CBRS Network Service Technical Specifications

CBRSA-TS-1002

V1.0.0

February 1, 2018

LEGAL DISCLAIMERS AND NOTICES

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. 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.

CBRS Alliance
3855 SW 153rd Drive
Beaverton, OR 97003
www.cbrsalliance.org
info@cbrsalliance.org

Table of Contents

CBRS Alliance

3855 SW 153rd Drive

Beaverton, OR 97003

www.cbrsalliance.org

info@cbrsalliance.org

CBRS Alliance
3855 SW 153rd Drive
Beaverton, OR 97003
www.cbrsalliance.org
info@cbrsalliance.org

LIST OF FIGURES

LIST OF TABLES

CBRS Alliance
3855 SW 153rd Drive
Beaverton, OR 97003
www.cbrsalliance.org
info@cbrsalliance.org

1 Scope

This specification provides the stage 2 and stage 3 aspects of Neutral Host Networks and Private Networks used in the CBRS band (3550-3700 MHz).

This specification is based on Release 1 of the Stage 2 and Stage 3 MulteFire Alliance specifications (e.g., MFA TS MF.202 [2], MFA TS 36.413 [9], MFA TS 24.301 [10]) and on 3GPP Release 14 specifications.

2 References

[1] Third Generation Partnership Project (3GPP). *Vocabulary for 3GPP Specifications,* 3GPP TR 21.905, http://www.3gpp.org/.

[2] MulteFire Alliance (MFA), Architecture for Neutral Host Network Access Mode Stage 2 (Release 1), MFA TS MF.202, https://www.multefire.org/, Release 1.0.

[3] 3GPP TS 36.331, "*Evolved Universal Terrestrial Radio Access (E-UTRA*); Radio Resource Control (RRC); Protocol specification", Release 14.

[4] 3GPP TS 23.402, "Architecture enhancements for non-3GPP accesses", http://www.3gpp.org/, Release 14.

[5] 3GPP TS 24.301, "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS)", http://www.3gpp.org/, Release 14.

[6] 3GPP TS 32.426, "Telecommunication management; Performance Management (PM); Performance measurements Evolved Packet Core (EPC) network", http://www.3gpp.org/, Release 14

[7] 3GPP TS 32.432, "Performance measurement: File format definition", http://www.3gpp.org/, Release 14.

[8] 3GPP TS 32.455, "Telecommunication management; Key Performance Indicators (KPI) for the Evolved Packet Core (EPC); Definitions", http://www.3gpp.org/, Release 14.

[9] MulteFire Alliance (MFA), Architecture for Neutral Host Network Access Mode Stage 2 (Release 1), MFA TS 36.413, https://www.multefire.org/, Release 1.0.

[10] MulteFire Alliance (MFA), Architecture for Neutral Host Network Access Mode Stage 2 (Release 1), MFA TS 24.301, https://www.multefire.org/, Release 1.0.

[11] 3GPP TS 36.413, "Evolved Universal Terrestrial Radio Access Network (E-UTRAN); S1 Application Protocol (S1AP)", http://www.3gpp.org/, Release 14.

[12] 3GPP TS 33.401, "3GPP System Architecture Evolution (SAE); Security architecture", http://www.3gpp.org/, Release 14.

[13] MulteFire Alliance (MFA), Architecture for Neutral Host Network Access Mode Stage 2 (Release 1), MFA TS 33.401, https://www.multefire.org/, Release 1.0.

[14] 3GPP TS 23.401, "3GPP System Architecture Evolution (SAE); Security architecture", http://www.3gpp.org/, Release 14.

[15] CBRSA-TS-1001-V1.0.0, "CBRS Network Services Requirements", October 2017.

[16] 3GPP TS 23.003, "Numbering, addressing and identification", http://www.3gpp.org/, Release 14.

[17] 3GPP TS 36.300, "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2", http://www.3gpp.org/, Release 14.

3 Abbreviations and Definitions

3.1 Abbreviations

AAA	Authentication, authorization and accounting
CBRS	Citizens Broadband Radio Service
CBRS-I	CBRS Identifier
CBRS-NID	CBRS Network Identifier
CBRSA	CBRS Alliance
CSG	Closed Subscriber Group
EMM	EPS Mobility Management
EPC	Evolved Packet Core
EPS	Evolved Packet System
ESM	EPS Session Management
GTP	GPRS Tunneling Protocol
GUTI	Globally Unique Temporary Identifier
IMSI	International Mobile Subscriber Identity
MF	MulteFire
MFA	MulteFire Alliance
MME	Mobility Management Entity
MNO	Mobile Network Operator
MSO	Multiple System Operator
NH	Neutral Host
NHN	Neutral Host Network
OID	Organization Identifier
PDN	Packet Data Network

PLMN	Public Land Mobile Network
PSP	Participating Service Provider
PSP-ID	PSP Identifier
RAN	Radio Access Network
SIM	Subscriber Identity Module
TAU	Tracking Area Update
UE	User Equipment
UICC	Universal Integrated Circuit Card
USIM	Universal Subscriber Identity Module

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.

Neutral Host Network A network deployed and operated by an NH operator, who may also be an independent entity, a MNO or a MSO, where the network resources are being shared by multiple wireless 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.

4 Void

5 Stage 2 Aspects

5.1 General

The stage 2 aspects cover both CBRS deployments based on NHN Access Mode and CBRS deployments based on 3GPP Access Mode. The corresponding key stage 2 baseline specifications are:

- MulteFire Alliance Technical Specification MFA TS MF.202 [2] and
- 3GPP Technical Specification 3GPP TS 23.401 [14]).

The modifications compared with [2] and [14] are described in this document.

5.2 Architecture Reference Model

Reference model for network architecture is depicted in Figures 5-1 through 5-5. The network elements and reference points associated with NHN EPC architecture are as in clause 5 of MFA TS MF.202 [2]. The network elements and reference points associated with 3GPP EPC architecture are as in 3GPP TS 23.401 [14].

The interface shown as "AAA" in [2] is named "cbAAA" in this specification. It provides the functions necessary for authentication and authorization between the NHN Core and the non-3GPP AAA.

