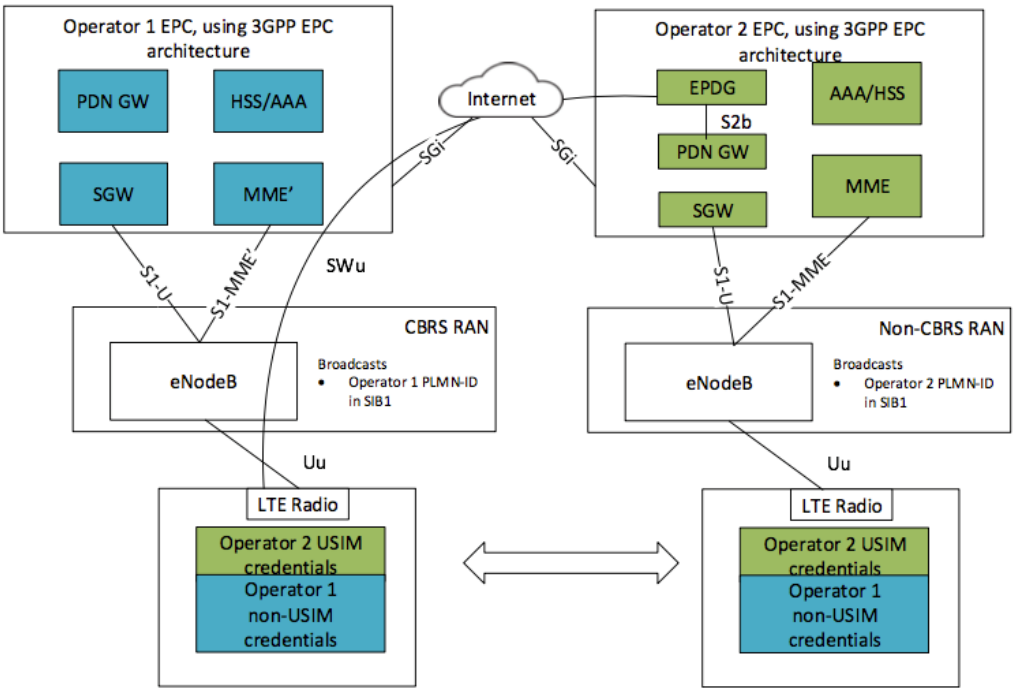

Figure A.1-2: Multi-subscription CBRS-Profile V based UE example (USIM and non-USIM Subscription Case)

In Figure A.1-2 above, the UE has non-USIM subscription with Operator 1 and USIM subscription with Operator 2.

The behavior of the UE inside, outside and during transition to a CBRS network are as follows.

- While registered as an Operator 1 subscriber in a CBRS network:
  - The UE may access the CBRS network operating in 3GPP Access Mode (EPS-AKA) or 3GPP-based Access Mode (non-EPS AKA) based on the Operator 1 subscription.
  - All services that are mapped to use the Operator 1 subscription are obtained using the CBRS network (using the Operator 1 subscription) while in the Operator 1 CBRS network.
  - In order to obtain services that are mapped to use the Operator 2 subscription and the Operator 2 network, the UE shall establish an SWu tunnel with the ePDG of Operator 2. The SWu tunnel will be established by UE via the Operator 1 CBRS network to which it is attached.
    - Example: The CBRS-Profile V based UE may use the Operator 1 CBRS network access (obtained using the Operator 1 subscription) to obtain voice services using the Operator 2 subscription over S2b via Operator 2's ePDG (LTE Calling).
- While outside Operator 1 coverage but within the Operator 2 network coverage:
  - The UE uses the Operator 2 network and the Operator 2 subscription for all PDN connections.

- The UE scans in the background for availability of the Operator 1 network, except when in an active voice call on the Operator 2 network.
- If a CBRS network is detected with the Operator 1 PLMN-ID, non-voice PDN connections are moved to the Operator 1 CBRS network, while the UE continues voice on the Operator 2 network using the Operator 2 subscription over S2b via Operator 2's ePDG.

A.2 CBRS-PROFILE XV DESCRIPTION

This section describes the CBRS-Profile XV with the UE operating with single Tx radio which is NR or LTE. The UE multiple subscriptions with at least one is a NR credential. There three scenarios that are described:

- LTE CBRS connection into EPC as Operator 1 and NR non-CBRS connection via untrusted network connection into 5GC as Operator 2. This is illustrated in Figure A.2-3.
- NR CBRS connection into 5GC as Operator 1 and NR non-CBRS connection via untrusted network connection into 5GC as Operator 2. This is illustrated in Figure A.2-2.
- NR CBRS connection into 5GC as Operator 1 and NR non-CBRS connection via untrusted network connection into EPC as Operator 2. This is illustrated in Figure A.2-1.

