CBRS Network Services – Private CBRS / Non-Public network geofencing, policies, and TAC collision avoidance

ONGO-TS-1004

V5.1.0

2022-12-15

LEGAL NOTICES AND DISCLOSURES

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, ONGO 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 ONGO ALLIANCE IPR POLICY. ONGO 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 ONGO 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.

THIS DOCUMENT (INCLUDING THE INFORMATION CONTAINED HEREIN) IS PROVIDED AS A CONVENIENCE TO ITS READERS, DOES NOT CONSTITUTE LEGAL ADVICE, SHOULD NOT BE RELIED UPON FOR ANY LEGAL PURPOSE, AND IS SUBJECT TO REVISION OR REMOVAL AT ANY TIME WITHOUT NOTICE. THIS DOCUMENT IS PROVIDED ON AN "AS IS", "AS AVAILABLE" AND "WITH ALL FAULTS" BASIS. ONGO ALLIANCE MAKES NO REPRESENTATION, WARRANTY, CONDITION OR GUARANTEE AS TO THE USEFULNESS, QUALITY, SUITABILITY, TRUTH, ACCURACY, OR COMPLETENESS OF THIS DOCUMENT OR ANY INFORMATION CONTAINED HEREIN. ANY PERSON THAT USES OR OTHERWISE RELIES IN ANY MANNER ON THE INFORMATION SET FORTH HEREIN DOES SO AT HIS OR HER SOLE RISK.

IMPLEMENTATION OF A [NETWORK] AND/OR RELATED PRODUCTS OR SERVICES IS OFTEN COMPLEX AND HIGHLY REGULATED, REQUIRING COMPLIANCE WITH NUMEROUS LAWS, STATUTES, REGULATIONS AND OTHER LEGAL REQUIREMENTS ("LEGAL REQUIREMENTS"). AMONG OTHER THINGS, APPLICABLE LEGAL REQUIREMENTS MAY INCLUDE NETWORK OPERATOR REQUIREMENTS UNDER FEDERAL LAW, REQUIREMENTS RELATING TO E-911, ETC. A DISCUSSION OF SUCH LEGAL REQUIREMENTS IS BEYOND THE SCOPE OF THIS DOCUMENT. ACCORDINGLY, NETWORK OPERATORS AND OTHERS INTERESTED IN IMPLEMENTING NETWORKS OR RELATED SOLUTIONS ARE STRONGLY ENCOURAGED TO CONSULT WITH APPROPRIATE LEGAL, TECHNICAL AND BUSINESS ADVISORS PRIOR TO MAKING ANY IMPLEMENTATION DECISIONS.

OnGo Alliance
3855 SW 153rd Drive, Beaverton, OR 97003
www.ongoalliance.org
info@ongoalliance.org

Table of Contents

Table of Figures

Table of Tables

1 Introduction and Scope

This document is a Technical Specification (TS) that provides recommendations for the operation of UEs and network functions for identification, geofencing, and TAC collision avoidance of Private CBRS / Non-Public Networks that employ shared PLMN ID. The current scope of the TS is centered on LTE based Private CBRS / Non-Public Network(s). Aspects needed for NR are not addressed in this release of the TS. Different use cases for providing network services for Private CBRS / Non-Public network operation are also described. It provides the stage 2 and stage 3 details involved.

The proposed geofencing framework may encompass UE policy management, but it is out of the scope of this release of the TS.

Note that the support of the features detailed in this document in recommended, but entirely optional for both the deployed Private CBRS / Non-Public Network and the UE.

1.1 KEY WORDS

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

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

2 References

[1] CBRSA TR-0101 CBRS Alliance Identifier Administration Guidelines for Shared HNI

[2] CBRSA-TS-1001 CBRS Network Services Use Cases and Requirements

[3] CBRSA TS-1002 CBRS Network Services Stage 2 and 3 Specification

[4] 3GPP TS 24.301 Technical Specification Group Core Network and Terminals ; Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3

[5] 3GPP TS 23.032 Universal Geographical Area Description (GAD)

[6] 3GPP TS 31.102 Technical Specification Group Core Network and Terminals; Characteristics of the Universal Subscriber Identity Module (USIM) application

[7] 3GPP 23.003 Technical Specification Group Core Network and Terminals; Numbering, addressing and identification

[8] 3GPP TS 24.008 Technical Specification Group Core Network and Terminals; Mobile radio interface Layer 3 specification; Core network protocols; Stage 3

[9] GSMA RSP Technical Specification Version 2.4

[10] 3GPP TS 36.331 Radio Resource Control (RRC); Protocol specification

[11] Remote Application Management over HTTP Card Specification v2.2 – Amendment B

[12] ETSI TS 102.226 Remote APDU structure for UICC based applications

3 Definition and Abbreviations

3.1 Definitions

Term	Definition
Cell-ID	This is the eNB / gNB identifier broadcasted by the node.
Enterprise or Private CBRS / Non-Public Network	Private or Neutral Host Networks with LTE deployed for Private CBRS / Non-Public network campus coverage for both indoor and outdoor footprints.
Enterprise Local Server	EIS server located within the intranet of an Private CBRS / Non-Public Network.
EnterprisePrivate CBRS / Non-Public network Central Public Server	EIS server located outside the intranet of an Private CBRS / Non-Public Network within the public IP domain.
Enterprise Identifier	A unique network identifier within a CBRS-I [3] that is associated with a specific Private CBRS / Non-Public Network. Note that SHNI is one such CBRS-I.
Enterprise Information	The information associated with a given enterprise consisting of one or more sites and includes the geofencing, enterprise deployed network identifiers, and policy information.
Enterprise Name	Set to the Enterprise Identifier converted to a text string. This Private CBRS / Non-Public network name is used to match against the name broadcasted on SIB9 from an Private CBRS / Non-Public network eNB by the UE.

3.2 Abbreviations

Abbreviation	Explanation
ASN.1	Abstract Syntax Notation One
CBRS	Citizens Broadband Radio Service
CBRS NID	CBRS Network Identifier
DMZ	Demilitarized Zone
DNS	Domain Name System
EIS	Enterprise Information Service
ELS	Enterprise Local Server
ECS	Enterprise Central Server
HNI	Home Network Identifier
LPA	Local Profile Assistant
RAT	Radio Access Technology

Abbreviation	Explanation
SM-DP+	Subscription Management Data Preparation
TAC	Tracking Area Code
TAI	Tracking Area Identity
UE	User Equipment

4 Geofencing Private CBRS / Non-Public network campuses

There are several features that may be enabled by associating the different Private CBRS / Non-Public network deployments with a geofenced area for the both the network and the UE.