Some highlights of the architecture are discussed below:

- The architecture enables deploying:
    - CBRS RAN operating in 3GPP Access Mode to serve PLMN CBRS devices that are equipped with a USIM based subscription;
    - Private CBRS network (RAN+Core) operating in 3GPP Access Mode to serve CBRS devices that are equipped with a USIM based subscription associated with a Private CBRS network;
    - CBRS NHN (RAN+Core) operating in NHN Access Mode to serve NHN-capable CBRS devices that are equipped with a USIM based subscription associated with a Participating Service Provider(s);
    - Private CBRS network (RAN + Core) operating in NHN Access Mode to serve NHN-capable CBRS devices that are equipped with a USIM based subscription or a certificate based subscription associated with a Participating Service Provider (PSP).

- The architecture also enables the use of a common shared CBRS RAN which serves a NHN Access Mode core network or/and multiple 3GPP Access Mode core networks.

- The architecture enables the CBRS NHN to operate as a trusted non-3GPP Access Network and/or untrusted non-3GPP Access Network for UEs associated with PSPs.
    - In trusted mode, a CBRS NHN uses the STa-N interface (as defined in MFA TS MF.202 [2]) for UE authentication and enables one or more simultaneous home routed PDN connections between the UE and the PSP's PDN-GW using the S2a interface. If the subscriber's home operator allows, the CBRS NHN may provide additional PDN connections for local breakout of data traffic. Legal Intercept is not specified for local breakout.
    - In untrusted mode, a CBRS NHN uses the SWa-N interface (as defined in MFA TS MF.202 [2]) for UE authentication. In this mode, all PDN connections use local breakout of data traffic. Legal Intercept is not specified in the untrusted case.
        - In untrusted mode, a UE with a USIM based subscription can establish a secure IPsec tunnel (i.e., SWu discussed in 3GPP TS 23.402 [4]) with its service provider's ePDG using the subscription and receive the service provider's services via the SWu interface.

- The architecture enables NHN Access Mode authentication using local or remote AAA servers depending on which AAA server the UE credentials are associated with.

- In 3GPP Access Mode, 3GPP EPS defined procedures using the S6a interface shall be used for authenticating the UE credential. In this mode, only USIM based credentials are supported.

Note: The architecture has no impact on the support of the traditional roaming between SPs.

5.2.1 Network Architecture – Use of CBRS RAN with non-CBRS-I PLMN-ID

Figure 5-1 shows the architecture for a CBRS network with a standard 3GPP EPC using a non-CBRS-I PLMN-ID and with the CBRS-RAN using the CBRS band. The UE is accessing the network using 3GPP Access Mode. This network architecture may be used for both Public Networks and Private Networks.

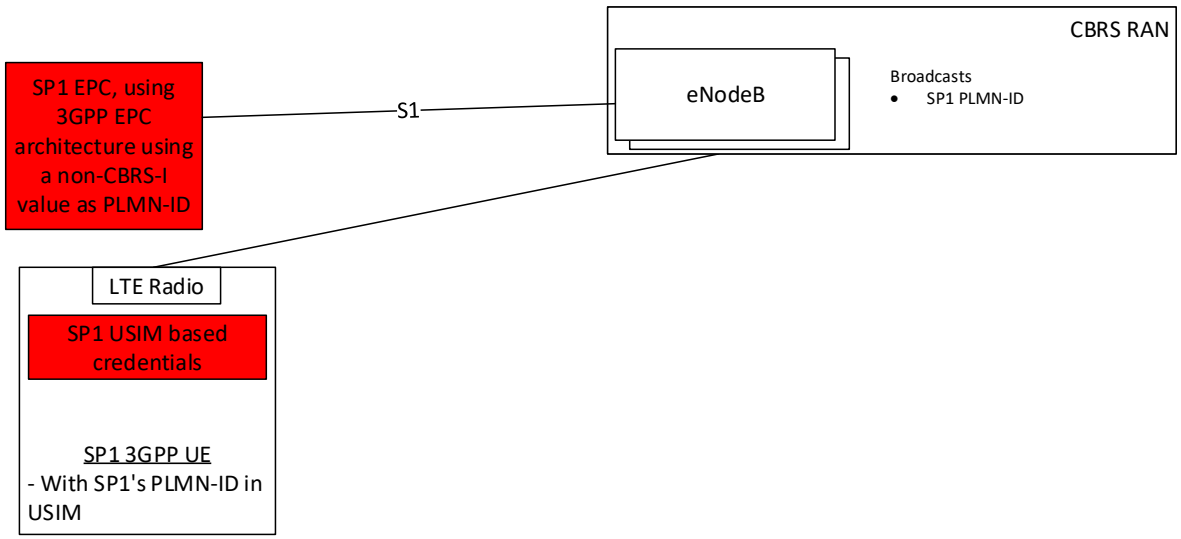

Figure 5-1 Network Architecture – Use of CBRS band and a non-CBRS-I PLMN-ID

5.2.2 Network Architecture – Private Network using CBRS-I and CBRS-NID

Figure 5-2 shows the architecture for a CBRS network with a standard 3GPP EPC using a CBRS-I value and a CBRS-NID. The UE is accessing the network using 3GPP Access Mode.