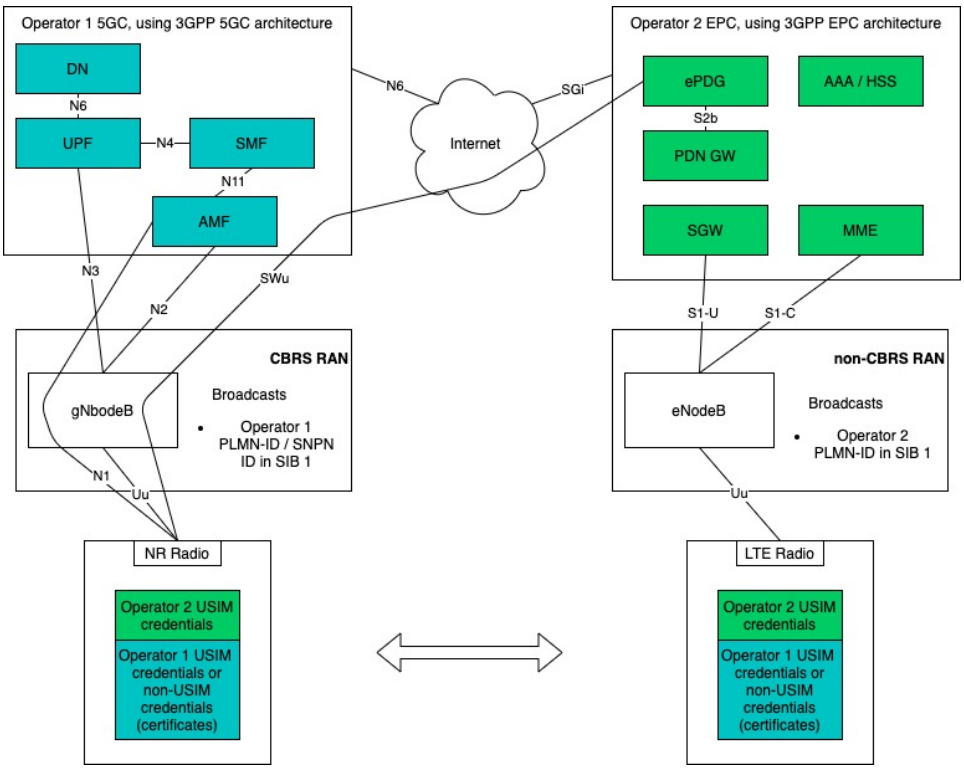

Figure A.2-1: Multi-subscription CBRS-Profile XV Based UE example (NR CBRS and LTE non-CBRS)