Employing geofenced areas allow the UEs to perform power optimized scans when searching for specific Private CBRS / Non-Public network campus network. The information provided to the UE includes information on home enterprise networks and can additionally also provide the roaming partner network related information as well associated with a given private network subscription.

From a network perspective, it primarily allows for better managing common address spaces that may potentially conflict with other deployments. This problem is inherent for LTE private network deployments employing the SHNI and obtaining IBNs, ECGI, GUMMEI, and TAIs. Even with the regulation, misuse may happen intentionally or unintentionally. This problem is particularly seen with TAIs, with only 6 allocated to each IBN allocation [1][3], which will restrict the number of deployments by the same entity within a given geographic area. This becomes less of an issue with a geofenced approach and the UE inherently avoiding regions where it does not need to look for Private CBRS / Non-Public Network(s).

Private CBRS / Non-Public Networks vary in size and may require a coarse geofencing, covering a large area or potentially require building level geofencing to allow the UEs determine proximity to an Private CBRS / Non-Public Network. Using GPS based geofencing alone may have power consumption implications on the UE side and hence other methods such as MNO network Radio Footprint may be considered. The GPS location of the Private CBRS / Non-Public network eNB obtained during deployment allows for determining the rough coverage of the campuses but do not directly translate to the actual available RF footprint of the Private CBRS / Non-Public Network.

The following sections provide mechanisms for UEs to identify the EIS server associated with the individual stored credentials and retrieve geofencing and policy-based information. It is to be noted that the support of the EIS is optional for both network and UE. Private CBRS / Non-Public network related information on geofencing and other policies may be delivered to the UE through alternative methods.

4.1 Geofencing information

The geofencing information carried as part of the Enterprise Information is specified as GPS information and / or Radio Footprint information.

- GPS information: The geofence information is specified based on the shapes defined in [5] using one or more of these entries to define the boundaries of the Private CBRS / Non-Public network campus.
    - Set of ellipsoid points with uncertainty circle (See Section 5.2 in [5]) identifying boundaries.
    - A polygon with the set of connected points of GPS coordinates in sequence connecting back to the initial point establishing the boundaries of the Private CBRS / Non-Public network campus (See Section 5.4 in [5]).
- Radio Footprint information: The radio footprint information is
    - Specified as a set of public network Cell-IDs indicating a potential availability of an Private CBRS / Non-Public network campus network when the UE enters these macro cells.

- Specified as a set of public network Cell-IDs along with the associated signal strengths to allow for finer control on the locations where the UE should start looking for Private CBRS / Non-Public network campus.

Figure 4-1 provides pictorial view of the different geofencing techniques. The UEs may employ the information provided to optimally search and camp on Private CBRS / Non-Public Networks.

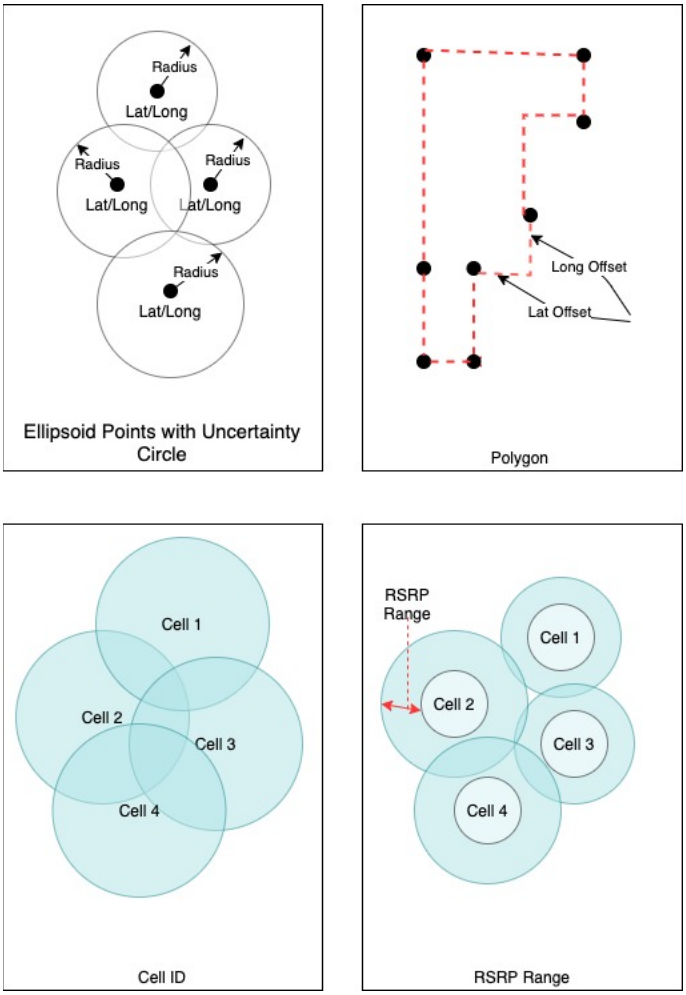

Figure 4-1: Geofencing Types

5 Enterprise credential identification in the UE

This section provides the mechanism to associate the credentials provisioned in the UE to belong to specific enterprises (Private CBRS / Non-Public network). The Enterprise Identifier is included as part of the SIM profile configuration for both physical and embedded SIMs.

Each Enterprise Network must have a unique Enterprise Identifier. This identifier can be obtained through

- OnGo Alliance by requesting for CBRS NID when the network is using SHNI that can be utilized for LTE and NR networks

  or

- IANA for a 3GPP NID that is globally unique

Note: Self-assigned NID can also be used but it may not be unique.

The SIM credential provisioned in the UE to access the Private CBRS / Non-Public Network is provisioned with this Enterprise Identifier. The Enterprise Identifier is used by the UE to receive Enterprise Information that is used to find and operate on the Private CBRS / Non-Public Network.

This Enterprise Identifier or a unique name associated with the identifier shall be transmitted by the eNB for the UE to recognize prior to accessing the network. When transmitting the name, the Enterprise Identifier is converted to a text string and the digits transmitted as string.