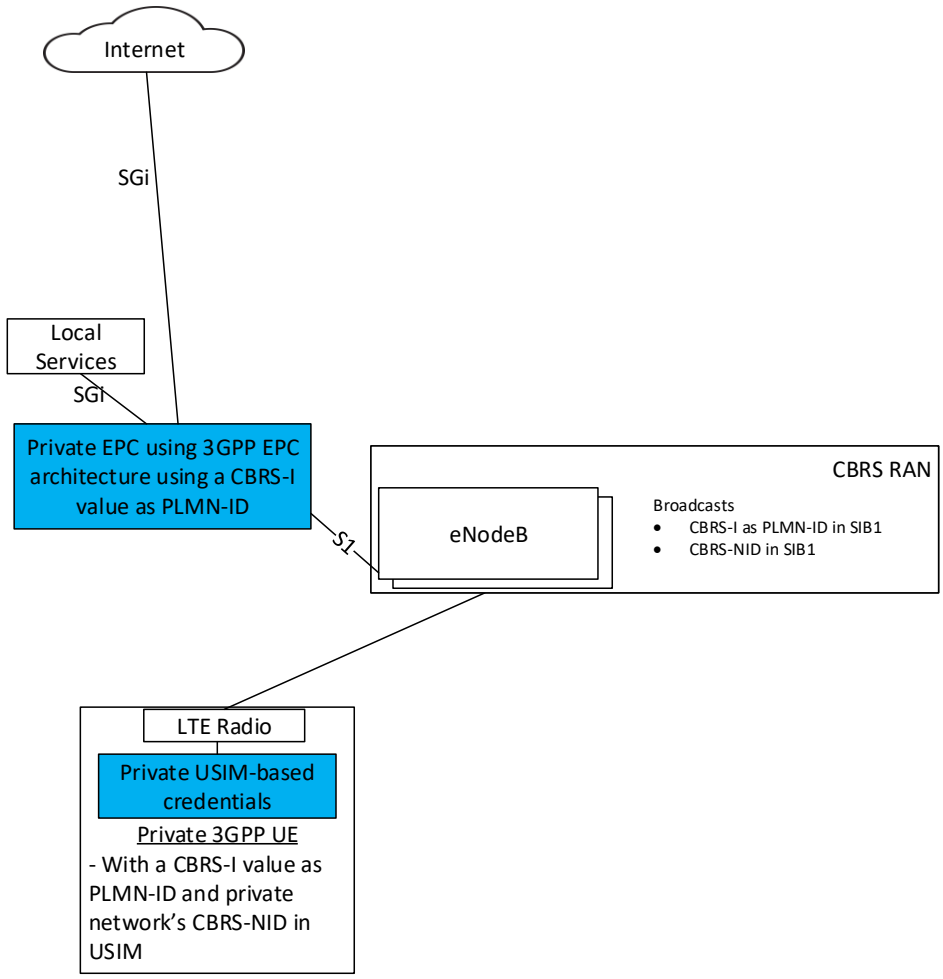

Figure 5-2 Network Architecture – Private Network using a CBRS-I value as PLMN-ID and CBRS-NID

5.2.3 Network Architecture – Neutral Host Network and PSP

Figure 5-3 shows the architecture for a UE to access a neutral host network using a CBRS-I value and a CBRS-NID. The UE is accessing the network using NHN Access Mode. The yellow line illustrates the data

plane path between the UE and the ePDG belonging to SP2, which can be used to access the service provider's services if the Neutral Host Network is considered untrusted by SP2.

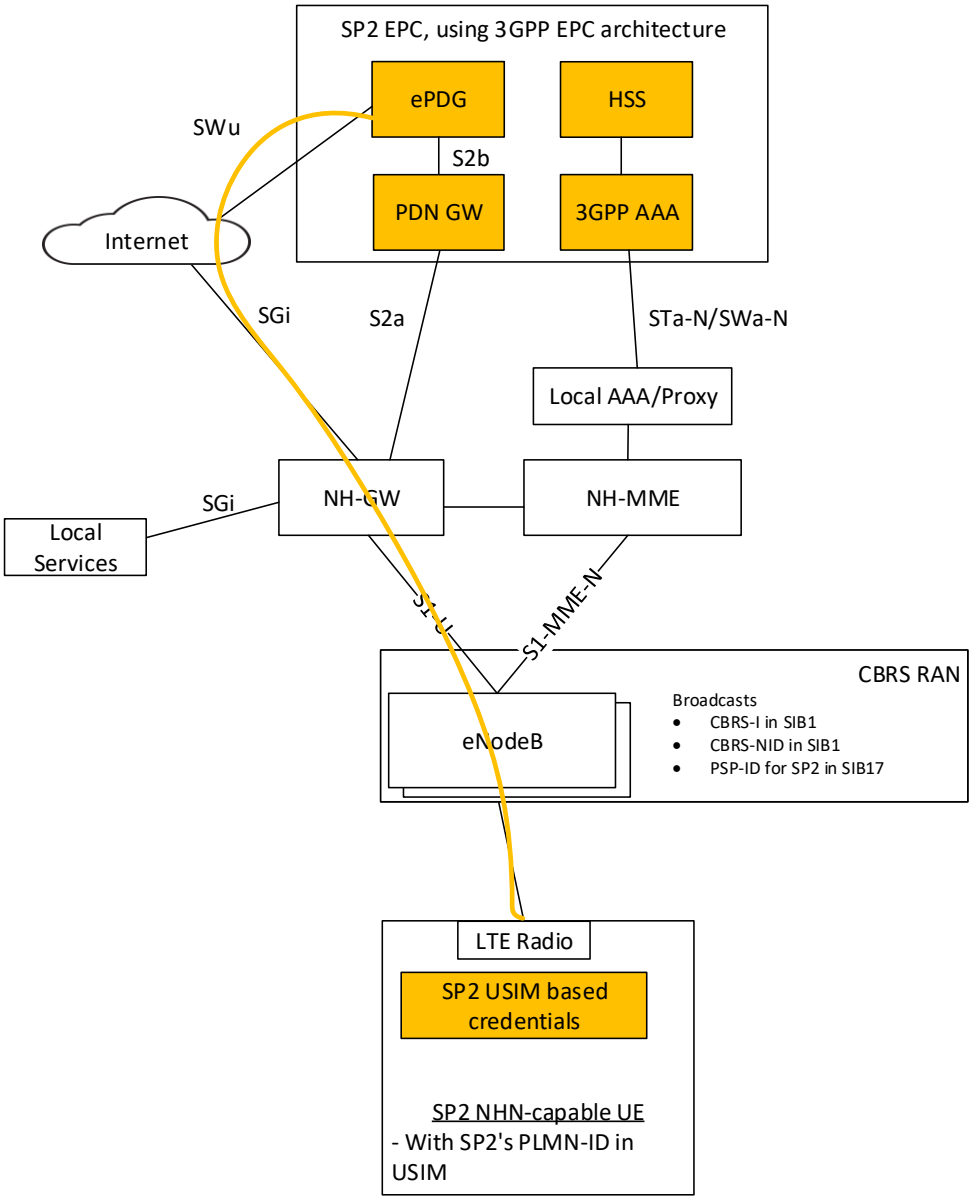

Figure 5-3 Network Architecture – Neutral Host Network and Participating Service Provider

5.2.4 Network Architecture – Private Network using Neutral Host Network

Figure 5-4 shows the architecture for a UE to access a private network based on the Neutral Host Network architecture using a CBRS-I value and a CBRS-NID. The UE is accessing the network using NHN Access Mode.