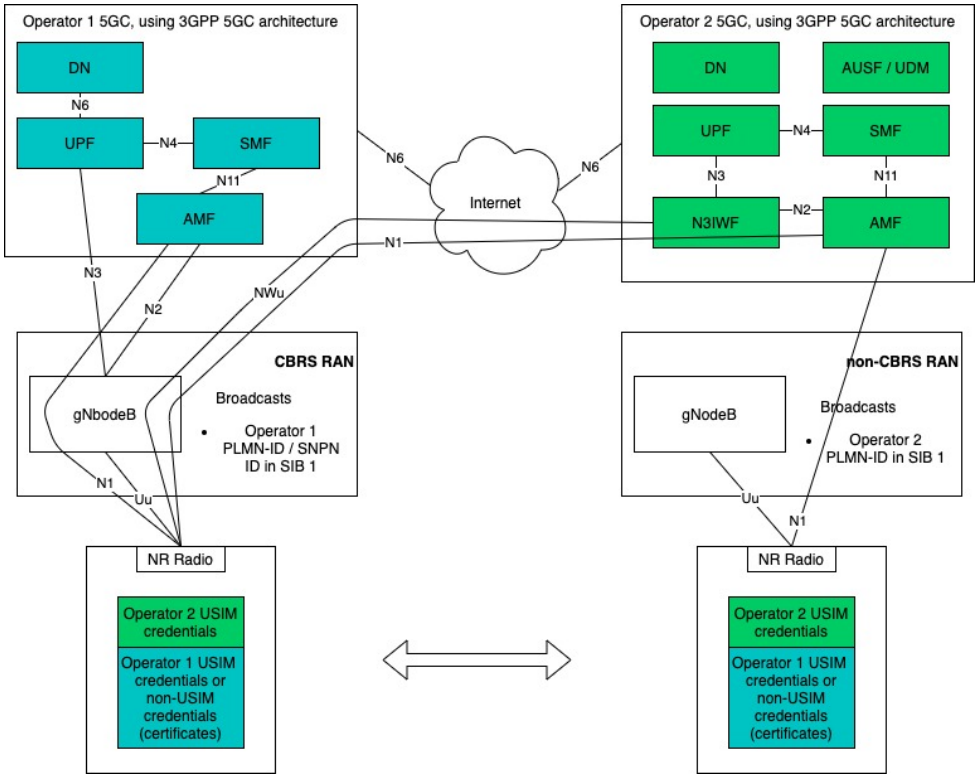

Figure A.2-2: Multi-subscription CBRS-Profile XV Based UE example (NR CBRS and NR non-CBRS)

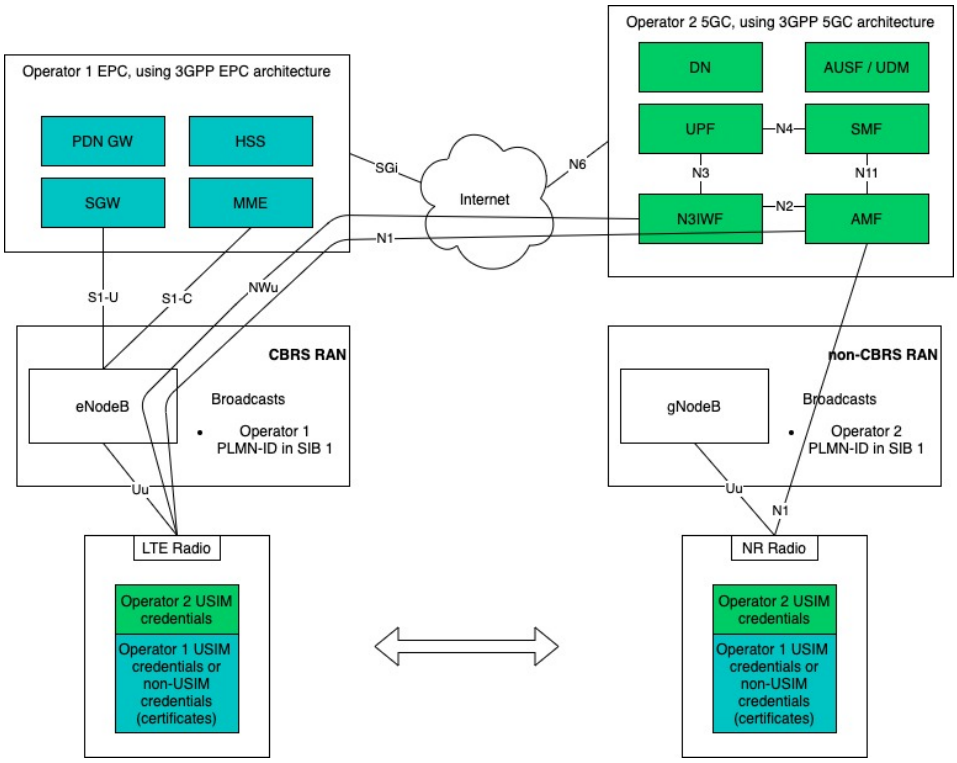

Figure A.2-3: Multi-subscription CBRS-Profile XV Based UE example (LTE CBRS and NR non-CBRS)

In Figure A.2-1, Figure A.2-2, and Figure A.2-3 above, the UE has a USIM subscription or a non-USIM (certificate based) subscription with Operator 1 and USIM subscription with Operator 2.

The behavior of the UE inside, outside and during transition to a CBRS network are as follows.

- While registered as an Operator 1 subscriber in a CBRS network:
  - The UE may access the CBRS network operating in 3GPP Access Mode (EPS-AKA) or 3GPP-based Access Mode (non-EPS AKA) based on the Operator 1 subscription.
  - All services that are mapped to use the Operator 1 subscription are obtained using the CBRS network (using the Operator 1 subscription) while in the Operator 1 CBRS network.
  - In order to obtain services that are mapped to use the Operator 2 subscription and the Operator 2 network, the UE shall establish an SWu tunnel with the ePDG when connecting to EPC or establish a NWu tunnel with N3IWF when connecting with 5GC of Operator 2. The SWu tunnel / NWu will be established by UE via the Operator 1 CBRS network to which it is attached.
    - Example: The CBRS-Profile XV based UE may use the Operator 1 CBRS network access (obtained using the Operator 1 subscription) to obtain voice services using the Operator 2 subscription over S2b via Operator 2's ePDG (LTE Calling) with EPC or

with 5GC use N2/ N3 interfaces and the UE talks to the AMF via the N1 interface connecting through the N3IWF[2].