Provisioning this identifier into the SIM credential may allow the UE to determine the association of specific credentials with Private CBRS / Non-Public network campuses. This association may further be used to identify policies and behaviors that the UE may employ when connecting with the Private CBRS / Non-Public network Network. This Enterprise Identifier may be employed by the UE to determine its Enterprise Information Server as defined in Section 6.

Note: The UE may obtain the Private CBRS / Non-Public network geofencing and policy information through other methods not explicitly covered in this technical specification.

The provisioning of the Enterprise Identifier in the SIM credential when included in the credential definition, shall follow the definitions in the SIM profile as defined below.

- Method 1: For 4G : PLMN + CSG-ID (E.g., SHNI + CBRS NID as CSG-ID) in SIM Profile[1]. The SIM profile must include the CSG-ID and can also support the Operator Home NodeB Name.
- Method 2: For 4G and 5G: Vendor specific extension that carries the Private CBRS / Non-Public network identifier in it. The vendor specific extension is defined as [per GSMA SGP.22-v2.4].

When a Private CBRS / Non-Public network identifier is associated with a SIM credential, at a minimum method 1 shall be used. Method 2 may be optionally supported.

See Section 9 for CSG-ID and eSIM metadata provisioning details.

[1] This Enterprise Network identifier definition in the SIM profile is not intended to require CSG capabilities from the UE. It is mearely used to employ CSG fields to point to an Enterprise Identifier

The UE may use the Enterprise Identifier to check with the Enterprise Information Server to identify the Private CBRS / Non-Public network campus and download the associated Enterprise Information that may be employed by the UE.

6 Enterprise Information Service (EIS)

The Enterprise Information Service is a server that can be hosted in a private or public cloud and is provisioned with the information relating to the individual enterprise deployments. This information is intended to provide information to UEs to optimally find specific Enterprise Network and also provide the network configuration (e.g., employed identifiers) to prevent denial of service. Figure 6-1 presents a high level architecture for the EIS.

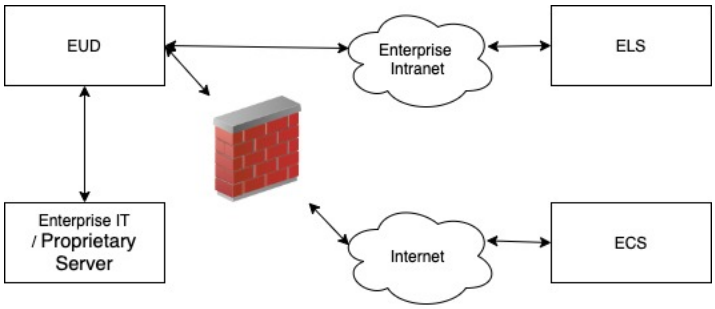

Figure 6-1: Enterprise Information Service High Level Architecture

The actual protocol used for Enterprise Information delivery to the UE is currently out of scope of this specification. However, see Appendix C for viable techniques with established protocols that are used for other purpose that are leveraged to deliver the *EnterpriseInformation* object.

6.1 Enterprise Information Service Server (EIS Server)

The Enterprise Information Server can be locally located within the Enterprise Network and / or in a central server. For some enterprises, the Enterprise Information can be sensitive and will not allow for it to be hosted on a public cloud. The EIS can be hosted on premise or in a central DMZ location for a multi-sited enterprise. The EIS can also be supported on a public cloud carrying publicly available information for the different enterprises and can also support data isolation for specific enterprises supporting authenticated access.

6.1.1 Enterprise local server (ELS)

An EIS Server deployed within the confines of the enterprise network is an Enterprise Local Server (ELS). To address security and potential ease of deployment based on the enterprise, the database is hosted within the Enterprise Network as ELS. The UE's authenticated connectivity to the enterprise is used as an implicit security measure to allow access to the Enterprise Information stored in the ELS.

Example of ELS is a MDM server, which is managed by the enterprise IT and can be customized to the specific EUD to which the Enterprise Information needs to be delivered. See Appendix C.

6.1.2 Enterprise central server (ECS)

An EIS Server deployed in a public cloud accessible to the UE through the public Internet is an Enterprise Central Server (ECS). The UE is provisioned with credentials to access the ECS when the specific Enterprise Information needs to be delivered only to authorized EUDs. Enterprise Information associated with one or more enterprises can be stored in a given ECS. When the Enterprise Information for a given network deployment is publicly available, any EUD is allowed access without specific authentication.

Example of ECS is OTA Update server associated with the SIM credential provisioned in the EUD for a given enterprise. See Appendix C.

6.2 Enterprise Information Service Client (EIS Client)

This section provides a description of the generic approach of the EIS client and EIS Server interactions and also identifies specific viable market realizations. Other possible solutions can be achieved as well based on the operators and vendors involved in a given deployment and this specification does not restrict any such realizations in the market.

A given EUD supports a EIS Client to access the EIS Server (ELS or ECS) to receive the Enterprise Information. The EIS Client can access a ELS deployed in the private cloud while connected within the Intranet of the specific Enterprise Network. The UE can access a ECS deployed in the public cloud from anywhere it has connectivity to the public Internet to receive information on one or more Enterprise Networks.

The Enterprise Information can be provided to the EUD by any proprietary methods deemed to be suitable by the Enterprise IT. The Enterprise IT / proprietary aspects are not in the scope of this technical specification.

The interaction between the UE and Enterprise Information Server can be based on the *EnterpriseInformationRequest* and *EnterpriseInformationResponse* procedures.

A UE sends the *EnterpriseInformationRequest* to the EIS providing a list of Enterprise Identifiers and optionally include its current GPS location information. The Enterprise Information Server responds to the request with *EnterpriseInformationResponse* providing the geofencing and enterprise deployment information as defined in Section 4.1. When the UE has not included its location information, the EIS server provides a subset or the full information associated with the enterprise. If the UE has provided its location information, the EIS Server optimizes the information provided to the locale indicated by the UE.