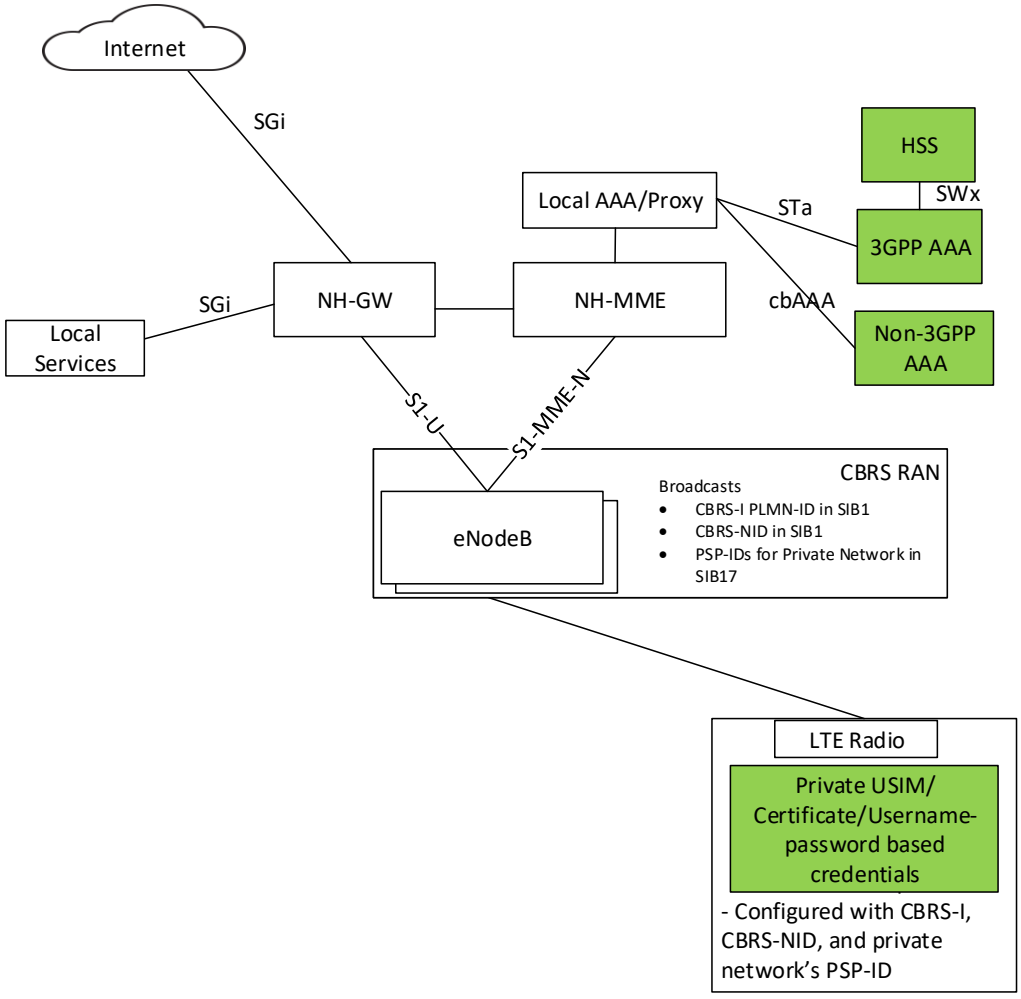

Figure 5-4 Network Architecture – Private Network using Neutral Host Network

5.2.5 Network Architecture – Hybrid Network

Figure 5-5 shows the architecture of a hybrid network. A hybrid network can be built on any combination of the architectures described in sections 5.2.1 through 5.2.4.