- While outside Operator 1 coverage but within the Operator 2 network coverage:
  - The UE uses the Operator 2 network and the Operator 2 subscription for all PDN (EPC) / PDU (5GC) connections.
  - The UE scans in the background for availability of the Operator 1 network, except when in an active voice call on the Operator 2 network.
  - If a CBRS network is detected with the Operator 1 PLMN-ID, non-voice PDN connections are moved to the Operator 1 CBRS network, while the UE continues voice on the Operator 2 network using the Operator 2 subscription over S2b via Operator 2's ePDG with EPC and N2 / N3 interface with 5GC with the UE employing N1 interface to talk to the AMF via the N3IWF.

[2] While the N3IWF looks functionally similar to the ePDG, a key difference between these approaches is that, unlike the ePDG which has been considered a core network element, the N3IWF is a peer of the 5G New Radio gNB and implements the N2 and N3 interfaces used to integrate the 5G Access Network to the 5GCN's Control Plane and User-Plane elements respectively. The UE talks to the AMF via the N3IWF tunnel using the N1 interface.

APPENDIX B: SHNI AND IMSI BLOCK

The Home Network Identifier (HNI) is part of the International Mobile Subscriber Identity (IMSI) and consists two fields: Mobile Country Code (MCC) and Mobile Network Code (MNC). The HNI represents an identification for the Public Land Mobile Network (PLMN) in a mobile network and therefore represents the identity of the Home Subscriber Subsystem (HSS) administering a subscription. The IMSI identifies the subscription corresponding to a UE and comprises the HNI (also known as the PLMN ID) and Mobile Subscriber Identity Number (MSIN). HNIs are assigned by an IMSI Administrator to qualifying mobile networks on the basis of their standing and eligibility to operate a mobile telecommunications network as defined in CBRSA-TR-0100 [16].

The Alliance of Telecommunications Industry Solutions (ATIS)' IMSI Oversight Council (IOC) has set up guidelines for the IMSI Administrator to assign the HNI to IOC-approved Radio Technologies using the shared CBRS spectrum. These guidelines depart from the normal procedures used to determine eligibility of an operator to create unique and valid IMSIs for their subscribers by designating at least one SHNI for use by shared spectrum users who are not already in possession of their own HNIs. The ATIS IOC guidelines divide the MSIN into 2 parts – a 4-digit IMSI Block Number (IBN) and 5-digit User Identification Number (UIN). This partition of MSIN will allow for 10,000 Blocks of 100,000 unique IMSIs within a SHNI defined in IMSI Guideline [15].

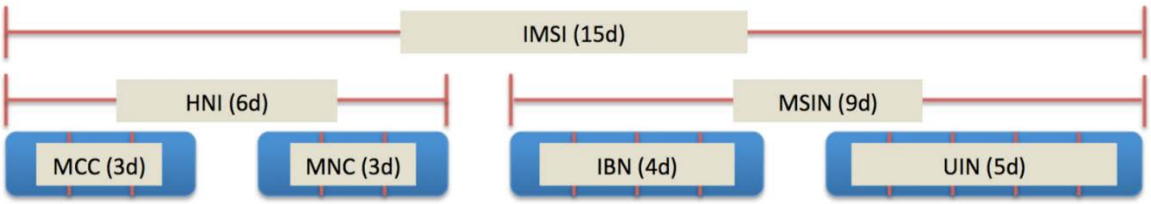

Figure B-1: The SHNI used in CBRS creates a need to route IMSIs to networks;

IMSI Allocation

The ATIS IOC has published IMSI guidelines [15] that provides the details on how the IMSI blocks can be procured by CBRS Network Operators. The flow diagram gives a brief overview of the process.