Figure 6-2 provides a high level sequence of messages exchanges between the UE and ELS / ECS. A mutual authentication, if required is performed to ensure the access to the Enterprise Information is provided only the required UEs and also only via the authorized servers. The *EnterpriseInformationRequest* is sent by the UE providing the enterprise identifier and its current location. The Enterprise Identifier can be excluded when the enterprise itself is implicitly identified based in the UE's domain of operation or based on specific UE identification (e.g., IMSI) that is used to recognize the associated enterprise. In such scenarios, the SIM profile will not be provisioned with the enterprise identifier.

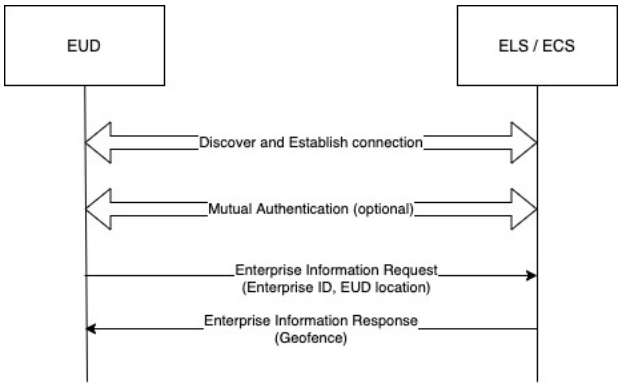

Figure 6-2: Enterprise Information Service Message Exchange

7 Enterprise Database High Level Schema

Figure 7-1 provides a representation of the Private CBRS / Non-Public network database high level schema supporting Enterprise Information. The information supported in the database schema supports including geofencing, enterprise deployment identifiers, and enterprise policy information. The database is structured to allow for multiple geofence areas to be specified per Private CBRS / Non-Public network. A given enterprise can have roaming agreements with other enterprise networks. The information associated with the home and roaming enterprise partners is specified in the database.

Within each instance of a geofence, multiple sites can be specified. Associated with each site, one or more of the geofence information is accommodated. The geofence information can be specified as geo shapes information, and as MNO network RF footprint based on e.g., coverage information and Private CBRS / Non-Public network RF deployment information.

The geolocation information can be specified as a 'Ellipsoid Points with Uncertainty Circle' or a 'Polygon'. The RF footprint information can be specified as 'Cell-ID', and 'signal strength'. The Cell-ID(s) are assumed to be in the proximity of the campus. One or more of the RSRP values of the active and candidate MNO Cell-IDs Radio Footprint can be used as entry point into the campus. Note that the individual signatures are retained independently to allow for recognizing multiple entry points into the camps.

The Private CBRS / Non-Public network RF deployment information is specified providing the type of CBSD (indoor and outdoor) and the CBSD identifiers.

It is expected that most if not all Private CBRS / Non-Public networks make available its Enterprise Information.

All information used for Geofence could change, therefore the Enterprise Information in the device might become outdated and required to be refreshed. Handling the process of information change is out of the scope of this document.

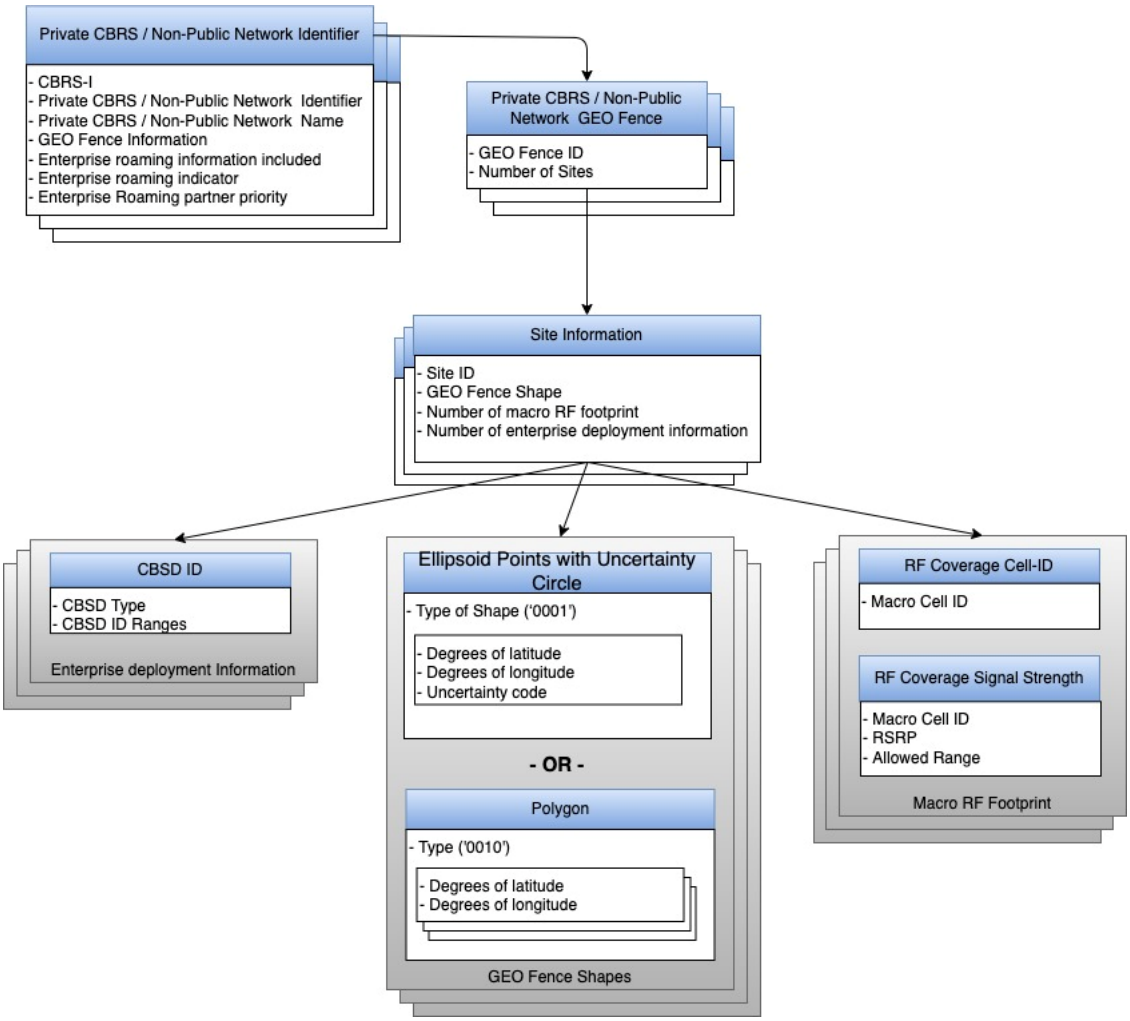

Figure 7-1: Private CBRS / Non-Public network Database High Level Schema

8 Enterprise information message payload and parameter definition

This section details the information exchange between the server and the UE to providing the enterprise (Private CBRS / Non-Public network) related information to the UE. Note that the support of the UE receiving Private CBRS / Non-Public network information and any specific processing based of the received Private CBRS / Non-Public network information is entirely optional for both the deployed Private CBRS / Non-Public network networks and the UE.