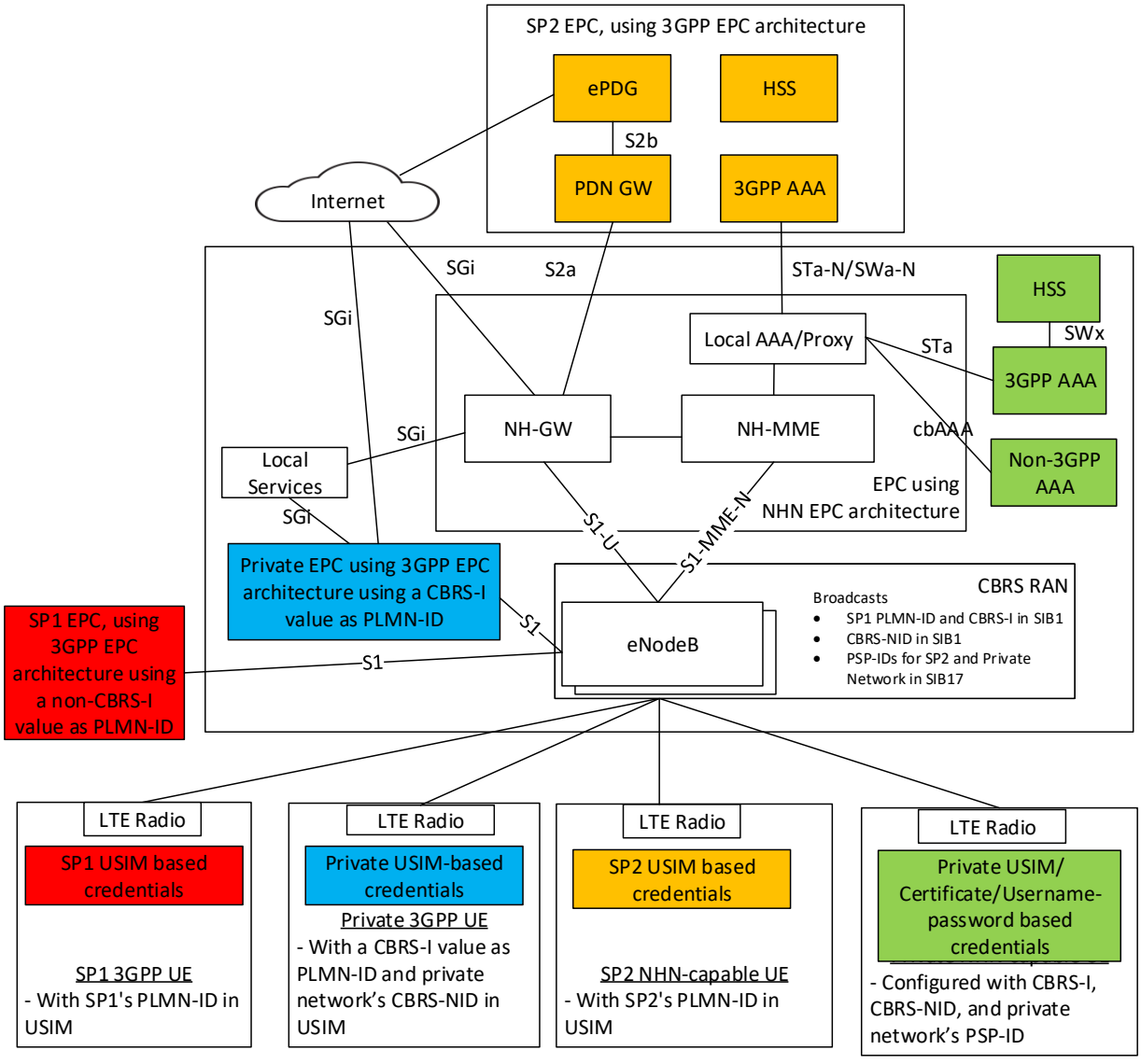

Figure 5-5 Network Architecture – Hybrid Network

The S1 interface to a Private EPC using the 3GPP EPC architecture shown in Figure 5-5 is the same as the 3GPP defined S1 interface if the PLMN-ID associated with the EPC is not used by any other EPC connected to the CBRS RAN. Otherwise (i.e., when a private 3GPP EPC and a NHN EPC are both associated with the same

PLMN-Identity), the architecture above is realized using a dual-mode EPC (supporting 3GPP EPC mode and NHN EPC mode) and a single interface from the CBRS network's RAN to the dual-mode EPC. The dual-mode EPC can function as a private 3GPP EPC and as a NHN EPC. Entities in the dual-mode EPC perform corresponding 3GPP and NHN functions. For instance, the MME/NH-MME in a dual-mode EPC determines if the UE is accessing the network using NHN Access Mode upon detecting a special IMSI (i.e., an IMSI composed of a CBRS-I value followed by 9 digits containing the value zero) and 3GPP Access Mode otherwise.

5.3 Identities

5.3.1 CBRS-I

CBRS-I is an indication that a CBRS network supports the architecture defined in this specification or that the CBRS network serves the CBRS-I PLMN identity using the 3GPP EPC architecture. The format of a CBRS-I is the same as a PLMN identity and the value is a globally unique PLMN value reserved by the CBRS Alliance. A CBRS-I is broadcasted in SIB1 as an entry in the PLMN-IdentityList. Some operators may also obtain their own PLMN-ID to be used as CBRS-I. Such CBRS-Is are called Supplemental CBRS-I values. Any CBRS-I values (i.e., a PLMN-Identity that is reserved by the CBRS-A or a PLMN-Identity configured as a supplemental CBRS-I value by a service provider) shall be interpreted equally in UE and network procedures or functions.

- As pointed out in clause 5.7.2 of [2], an NH-MME/MME serving a UE attached using CBRS-I shall form the GUMMEI per [16] using the CBRS-I as the source of the MCC and MNC (size is per 3GPP specifications). The MMEI used to create the GUMMEI is formed per [16] using the MME Group ID (16 bits) and MME Code (8 bits) assigned to the NH-MME/MME. The GUTI is formed per [16] from the GUMMEI and the M-TMSI (32 bits) assigned by the NH-MME/MME.

5.3.2 CBRS-NID

CBRS-NID is the identity of the NHN or the Private EPS Network. The CBRS-NID may identify a single venue (e.g. a stadium) or a collection of venues (e.g., a chain of fast food restaurants).

- CBRS-NID is associated with the CBRS-I and is broadcasted in the CSG-ID field of SIB1 (see section 6.2.2) and is unique within a given CBRS-I value.
- CBSDs using the same CBRS-NID must support the same list of PSPs.
- Length of CBRS-NID applicable for networks broadcasting CBRS Alliance CBRS-I is 27 bits
- An NH-MME/MME's Group ID and MME Code shall be considered as unique only within a network using a given CBRS-NID value.

5.3.3 PSP-ID

PSP-ID is an identity of a participating service provider that provides services via a NHN.
Three types of PSP-IDs are supported:

- PLMN based PSP-ID is a PLMN-ID of the PSP (as in [1]),
- OID based PSP-ID can be constructed using Organization Identifier of the PSP as discussed in clause 5.7.1 of [2]. If OID-based PSP-ID is longer than 24 bits, a short-form PSP-ID is calculated as described in clause 5.7.1 of [2].

- Domain based PSP-ID can be constructed using domain name of the PSP as discussed in clause 5.7.1 of [2]. A short-form PSP-ID is calculated as described in clause 5.7.1 of [2].
- PSP-IDs of length 24 bits and short-form PSP IDs are broadcasted in SIB17 by re-using the wlan-OffloadInfoPerPLMN-List-r12 for the CBRS-I PLMN value as described in section 6.2.2.
- The components in the NHN EPC and the CBRS RAN shall be provisioned with the list of PSP Identities under NHN access mode.
- A PSP may or may not support S2a. Support for S2a interface is indicated to the UE in the PSP information that is broadcasted in SIB17. Pre-provisioned policy in the UE can guide the UE to utilize this indication. For example, there may be a policy to select the PSP only if S2a interface is supported.
- CBRS Network Name: CBRS Network-Name is a meaningful name of the NHN/Private Network to be presented to the end user when doing manual network selection and when UE is attached to a NHN/Private Network. CBRS Network Name is a 48-character string and is broadcasted using SIB9 field hnb-name. The presence of CBRS-I will indicate to the UE that hnb-name should be interpreted as CBRS Network-Name.

5.4 UE Types and states

5.4.1 General

A UE may have one or more subscriptions.