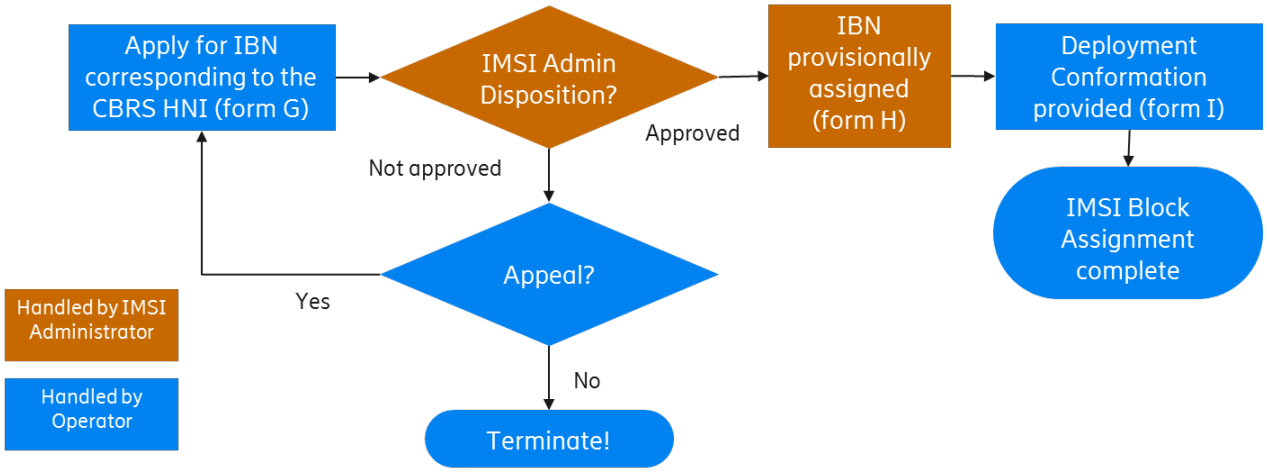

Figure B-2: A flow diagram detailing the IMSI Administrator's role in assigning IBNs for use by CBRS operators who do not possess their own HNI

APPENDIX C: REQUIREMENTS MAPPING - OLD VS NEW

In release 3, a numbering format for all requirements in this Technical Specifications was defined. As a result of this, all requirement numbers were updated. This section provides the mapping of old requirement to the new requirement.

C.1 REQUIREMENT NUMBERING FORMAT

Format => Rx-ABC-DEF-nnn, where

- x: defines the release number
  - 1 – for Release 1
  - 2 – for Release 2
  - 3 – for Release 3
  - etc.

- ABC: defines the use case or feature/functioanlity
  - "SPN" for Service Provider Use Case
  - "NHN", for Neutral Host Network Use Case
  - "PRV", for Private Network Use Case
  - "MSO", for MSO Use case
  - "FWN", for Fixed Wireless Network Use Case
  - "5NR", for 5G NR Use Case
  - "UEP", for UE Profile
  - "TLB" for Traffic Local Breakout
  - "ROM", for Roaming Functionality
  - "XAU" for extended Authentication

- DEF: defines the sub-feature classification
  - "IMS", for IMS
  - "DAT", for DATA
  - "SEC", for Security
  - "DIS", for Discovery
  - "RSH", for RAN Sharing
  - "MES", for Measurement
  - "GEN", for General or Generic Functionality
  - "ARC", for Architecture
  - "SVC", for Service

- nnn: a three digit number defining the requirement in the same category starting from 001

C.2 REQUIREMENT MAPPING

Table C.2-1: Requirement Mapping

OLD Requirement #	Release	New Requirement #

RAN-Share-001	Release 1	R1-NHN-RSH-001
RAN-Share-002	Release 1	R1-NHN-RSH-002
RAN-Share-003	Release 1	R1-NHN-RSH-003
RAN-Meas-001	Release 1	R1-NHN-MES-001
RAN-Meas-002	Release 1	R1-NHN-MES-002
RAN-Meas-003	Release 1	R1-NHN-MES-003
RAN-Meas-004	Release 1	R1-NHN-MES-004
RAN-Meas-005	Release 1	R1-NHN-MES-005
RAN-Meas-006	Release 1	R1-NHN-MES-006
RAN-Meas-007	Release 1	R1-NHN-MES-007
RAN-Meas-008	Release 1	R1-NHN-MES-008
RAN-Disc-001	Release 1	R1-NHN-DIS-001
RAN-Mob-001	Release 1	R1-NHN-MOB-001
RAN-Mob-002	Release 1	R1-NHN-MOB-002
Security-001	Release 1	R1-NHN-SEC-001
Security-002	Release 1	R1-NHN-SEC-002
Security-003	Release 1	R1-NHN-SEC-003
AUTH-001	Release 1	R1-NHN-AUT-001
AUTH-002	Release 1	R1-NHN-AUT-002
AUTH-003	Release 1	R1-NHN-AUT-003
AUTH-004	Release 1	R1-NHN-AUT-004
AUTH-005	Release 1	R1-NHN-AUT-005
RAN-Share-004	Release 2	R2-NHN-RSH-004
RAN-Share-005	Release 2	R2-NHN-RSH-005
RAN-Share-006	Release 2	R2-NHN-RSH-006
RAN-Share-007	Release 2	R2-NHN-RSH-007
MSO-RAN-001	Release 2	R2-MSO-RAN-001
UE-001	Release 2	R2-UEP-GEN-001
UE-002	Release 2	R2-UEP-GEN-002
UE-003	Release 2	R2-UEP-GEN-003
UE-004	Release 2	R2-UEP-GEN-004
UE-005	Release 2	R2-UEP-GEN-005
UE-006	Release 2	R2-UEP-GEN-006
UE-007	Release 2	R2-UEP-GEN-007
UE-008	Release 2	R2-UEP-GEN-008
UE-009	Release 2	R2-UEP-GEN-009
UE-010	Release 2	R2-UEP-GEN-010
UE-011	Release 2	R2-UEP-GEN-011
UE-012	Release 2	R2-UEP-GEN-012
UE-013	Release 2	R2-UEP-GEN-013