The UE provides this request information and optionally provides the Private CBRS / Non-Public network identifier, the UE location, and the MNO subscription supported. The UE can request information for one or more Private CBRS / Non-Public networks in the same request. If the server knows these attributes associated with a given UE, it implicitly caters the Private CBRS / Non-Public network information accordingly.

The UE provides the location information for the server to provide Private CBRS / Non-Public network information that is localized to the location indicated. Otherwise, information for all locations of the Private CBRS / Non-Public network is provided to the UE.

A specific site associated with an Private CBRS / Non-Public network network has coverage from one or more MNO networks. The UE based on the macro MNO network subscription enters the Private CBRS / Non-Public network campus via a specific macro network. Based on the macro MNO network subscription association, the RF footprint information for geofencing is provided to the UE. Otherwise all macro MNO footprint information is sent to the UE.

8.1 Enterprise Information Request Message

Table 8-1: Enterprise Information Request Message

Enterprise Info Request	R/O/C	Description
NAME: *nEnterprises* **DATA TYPE**: Unsigned Integer (8-bits)	Required	Number of Private CBRS / Non-Public Networks. Indicates the number of Private CBRS / Non-Public Networks included in the message.
NAME: *minVersionSupported* **DATA TYPE**: Unsigned Integer (8-bits)	Required	Minimum version supported Indicates the minimum version of the Private CBRS / Non-Public Network information format supported.
NAME: *maxVersionSupported* **DATA TYPE**: *deviceLocation*	Required	Maximum version supported Indicates the maximum version of the Private CBRS / Non-Public Network information format supported.

Enterprise Info Request	R/O/C	Description
NAME: *enterpriseInfoRequest* **DATA TYPE**: array of object: *EnterpriseInformationRequest* (The size of the array is *nEnterprises*)	Conditional	Array of *EnterpriseInformationRequest* data objects – see Section 8.1.1 for the format of the object. Each *EnterpriseInformationRequest* data object represents a request for information associated with an enterprise. Included when *nEnterprises* is greater than zero. The size of the array is *nEnterprises*, if it is included.

8.1.1 EnterpriseInformationRequest object

Table 8-2: *EnterpriseInformationRequest* Object Definition

Enterprise Information Request Object	R/O/C	Description
NAME: *CBRS-I* **DATA TYPE**: See subclause 10.5.5.36 [8]; *(3-bytes)*	Required	CBRS Identifier. This field is formatted as the last 3-bytes of PLMN Identifier as per subclause 10.5.5.36 [8].
NAME: *InformationIncluded* **DATA TYPE**: Unsigned *Integer (8-bits)*	Required	Each bit of this value determines which of the information are requested by the UE. • Bit 1: If it is "1" *enterpriseID* is included • Bit 2: If it is "1" *deviceLocation* is included • Bit 3: If it is "1" *MNOPLMNId* is included If all bits are "0", it means the network knows by other means (e.g. subscription) on the Private CBRS / Non-Public Network information to be provided to the UE. Bits 4-8 are reserved.
NAME: *enterpriseIDType* **DATA TYPE**: *(1-byte)*	Conditional	Private CBRS / Non-Public Network Id Type It is set to: • '0' to indicate 'Closed Subscriber Group' • '1' to indicate '3GPP NID' All other values are reserved. Included if Bit 1 of *InformationIncluded is equal to "1"*
NAME: *enterpriseID* **DATA TYPE**: • Closed Subscriber Group per Section 4.7 in [7] for LTE networks Or	Conditional	Private CBRS / Non-Public Network Identifier This is the Private CBRS / Non-Public Network Identifier associated with the Private CBRS / Non-Public Network credential. This information may be obtained from the SIM profile, if configured, associated with Private CBRS / Non-Public Network credentials.

Enterprise Information Request Object	R/O/C	Description
• 5GC-NID as defined in Section 5.3.3 of [3] for 5G NR SNPN networks *(Size is 11 hexadecimal digits)*		The 11-hexadecimal digits are formatted as • per Closed Subscriber Group as per Section 4.7 in [7] for LTE when *enterpriseIDType = '0'*. When Closed Subscriber Group is specified the lower order 27-bits are used and the higher order bits are set to zero. Or • 5GC-NID as defined in Section 5.3.3 of [3] for 5G NR SNPN networks when *enterpriseIDType = '1'.* Included if Bit 1 of *InformationIncluded is equal to "1"*
NAME: *deviceLocation* **DATA TYPE**: See section 7.3.1 in [5]; *(7-bytes)*	Conditional	Device location This field is specified per Section 7.3.1 in [5] providing the device longitude and latitude. Included if Bit 2 of *InformationIncluded is equal to "1"*
NAME: *nMNOPLMNId* **DATA TYPE**: Unsigned *Integer (8-bits)*	Conditional	Number of MNO PLMN-IDs Included if Bit 3 of *InformationIncluded is equal to "1"*
NAME: *MNOPLMNId* **DATA TYPE**: array of PLMN ID per subclause 10.5.5.36 [8]; (The size of the array is *nMNOPLMNId*)	Conditional	MNO PLMN Identifier. Each element of this array includes the last 3-bytes of PLMN Identifier as per subclause 10.5.5.36 [8], if *nMNOPLMNId* is greater than zero. This field provides the MNO subscription(s) in the UE that will be used as macro footprint to find the Private CBRS / Non-Public Network campus.