5.4.2 UE Types

The following four UE types are defined. Capabilities are cumulative, i.e., a CBRS-Type III UE has all the capabilities of CBRS-Type I-III UEs. A CBRS-Type II UE is the minimum level required for NHN support. No assumptions are made about support for other radio technologies such as 3G.

1. A CBRS-Type I UE is a normal LTE UE supporting 3GPP procedures with CBRS band support.
    - A CBRS-Type I UE cannot attach to a NHN and does not support NHN procedures.
2. A CBRS-Type II UE supports NHN selection procedures, mobility procedures, security procedures, and RAN identifiers. A CBRS-Type II UE has a single LTE transmit radio and a dual EMM context. A CBRS-Type II device can be EMM Registered on at most one access network at a time.
    - For a CBRS-Type II UE, all PDN connections over 3GPP access are assigned to the same access network (e.g., all on an SP network or all on a NHN).
3. A CBRS-Type III UE has a single LTE transmit radio, dual EMM contexts, and can listen for paging on both EMM contexts, plus search and identify target cells on the non-serving NHN or SP network (possibly at some cost to performance). A CBRS-Type III device can be EMM Registered on two access networks simultaneously.
    - For a CBRS-Type III UE, PDN connections over 3GPP access can be assigned to different access networks (e.g., Internet on the 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-Type III UE has a single transmit radio, 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-Type III UE may have to perform periodic TAU procedures on the access network where it is in IDLE state.

4. A CBRS-Type IV UE has dual LTE transmit radios, dual EMM contexts, and dual ESM contexts.
    - User-plane data can flow over both ESM contexts simultaneously, at the granularity of PDN connections.

The UE CBRS-Types II-IV use the same NHN attach, service request, mobility and session procedures as defined in MFA TS MF.202 [2] and 3GPP TS 23.401 [14] with the changes defined in this specification.

5.4.3 Operation of Mobile Devices

CBRS-Type I device: Since this is a normal LTE UE with CBRS band support, there are two radio states:

- camped on SP access network (RRC Idle)
- connected on SP access network (RRC Connected)

CBRS-Type II device: All PDN connections are established over 3GPP access, for example the Internet and IMS PDN connections, are assigned to the access network on which the device is EMM Registered. A CBRS-Type II device has the following mutually exclusive main radio states:

- camped on SP access network (RRC Idle)
- connected on SP access network (RRC Connected)
- camped on NHN access network (RRC Idle)
- connected on NHN access network (RRC Connected)

CBRS-Type III device: For a device capable of being simultaneously registered to two access networks (e.g., SP and NHN), different PDN connections may be assigned to different access networks. In accordance with 3GPP specifications, mobile-originated or network-originated data for a PDN connection is routed over the corresponding access network. The assignment of PDN connections to access networks is governed by policies provisioned in the UE and/or SP network. For example, the device may implement switching logic such that the IMS PDN connection (for VoLTE) remains on the SP access network whenever possible.

While registered to two access networks, a CBRS-Type III device has the following mutually exclusive main radio states:

- camped on SP Network (RRC Idle), camped on NHN (RRC Idle)
- camped on SP Network (RRC Idle), connected on NHN (RRC Connected)
- connected on SP Network (RRC Connected), camped on NHN (RRC Idle)
    - This is an optional state.
- Not camped on SP Network, camped on NHN (RRC Idle)

- Not camped on SP Network, connected on NHN (RRC Connected)

A CBRS-Type III device can receive paging messages on both access networks, with the limitations such as the one described below.

> A CBRS-Type III device may be RRC Connected on only one access network at a time. Conflicts can occur; for example, the device may receive a paging message for the IMS PDN connection on the SP access network indicating an incoming VoLTE call, while the device is in RRC Connected state on the NHN for the Internet PDN connection. An implementation-dependent policy resolves such conflicts, for example by switching to RRC Connected on the SP access network and causing an interruption in service for the Internet PDN connection.

CBRS-Type IV device: A CBRS-Type IV device has dual uplink/downlink radio chains and a full LTE state machine for both access networks.

5.5 Functions and Procedures

5.5.1 General

Functions and procedures applicable to NHN Access Mode described in clause 5.5.2 are supported. On the network side, they are realized primarily using CBRS RAN and EPC using NHN EPC architecture depicted in Figure 5-5.

3GPP procedures applicable to 3GPP Access Mode described in clause 5.5.3 are supported. On the network side, they are realized primarily by CBRS RAN and EPC using 3GPP EPC architecture depicted in Figure 5-5.

EPC selection is carried out as specified in 3GPP TS 36.331 [13]. When connecting to a cell in CBRS RAN broadcasting multiple PLMN-Identities, a UE indicates the PLMN-Identity of the EPC that it wants to attach to and the cell selects an EPC connected to it based on the indication. This also applies to the case when using a dual-mode EPC discussed in Section 5.2.

The IMSI used in the Attach Request of the initial Attach procedure indicates the preferred Access Mode for a UE to the appropriate EPC. An IMSI comprised of a CBRS-I value and 9 zeros is used to indicates preference for NHN Access Mode. Any other IMSI indicates the UE's preference for 3GPP Access Mode.

5.5.2 NHN Access Mode functions and procedures

5.5.2.1 General

The following terminology differences exist between the terminology of the MulteFire Alliance and the terminology of the CBRS Alliance.

- MFA TS MF.202 term *"MulteFire cell"* or *"MF cell"* is interpreted as *CBRS cell*
- MFA TS MF.202 term *"MulteFire RAN"* is interpreted as *CBRS RAN*
- MFA TS MF.202 term *"MulteFire network"* is interpreted as *"CBRS network"*

- MFA TS MF.202 term *"MulteFire AP"* is interpreted as *CBRS eNB*
- MFA TS MF.202 term *"MulteFire UE"* is interpreted as *CBRS UE*
- MFA TS MF.202 term *"NHAMI"* is interpreted as *"CBRS-I"*
- MFA TS MF.202 term *"NHN-ID"* is interpreted as *"CBRS-NID"*

All functions and procedures specified in [2] are supported except for the following:

- Online Sign-up (OSU) and broadcast of indication for support of OSU,
- Locally administered CBRS-NIDs,
- NHN service discovery,
- Access service Authorization.