UE-014	Release 2	R2-UEP-GEN-014
UE-015	Release 2	R2-UEP-GEN-015
UE-016	Release 2	R2-UEP-GEN-016
UE-017	Release 2	R2-UEP-GEN-017
UE-018	Release 2	R2-UEP-GEN-018
UE-019	Release 2	R2-UEP-GEN-019
FWN-ARCH-001	Release 2	R2-FWN-ARC-001
FWN-ARCH-002	Release 2	R2-FWN-ARC-002
FWN-ARCH-003	Release 2	R2-FWN-ARC-003
FWN-ARCH-004	Release 2	R2-FWN-ARC-004
FWN-SERV-001	Release 2	R2-FWN-SVC-001
FWN-SERV-002	Release 2	R2-FWN-SVC-002
FWN-SERV-003	Release 2	R2-FWN-SVC-003
NEPS-GEN-001	Release 2	R2-XAU-GEN-001
NEPS-GEN-002	Release 2	R2-XAU-GEN-002
NEPS-AUTH-001	Release 2	R2-XAU-AUT-001
NEPS-AUTH-002	Release 2	R2-XAU-AUT-002
NEPS-AUTH-003	Release 2	R2-XAU-AUT-003
LBO-ARCH-001	Release 3	R3-TLB-ARC-001
LBO-ARCH-002	Release 3	R3-TLB-ARC-002
LBO-ARCH-003	Release 3	R3-TLB-ARC-003
SR-ROAM-001	Release 3	R3-ROM-DAT-001
SR-ROAM-002	Release 3	R3-ROM-DAT-002
SR-ROAM-003	Release 3	R3-ROM-DAT-003
SR-ROAM-004	Release 3	R3-ROM-DAT-004
SR-ROAM-005	Release 3	R3-ROM-DAT-005
IMS-ROAM-001	Release 3	R3-ROM-IMS-001
IMS-ROAM-002	Release 3	R3-ROM-IMS-002

APPENDIX D: UE DUAL SIM CONFIGURATIONS

Single credential devices are viable for deployment of private CBRS Networks based on connectivity needs, and the more prevail need of ubiquitous connectivity is addressed through devices with the dual subscription capabilities or dual SIM configurations, for example, as described in section 4.2.3.2. This section is an informative appendix providing some information of UEs with dual SIM configuration and some aspects in relation to CBRS UE Profiles.

A UE with dual SIM configuration has two SIM credentials. As per GSMA TS.37 [28], these credentials can be stored in following combinations of physical SIM (pSIM) and eUICC (removable or embedded):

- pSIM + pSIM
- pSIM + eUICC
- eUICC + eUICC

GSMA TS.37 [28] defines following four dual SIM UE operational modes :

- Dual SIM Single Standby (DSSS) or Passive Dual SIM
- Dual SIM Dual Standby (DSDS)
- Dual SIM Dual IMS, or Dual SIM, Dual VoLTE (DSDI, or DSDV)
- Dual SIM Dual Active (DSDA)

Based on UE's dual-SIM operational mode (i.e., DSDS, DSDI, DSDA), a given UE can operate by monitoring both networks. The UE can be in RRC states of IDLE / INACTIVE (only for NR) in both networks or CONNECTED for one network and IDLE / INACTIVE (only for NR) on the other or CONNECTED on both networks.

The preferences for operation are controlled by using a device configuration on the two networks providing relative preferences for different services.

GSMA might also extend to Multi SIM Multi Standby (MSMS) and Multi SIM Multi Active (MSMA) and some possibly derivatives of these configurations in the future.