8.2 Enterprise Information Response Message Definition

Table 8-3: Enterprise Information Response Message

Enterprise Info Response	R/O/C	Description
NAME: *nEnterprises* **DATA TYPE**: Unsigned Integer (8-bits)	Required	Number of Private CBRS / Non-Public Networks. Indicates the number of Private CBRS / Non-Public Networks included in the message.
NAME: *enterpriseInformation* **DATA TYPE**: array of object: *EnterpriseInformation* (The size of the array is *nEnterprises*)	Conditional	Array of *EnterpriseInformation* data objects - see Section 8.3.1 for the format of the object. Each *EnterpriseInformation* data object represents information associated with an enterprise. Included when *nEnterprises* is greater than zero. This supports the Private CBRS / Non-Public Network information as specified in Section 8.3.

8.3 Enterprise information format

This section defines the format of the Enterprise Information associated with an Private CBRS / Non-Public Network Network. This information is provided to the UE. The UE can use this information for specific optimization for finding and camping on the Private CBRS / Non-Public Network Networks. The Enterprise Information should at least include geofencing information. Figure 8-1 provides a pictorial representation of the Private CBRS / Non-Public Network information format that is carried in the response message showing the nested structure. The Enterprise Information is encoded as information associated with each Private CBRS / Non-Public Network identifier (e.g. CBRS-I + CSG-ID) providing one or more geofence information. Associated with each geofence, one or more sites are specified, and for each site, a geofence shape is provided. The site information also optionally specifies the macro RF footprint and Private CBRS / Non-Public Network deployment information.

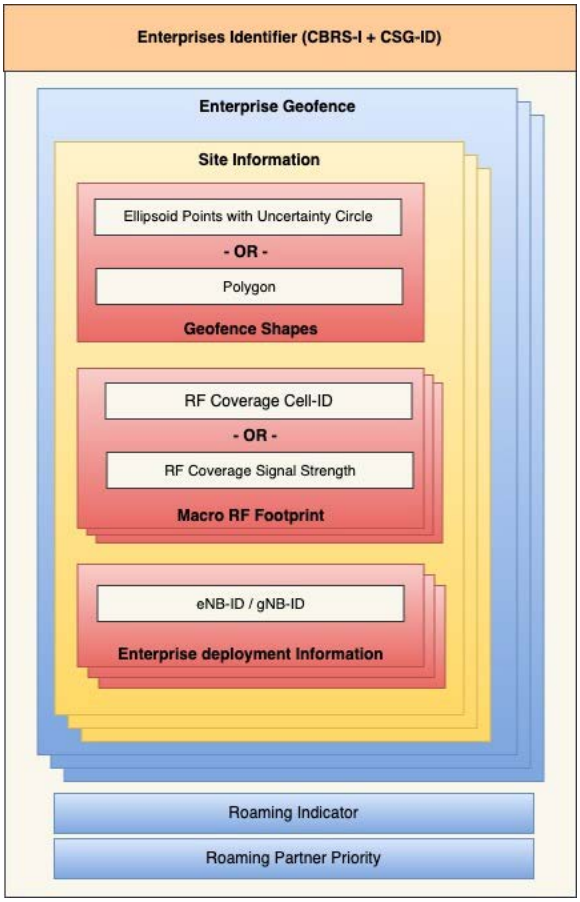

Figure 8-1: Private CBRS / Non-Public Network Information Format

8.3.1 *EnterpriseInformation* object

Note: Unless otherwise specified, all fields are supported in version '0'. Added, Modified, and deprecated fields are explicitly identified associated with the individual versions. When a field is added, modified, deprecated fields are introduced in a version, it applies to subsequent versions and do not apply to earlier versions.

Table 8-4: *EnterpriseInformation* object definition

Enterprise Information Object	R/O/C	Description
NAME: *enterpriseInfoVersion* **DATA TYPE**: Unsigned Integer (8-bits)	Required	Enterprise information version. Specifies the version of the Private CBRS / Non-Public Network information structure specified. The supported versions are '0' and '1'.
NAME: *CBRS-I* **DATA TYPE**: See subclause 10.5.5.36 [8]; (3-bytes)	Required	CBRS Identifier. This field is formatted as the last 3-bytes of PLMN Identifier as per subclause 10.5.5.36 [8];
NAME: *enterpriseIDType* **DATA TYPE**: (1-byte)	Required	Enterprise Id Type It is set to: • '0' to indicate 'Closed Subscriber Group' • '1' to indicate '5GC-NID' • All other values are reserved.
NAME: *enterpriseID* **DATA TYPE**: • Closed Subscriber Group per Section 4.7 in [7] for LTE networks Or • 5GC-NID as defined in [3] Section 5.3.3for 5G NR SNPN networks (11 hexadecimal digits)	Required	Enterprise Identifier It is an identifier associated with a given Private CBRS / Non-Public Network. This is the unique Private CBRS / Non-Public Network Identifier acquired by an entity to reference an Private CBRS / Non-Public Network deployment. See section 5. The 11-hexadecimal digits are formatted as • per Closed Subscriber Group as per Section 4.7 in [7] for LTE when *enterpriseIDType* = '0'. When Closer Subscriber Group is specified the lower order 27-bits are used and the higher order bits are set to zero. • 5GC-NID as defined in [3] Section 5.3.3 for 5G NR SNPN networks when *enterpriseIDType* = '1'.
NAME: *enterpriseNameLength* **DATA TYPE**: Unsigned Integer (8-bits)	Required	Enterprise name length. Indicates the length of the Private CBRS / Non-Public Network name.
NAME: *enterpriseName* **DATA TYPE**: string	Conditional	Enterprise Name. Included only when the *PrivateCBRSNon-PublicNetworkNameLength* is greater than zero. This provides the Private CBRS / Non-Public Network name. This name when specified, is used to match against the name broadcasted on SIB9 from an Private CBRS / Non-Public Network CBSD. This field is populated with the Private CBRS / Non-Public Network Identifier converted to a text string.