5.5.2.2 Modifications to MulteFire Features

This specification explicitly uses the following technical aspects that are different from [2].

- Network Discovery and Selection: A UE discovers NHN CBRS networks by scanning CBRS frequency bands for networks broadcasting a pre-provisioned CBRS-I as a PLMN-Identity in SIB1.
    - The following aspects are common with [2]
        - A NHN-capable UE using a USIM based subscription may select a CBRS-network (and attach to the network using NHN procedures) when the network broadcasts a PSP-ID in SIB17 which identifies the service provider that provisioned the credentials/subscription information into the UE. The PSP-IDs may be the Home PLMN (HPLMN) ID or an equivalent HPLMN ID stored in the USIM.
        - A NHN-capable UE using a non-USIM based subscription may select a CBRS-network (and access the network using NHN procedures) if the network broadcasts a PSP-ID associated with the subscription. In this scenario, PSP-IDs may be an OID of the service provider or a short form based identity of service provider.
- Mobility in RRC Idle: Mobility between two CBRS networks with different CBRS-NIDs or CBRS-Is in RRC Idle mode relies on policies configured in the UE, and may not rely on network configured neighbor lists or thresholds. The UE uses the following procedure during such mobility.
    - Access attempts (Attach procedure, Service Request procedure, TAU procedure) by a UE using 3GPP access mode and with IMSI not belonging to network shall be rejected as specified in section 5.5.3.1.
    - For mobility between cells broadcasting different CBRS-NIDs, 3GPP defined LTE procedures apply, and in addition the UE shall perform a Tracking Area Update (TAU) procedure after selecting or reselecting to the target cell. If the NH-MME associated with the target cell does not recognize a GUTI provided by the UE, for example because the source and target cells are connected to different core networks, the target NH-MME should reject the TAU procedure with an appropriate cause. The UE could then perform an Initial Attach procedure for the existing PDN connections.

- UE performs Initial Attach procedure when moving between two CBRS networks broadcasting different CBRS-I values.

5.5.3 3GPP Access Mode functions and procedures

The functions and procedures specified by 3GPP are supported with one adaptation discussed in Section 5.5.3.1.

Note that 3GPP Access Mode is supported by a UE supporting functions and procedures specified by 3GPP.

Operational considerations for deployments using 3GPP EPS Architecture are discussed in Appendix A.1.

5.5.3.1 Rejecting access attempts by a UE with IMSI not belonging to network

The EMM cause used for ATTACH REJECT, TRACKING AREA UPDATE REJECT and SERVICE REJECT by a CBRS network's EPC identified by CBRS-I and connected to a hybrid CSG RAN [17] shall be Cause #12 defined in 3GPP TS 24.301 [5], when the associated UE uses an IMSI that does not belong to the network. Exceptions to this requirement include but are not limited to:

- security attacks by the UE,
- the UE is determined to be stolen using ME identity check procedure (see clause 5.3.10.5 of 3GPP TS 23.401 [14]),
- repeated access attempts by the UE,
- the UE causes excessive signaling.

Note: Use of other EMM cause values (e.g., Cause #3, Cause #8) can cause the UE to suspend access to all networks broadcasting CBRS-I, including networks where the UE's USIM based subscription is accepted (see clause 5.5.1.2.5 of 3GPP TS 24.301 [5]).

Note: When using the EMM Cause #12, TACs of nearby networks should be coordinated to ensure that nearby networks do not use same TAC. When two nearby networks use the same TAC, a UE belonging to one of the networks on receiving a reject from other network with above cause code will temporarily not attempt access to its home network.

A type-I UE can be enhanced so that it does not connect to a hybrid cell [17] to register with an EPC identified by CBRS-I if the cell broadcasts a CBRS-NID that is not in the UE's CSG list. However, this requires that the lists are well maintained. If the lists are not well maintained, the enhancement can result in the UE not connecting to its home network.

6 Stage 3 Aspects

6.1 General

Stage 3 aspects for NHN Access Mode based on MFA NHN specifications is discussed in Section 6.2. Stage 3 aspects for 3GPP Access Mode based on 3GPP specifications is discussed in Section 6.3.

6.2 Stage 3 aspects of NHN access mode

6.2.1 General

In NHN Access Mode, Stage 3 functionality, procedures, messages and IEs shall comply to the 3GPP EPS stage 3 specifications, with the following exceptions:

- Instead of 3GPP TS 36.413 (S1-AP) [11], the MFA TS 36.413 [9] shall be used.
- Instead of 3GPP TS 24.301 (NAS) [5], the MFA TS 24.301 [10] shall be used with the following adaptations:
    - If an NH-MME does not recognize a GUTI provided by a UE for Tracking Area Update (TAU) procedure, the NH-MME should reject the TAU procedure with cause value #9 (UE identity cannot be derived by the network) or #10 (Implicitly detached) (see Section A.1 in [5]).
- Instead of 3GPP TS 33.401 (Security) [12], the MFA TS 33.401 [13] shall be used.
- Modifications as outlined in the sub-sections 6.2.2 and 6.2.3.

6.2.2 RRC

The CBRS-I is broadcasted in SIB1 as an entry in the PLMN-IdentityList. In addition to being configured with one or more of the CBRS-I values reserved by the CBRS Alliance, the UE may be configured with supplemental CBRS-I values. Such additional CBRS-I values may be used by large NHN operators who can obtain their own CBRS-I value (PLMN-ID).

In NHN Access mode, SIB17 shall be broadcasted by the CBRS RAN.

The following technical aspects are different from [3]:

- CSG-ID field within SIB type 1 is used to carry the CBRS-NID. Format of the field remains as specified in [3].

- CBRS Network-Name is a string of less than or equal to 48 characters and is broadcasted using SIB type 9 field hnb-name. The presence of CBRS-I shall indicate to the UE that hnb-name should be interpreted as CBRS Network-name.