CBRS UE profiles in section 4.3.1 define UE capabilities in terms of the number of subscriptions the UE maintains at any given time, status of each of those subscriptions, and the associated functionality enabled on these devices. GSMA TS.37 [xx] defines radio capabilities with requirements related to functional realizations to support different services for devices with dual SIM configurations. Each device with GSMA dual SIM configurations can operate based on one or more CBRS UE profiles.

Table D.1 depicts a mapping to show which CBRS Profiles can be realized or implemented based on the capabilities of given GSMA Dual SIM operation mode on a device.

Note that the mapping in Table D.1 is informative. The implementation by UE/Device vendors will need to follow the relevant CBRS UE Profile requirements that are specified in the normative sections of this specification, TS-1002 [10] and TS-1003 [12].

Table D-1: CBRS UE Profiles Implemented on Specific GSMA Dual SIM Operational Mode.

GSMA Dual SIM Operational Mode	**CBRS UE Profile**
DSSS	I, I-A, XI, XI-A, II
DSDS	I, I-A, XI, XI-A, II, III, XIII, V, XV
DSDI	I, I-A, XI, XI-A, II, III, XIII, V, XV
DSDA	I, I-A, XI, XI-A, II, IV, XIV

APPENDIX E: CHANGE HISTORY

Table E-1: Change History

VERSION	DATE (dd-mm-yyyy)	DESCRIPTION
V1.0.0	01-02- 2018	Release 1 of this Specification
V1.0.0 Rev 1	08-02-2018	Beginning of work for Release 2 Implemented NSTG-18-004
V1.0.0 Rev 2	26-02-2018	Beginning of work for Release 2 Implemented NSTG-18-004-r4
V1.0.0 Rev 3	02-04-2018	Implemented NSTG-18-031-r0 (Move UE Types to TS-1001) Corrected implementation of NSTG-18-017. Implemented NSTG-18-023 rev 4 (UE requirements)
V1.0.0 Rev 3.1	04-04-2018	Draft text for categories of 3GPP Access Mode
V1.0.0 Rev 3.2	09-04-2018	Implemented NSTG-18-039 (FWA requirements)
V1.0.0 Rev 3.3	17-04-2018	Implemented 3GPP Access Mode terminology agreed at the NSTG meeting on 2018-04-16.
V1.0.0 Rev 4.0	24-04-2018	Changes agreed on-screen during the meeting on 2018-04-23.
V1.0.0 Rev 5.0	08-05-2018	Implemented NSTG-18-056_r2(NSTG-18-051)_2018.05.08_Ruckus Networks_Technical_3GPP-Based Access Mode (non-USIM) Stage 1
V1.0.0 Rev 6.0	14-05-2018	Implemented NSTG-18-063_r2(NSTG-18-057)_2018.05.21_Ruckus Networks_Technical_UE Enhancements for 3GPP-Based Access Mode (non-EPS-AKA) TS Stage 1
V1.0.0 Rev 7.0	11-06-2018	Implemented NSTG-18-066_r1_2018.06.04_Ruckus Networks_Technical_UE Types Modifications to TS Stage 1. This CR updates Section 3.3
V1.0.0 Rev 8.0	11-06-2018	- Implemented NSTG-18-071_r1(NSTG-18-067)_2018.06.11_Ruckus Networks_Technical_Additional NHN Architecture Options for Stage 1 TS. - Section 3.3 moved as section 5 - Updates to Section 3 & section 4.3

V1.0.0 Rev 9.0	11-07-2018	- Incorporated accepted comments from Meeting held on 9 Jul 2018 (Ref -> NSTG-18-083_r1 (NSTG-18-081)_2018.07.09_Chair_TG_TS-1001 Comments) - Incorporated all "Editorial" comments from Ballot Review (Ref -> NSTG-18-085_r2 (NSTG-18-083)_2018.07.11_TS_Editor_TG_TS-1001 Comments)
V1.0.0 Rev 10.0	24-07-2018	- Incorporated accepted comments from Meeting held on 24 Jul 2018 (Ref -> NSTG-18-092_r3 (NSTG-18-081)_2018.07.24_Chair_TG_TS-1001 Comments.docx)
V1.0.0 Rev 11.0	22-08-2018	- Incorporated CR approved in meeting held on 20 Aug 2018 - NSTG-18-113_r1_2018.08.11_Ruckus Networks - Comcast - Charter - Federated - Nokia - Extenet_Technical_UE Profiles Enhancements.docx
V1.0.0 Rev 12.0	23-09-2018	- Incorporated accepted comments from NSTG-18-097_r8 (NSTG-18-081)_2018.07.27_Chair_TG_TS-1001 Comments.docx - Incorporated NSTG-18-108_r0_2018.08.06_American Tower_Technical_TS1001 Section4.6 Fixed Wireless Networks.docx
V1.0.0 Rev 13.0	01-10-2018	- Implemented "accepted" comments as in NSTG-18-097_r9 (NSTG-18-081)_2018.07.27_Chair_TG_TS-1001 Comments.docx - Implemented NSTG-18-125_r1_2018.09.26_Ericsson_Technical_Shared_HNI_AppB.docx
V1.0.0 Rev 14.0	03-10-2018	- Editorial modifications done throughout the document to enhance readability.
V2.0.0	16-04-2019	- Published version for Release 2.0
V2.0.0 Rev 1.0	30-08-2019	- Editorial modifications o Update document per new OnGo template o Improve readability - Incorporated CRs o NSTG-19-080_r0_2019.07.23_Ruckus Wireless_Technical_TS1 New Template.docx o NSTG-19-038_r6_2019.04.08_Athonet_Technical_CR for TS 1001 on LBO.docx