Enterprise Information Object	R/O/C	Description
NAME: *nGeofenceInformation* **DATA TYPE**: Unsigned Integer (8-bits)	Required	Number of geofence information Provides the number of GEO fences included in this message.
NAME: *geofenceInformation* **DATA TYPE**: array of object: *GeofenceInformation* (The size of the array is *nGeofenceInformation*)	Conditional	Array of *GeofenceInformation* data objects - see Section 8.3.2 for the format of the object. Each *GeofenceInformation* data object represents geofence information associated with an Private CBRS / Non-Public Network. Included when *nGeofenceInformation* is greater than zero.
NAME: *enterpriseRoamingInfoIncluded* **DATA TYPE**: boolean	Required	Enterprise Roaming Information Included This field is introduced in version 1. When set to 'True', it Indicates the fields *enterpriseRoamingIndicator* and *enterpriseRoamingPartnerPriority* are included. When set to 'False', it Indicates the fields *enterpriseRoamingIndicator* and *enterpriseRoamingPartnerPriority* are not included. When set to 'False', it implicitly indicates that the information provided is for 'Home' enterprise network.
NAME: *enterpriseRoamingIndicator* **DATA TYPE**: boolean	Optional	Enterprise Roaming Indicator Included when *enterpriseRoamingInfoIncluded* = 'True'. This field is introduced in version 1. When set to 'False', it Indicates a 'Home' enterprise network. When set to 'True', it indicates a 'Roaming' enterprise partner network.
NAME: *enterpriseRoamingPartnerPriority* **DATA TYPE**: (1-byte)	Optional	Enterprise Roaming Partner Priority Included when *enterpriseRoamingInfoIncluded* = 'True'. This field is introduced in version 1. Allowed values are 0x01 through 0x0F indicating the priority levels of the enterprise roaming partner, where 0x01 is the highest priority and it reduces in priority with subsequent increments with 0x0F as the lowest priority. The remaining values are reserved. This priority field is used to arbitrate network camping decisions only when there are multiple enterprise roaming partner networks available in a given vicinity.

Enterprise Information Object	R/O/C	Description
		When the relative priority of the across the enterprise roaming partners is already defined by the PLMN list associated with the enterprise credential, the priority specified by this field is ignored and the relative priority specified in the PLMN list takes precedence.

8.3.2 GeofenceInformation object

Table 8-5: GeofenceInformation object definition

Enterprise Geofence	R/O/C	Description
NAME: *geofenceId* **DATA TYPE**: Unsigned Integer (32-bits)	Required	Geofence Identifier. Provides the GEO fence identifier associated with the GEO fence.
NAME: *nSiteLocations* **DATA TYPE**: Unsigned Integer (16-bits)	Required	Number of Site Locations. Provides the number of sites associated with the Geofence identifier.
NAME: *siteInformation* **DATA TYPE**: array of object: *SiteInformation* (The size of the array is *nSiteLocations*)	Conditional	Array of *SiteInformation* data objects - see Section 8.3.3 for the format of the object. Each *SiteInformation* data object represents site information associated with an Private CBRS / Non-Public Network. Included when *nSiteLocations* is greater than zero.

8.3.3 SiteInformation object

Table 8-6: *SiteInformation* object definition

Enterprise Site Information	R/O/C	Description
NAME: *siteLocationId* **DATA TYPE**: Unsigned Integer (16-bits)	Required	Site locations identifier. Provides the identifier associated with the site.
NAME: *geofenceShapeInfo* **DATA TYPE**: • Per Section 7.3.2 in [5] for Ellipsoid Point with uncertainty Circle. (8-bytes) Or	Required	Geofence shape information This field is formatted as per • Section 7.3.2 in [5] for a single “Ellipsoid Points with Uncertainty Circle” Or • Section 7.3.4 in [5] for “Polygon”.

Enterprise Site Information	R/O/C	Description
• Per Section 7.3.4 in [5] for Polygon. (1-byte + 6*n where n is the number of points in the polygon)		
NAME: *nMacroRFFootprintInfo* **DATA TYPE**: Unsigned Integer (16-bits)	Required	Number of Macro RF Footprint Information. Provides the number of macro RF footprint information associated with the site id.
NAME: *macroRFFootprintInformation* **DATA TYPE**: array of object: *MacroRFFootprintInformation* (The size of the array is *nMacroRFFootprintInfo*)	Conditional	Array of *MacroRFFootprintInformation* data objects – see Section 8.3.4 for the format of the object. Each *MacroRFFootprintInformation* data object represents macro RF footprint information associated with an Private CBRS / Non-Public Network site. Included when *nMacroRFFootprintInfo* is greater than zero.
NAME: *nEnterpriseDeploymentInfo* **DATA TYPE**: Unsigned Integer (16-bits)	Required	Number Enterprise Deployment Information Provides the number of Private CBRS / Non-Public Network deployment information associated with the site id.
NAME: *enterpriseDeploymentInformation* **DATA TYPE**: array of object: *EnterpriseDeploymentInformation* (The size of the array is *nEnterpriseDeploymentInfo*)	Conditional	Array of *EnterpriseDeploymentInformation* data objects – see Section 8.3.6 for the format of the object. Each *EnterpriseDeploymentInformation* data object represents macro RF footprint information associated with an Private CBRS / Non-Public Network site. Included when *nEnterpriseDeploymentInfo* is greater than zero.

8.3.4 *MacroRFFootprintInformation* object

Table 8-7 provides the types of RF footprint information that can be used to define the location of an Private CBRS / Non-Public Network system.

Table 8-7: RF Footprint Type Values

RF Footprint Type	Value
Cell-ID Based	0
Signal-Strength Based	1
Reserved	All other values

Table 8-8: *MacroRFFootprintInformation*-Cell-Id object definition

RF Footprint Information	R/O/C	Description
NAME: *rfFootprintType*	Required	RF Footprint Type.

RF Footprint Information	R/O/C	Description
DATA TYPE: Unsigned Integer (8-bits)		Set to '0' to indicate Cell-ID based.
NAME: *macroPLMNId* **DATA TYPE**: See subclause 10.5.5.36 [8]; (3-bytes)	Required	PLMN identifier. This field is formatted as the last 3-bytes of PLMN Identifier as per subclause 10.5.5.36 [8];
NAME: *nCellId* **DATA TYPE**: Unsigned Integer (8-bits)	Required	Number of cell identifier. Number of Cell-IDs included.
NAME: *cellId* **DATA TYPE**: array of Cell ID (The size of the array is *nCellId*)	Conditional	Cell-Identifier. Included if *nCellId* is greater than zero. Size each Cell-ID is 28-bits. Identifies the Cell-IDs of the MNO network. When the UE enters any one of these cells, it can search for available Private CBRS / Non-Public Network Network.