- SIB type 17 that is used for providing WLAN configuration information for LTE-WLAN Interworking shall be used for announcing PSP identities (PSP-IDs) in NHN. SIB type 17 is specified in [3]. The PSP-IDs are announced using the WLAN-Id-List-r12 corresponding to CBRS-I and shall always be placed after the WLAN configuration (if WLAN configuration is announced in the network). WLAN-OffloadInfoPerPLMN-r12 shall not be present for PSP Information. WLAN-Identfiers-r12 is comprised of a sequence of ssid-r12, bssid-r12 and hessid-r12.
    - The WLAN-Identfiers-r12 announcing PSP information shall contain a multicast and locally administered bssid-r12 value. This bssid-r12 shall be a fixed value and serve as an indication to the receiver that the information present in the ssid-r12 shall be interpreted as PSP information and shall not be interpreted as WLAN information. Considering that there can be

different PSP types, the following table provides the mapping of bssid-r12 value and the corresponding PSP type.

Value of bssid-r12	Interpretation by receiver
03:ff:ff:ff:ff:ff	WLAN-Identfiers-r12 contains PLMN based PSP Information
03:ff:ff:ff:ff:fe	WLAN-Identfiers-r12 contains OID based PSP Information
03:ff:ff:ff:ff:fd	WLAN-Identfiers-r12 contains short-form based PSP Information

- The ssid-r12 field (of length 32x8=256 bits) shall be interpreted as a sequence of PSP Information entries. Each PSP Information entry is 28 bits and is composed of a 24 bit PSP-ID followed by four feature bits. Reserved feature bits shall be set to zero by the sender and ignored by the receiver. The meaning and purpose of the feature bits is as follows:

B3	B2	B1	B0 (LSB)
PLMN based PSP identities: PSP supports S2a if bit is set. Reserved for other types of PSP identities.	Reserved	Reserved	Reserved

- For a WLAN-Identifiers-r12 entry with a PSP-information list, the hessid-r12 field is reserved for future use and shall not be included by the sender and shall be ignored by the receiver.

6.2.3 STa interface

The following technical aspects are different from [2]:

- The ANID AVP shall be created as the concatenation of the following:
  - Constant character string “CBRS” shall be used as a prefix
  - CBRS-NID represented as a 7-digit hexadecimal number using UTF-8 encoding of the digits

6.3 Stage 3 aspects of 3GPP access mode

In 3GPP Access Mode, Stage 3 functionality, procedures, messages and IEs shall comply to the 3GPP EPS stage 3 specifications.

7 Other Aspects

7.1 NHN KPIs

The minimal set of KPIs supported in a NHN are:

- The number of Attempted EPS attach procedures [6, Sect. 4.1.1.1]
- The number of Successful EPS attach procedures [6, Sect. 4.1.1.2]
- The number of Failed EPS attach procedures [6, Sect. 4.1.1.3] per reject cause
- EPS Attach Success Rate [8, Sect. 5.1.1]
- Dedicated EPS Bearer Creation Success Rate [8, Sect. 5.1.2]
- Service Request Success Rate [8, Sect. 5.1.4]

The KPIs can be reported to the PSP according to the performance measurement file format defined in [7]. The PSP and NHN operator agree on the end points and file transfer method (e.g., TCP) for the transfer of files containing performance measurements.

Appendices (Informative)

Appendix A: Operational considerations

A.1 Deployments using 3GPP EPS Architecture

The CBRS Alliance (CBRSA) will operationalize the following administrative tasks:

- Acquire an MNO independent PLMN-ID for the CBRS Alliance
- Enable 3rd party entities to reserve CBRS-NID values from CBRS-NID pool for the CBRSA PLMN-ID. These values will be broadcast in the CSG-Identity field of SIB1.

When the CBRSA has its own PLMN-ID value, then the CBRSA also has full control of the associated IMSI pool (PLMN-ID + 9 digits). This would allow the CBRSA to enable CBRS-NID holders to also reserve IMSI values from the CBRSA IMSI pool.

USIM providers can produce private USIMs (e.g., a UICC card containing credentials to a Private Network) for the CBRSA CBRS-NID holders who have reserved CBRSA IMSIs. These private USIMs would be associated with a private authentication backend solution. The backend solution could be a distributed local solution "AuC-on-a-USB-stick" or a cloud solution exposing Web APIs for private USIM authentication.

An entity desiring to deploy a Private CBRS Network would reserve its own CBRS-NID and a desired amount of IMSI values from CBRSA. The deploying entity would source private EPS infrastructure (CBRS RAN + EPC) from infrastructure vendors. A Private Network would be configured to operate as a closed CSG network broadcasting the CBRSA PLMN-ID and the CSG-ID equal to reserved CBRS-NID.

The Private Network may also use hybrid CSG [17] configuration if it is expected that the CSG lists configured in the associated UEs are not well maintained. However, hybrid CSG [17] configuration makes the network vulnerable to attempts from UEs of other networks (also see Section 5.5.3.1).

The deploying entity would acquire private USIMs and an associated private USIM authentication solution for its approved IMSIs from a USIM provider. USIMs would be used within the UEs and the CBRS-NID would be configured to the UE CSG white list. Naturally the Private USIM authentication backend would authenticate only the specific IMSI values and the matching shared secret credential (K) which are associated with the accessed Private CBRS network as identified by the network's CSG-ID.

A.2 Deployments using Private EPCs

For a Private Network using only a Private NHN EPC (supporting only CBRS type 2 and above UEs), closed CSG configuration is strongly recommended as it will significantly reduce the chances of UEs of other networks from attempting access to the network. CSG configuration for a Private Network with type 1 UEs is discussed in Appendix A.1.

CBRS-A can reserve a set of TACs for use only by networks using closed CSG configuration. It is recommended that networks using closed CSG configuration use any such reserved TACs since the UEs of such a network would then not be blocked from attempting an access to their home network by another network rejecting the UEs using EMM Cause #12 as specified in clause 5.5.3.1 (since they would not blacklist a TAC from the set of reserved TACs).

Appendix B: A note about this document's development

The normative material in this document was developed based on:

- CBRS Network Services Technical Report, CBRSA-TR-1001 V1.0.0.
- CBRS Network Services Private Networks Technical Report, CBRSA-TR-1002 V0.15.0.

The technical reports further contain more detailed discussions and recommendations for best practices.

Note: The technical reports may only be available internally to CBRS Alliance members.

Appendix C: Revision History

Table C-1 : Change History

Version	Date	Description
V1.0.0	2018-02-01	Release 1 of this Specification