		o NSTG-19-049_r2_2019.05.01_Ruckus Wireless_Technical_Stage 1 Roaming Requirements.docx
V2.0.0 Rev 2.0	15-10-2019	- Incorporated CRs o NSTG-19-108_r1_2019.10.07_Athonet_Technical_IMS roaming.docx o NSTG-19-111_r3_2019.10.15_Ruckus_Technical_Roaming Text.docx
V2.0.0 Rev 3.0	03-12-2019	- Release 3 Ballot Review comments incorporated per NSTG-19-128_r1_(NSTG-19-120)_2019.12.09_Chair_TG_Comments for TS-1001 Rel 3.docx
V2.0.0 Rev 4.0	16-12-2019	- Release 3 Ballot Review comments: NSTG-19-120_r0_2019.11.18_Chair_TG_Comments for TS-1001 Rel 3_Rev 6.docx - NSTG-19-134_r0_2019.12.16_Ruckus_Technical_NHN Roaming Text for TS1
V3.0.0	18-02-2020	- Published version of Release 3 specification.
V3.0.0 Rev 1.0	19-08-2020	- NSTG-20-067_r1_2020.07.20_Nokia_Technical_CR_SNPN_PNI-NPN_CBRSA-TS-1001_Rel-4.docx
V3.0.0 Rev 2.0	15-10-2020	- NSTG-20-087_r1_2020.09.14_Ruckus_Technical_TS1 modifications for 5G NR SA.docx
V3.0.0 Rev 3.0	19-10-2020	- NSTG-20-081_r2_2020.08.31_CableLabs_Technical_CR_5GC_CBRSA-TS-1001_Rel-4.docx - NSTG-20-099_r0_2020.10.19_Celona_Technical_UE Profiles in TS-1001.docx
V3.0.0 Rev 4.0	14-12-2020	- NSTG-20-114_r0_2020.11.30_Chair_TG_Comments TS-1001 Rel4 - V5.docx
V4.0.0 Rev 1.0	17-02-2021	- NSTG-20-113_r3_2020.11.22_Celona_Technical_NR SA UE requirements in TS-1001 – Approved.docx - NSTG-20-104_r7_2020.10.26_Celona_Technical_NR SA UE Profiles in TS-1001 R8 – Approved.docx
V4.0.0 Rev 2.0	30-03-2021	- Added Appendix D mapping CBRS UE Profiles and GSMA Dual SIM Configurations

V4.0.0 Rev 3.0	07-05-2021	- NSTG-21-048_r2_2021.05.03_Chair_TG_TS-1001 Ballot.docx
V4.0.0 Rev4.0	10-05-2021	- Editorial modifications during the meeting.
V4.1.0 Rev1.0	28-10-2021	- Rev 8 of NSTG-21-076_r0_2021.08.09_Celona_Technical_Geofencing and TAC collision avoidance requirem.docx
V4.1.0 Rev2.0	01-11-2021	- Minor modifications to revision history - Added the Rev number of the approved CR. - Added abbreviation of MDT.
V4.1.0 Rev3.0	21-12-2021	- Release 5 Ballot Comment resolution. Ref: NSTG-21-121_r1_2021.12.13_Chair_TG_TS-1001 Ballot.docx
V4.1.0 Rev4.0	10-01-2022	- NSTG-21-115_r2_2021.12.15_CommScope_Technical_R15 NR Private Networks.docx
V4.1.0 Rev5.0	18-01-2022	- Editorial Change in Appendix C.1