Table 8-9: *MacroRFFootprintInformation*-SignalStrength object definition

RF Footprint Information	R/O/C	Description
NAME: *rfFootprintType* **DATA TYPE**: Unsigned Integer (8-bits)	Required	RF Footprint Type. Set to '1' to indicate signal strength based.
NAME: *macroPLMNId* **DATA TYPE**: See subclause 10.5.5.36 [8]; (3-bytes)	Required	Macro PLMN identifier. This field is formatted as the last 3-bytes of PLMN Identifier as per subclause 10.5.5.36 [8];
NAME: *nCellIdWithRSRPRange* **DATA TYPE**: Unsigned Integer (8-bits)	Required	Number of cell identifier with RSRP range Number of Cell-IDs with RSRP range included.
NAME: *cellIdRSRPRange* **DATA TYPE**: array of object: *CellIdRSRPRange* (The size of the array is *nCellIdWithRSRPRange*)		Array of *CellIdRSRPRange* data objects – see Section 8.3.5 for the format of the object. Each *CellIdRSRPRange* data object represents macro RF footprint information associated with an Private CBRS / Non-Public Network site. Included when *nCellIdWithRSRPRange* is greater than zero.

8.3.5 *CellIdRSRPRange* object

Table 8-10: *CellIdRSRPRange* object definition

CellIdRSRPRange object	R/O/C	Description
NAME: *cellId* **DATA TYPE**: (28-bits)	Required	Cell identifier. Cell-IDs of the MNO network.

CellIdRSRPRange object	R/O/C	Description
		When the UE enters measures the RSRP signal strength of these cells to be within the specified range, it can search for available Private CBRS / Non-Public Network Network.
NAME: *cellRSRP* **DATA TYPE**: (12-bits)	Required	Cell RSRP (Reference Signal Received Power). Provides the signal strength of the associated Cell-ID for which the device is to consider itself to be in the GEO Fence. Values are in the range INTEGER (0..97)
NAME: *allowedRSRPRange* **DATA TYPE**: (4-bits)	Required	Allowed RSRP Range. Specifies the +/- range of the signal strength relative to the CELL_RSRP that the device is to consider itself to be in the GEO Fence. Values are in the INTEGER (0..16) and treated against the digitized scale of (0..97). The values below 0 and above 97 are ignored when applying the range.

8.3.6 *EnterpriseDeploymentInformation* object

Table 8-11 provides the types of enterprise deployment information that can be used to define the specific details of the deployment of an Private CBRS / Non-Public Network system.

Table 8-11: Enterprise Deployment Information Type Values

Enterprise Deployment Information Type	Value
CBSD Information	0
Reserved	All other values

Table 8-12: *EnterpriseDeploymentInformation* object definition

Enterprise CBSD Information	R/O/C	Description
NAME: *InformationIncluded* **DATA TYPE**: Unsigned Integer (8-bits)	Required	Each bit of this value determines which of the information is included. • Bit 1: If it is "1" *enterpriseDeployedCellInformation* is included • Bit 2: If it is "1" *MNOPLMNId* is included • Bits 3-8 are reserved.
NAME: *nEnterpriseDeployedCellId* **DATA TYPE**: Unsigned Integer (8-bits)	Conditional	Number of enterprise deployed cell identifier. Number of Cell-IDs included. Included if Bit 1 of *InformationIncluded* is equal to "1"

Enterprise CBSD Information	R/O/C	Description
NAME: *enterpriseDeployedCellInformation* **DATA TYPE**: array of object: *EnterpriseDeployedCellInformation* (The size of the array is *nEnterpriseDeployedCellId*)		Array of *EnterpriseDeployedCellInformation* data objects – see Section 8.3.7 for the format of the object. Each *EnterpriseDeployedCellInformation* data object represents macro RF footprint information associated with an Private CBRS / Non-Public Network site. Included when *nEnterpriseDeployedCellId* is greater than zero and if Bit 1 of *InformationIncluded* is equal to "1"
NAME: *nMNOPLMNId* **DATA TYPE**: Unsigned Integer (8-bits)	Conditional	Number of MNO PLMN-IDs Included if Bit 2 of *InformationIncluded* is equal to "1"
NAME: *MNOPLMNId* **DATA TYPE**: array of PLMN ID per subclause 10.5.5.36 [8]; (3-bytes) (The size of the array is *nMNOPLMNId*)	Conditional	MNO PLMN Identifier. This field is formatted as the last 3-bytes of PLMN Identifier as per subclause 10.5.5.36 [8] if *nMNOPLMNId* is greater than zero and if Bit 2 of *InformationIncluded* is equal to "1" This field provides the MNO subscription(s) in the UE that will be used as macro footprint to find the Private CBRS / Non-Public Network campus.

8.3.7 *EnterpriseDeployedCellInformation* object

Table 8-13: *EnterpriseDeployedCellInformation* object definition

Enterprise Deployed Cell Information object	R/O/C	Description
NAME: *enterpriseDeployedCellType* **DATA TYPE**: Unsigned *Integer (8-bits)*	Required	Enterprise Deployed Cell Type • Set to '0' to indicate CAT-A Indoor CBSD. • Set to '1' to indicate CAT-A Outdoor CBSD. • Set to '2' to indicate CAT-B Outdoor CBSD. All other values are reserved.
NAME: *cellIdSize* **DATA TYPE**: Unsigned *Integer (8-bits)*	Required	Cell Identifier Size Specifies the size in bits of the Cell-ID information included. The maximum value is 28-bit. When a value less than 28-bits is specified, it refers to all the 28-bit CBSD-IDs that can be with the specified Cell-ID as the MSB.
NAME: *cellId* **DATA TYPE**: *cellIdSize bits*	Conditional	Cell Identifier Specifies the MSB of the Cell-IDs of Private CBRS / Non-Public Network CBSD campus deployments.

9 Enterprise Identifier population in the SIM credential

The Enterprise Identifier may be specified in the SIM profile. The 'CSG ID' or 'VendorSpecificExtension' is leveraged to include the Enterprise Identifier information in it as part of the SIM profile. Given that a single credential may be applied to one or more enterprise deployments, both the CSG-ID and VendorSpecificExtension is supported as a list of entries containing the Enterprise Identifier information.

9.1 CSG-ID definition in the SIM credential

See [6] for the details of the CSG configuration. A specifics for the SIM provisioning to include the CSG-ID is provided below.

See Figure 4.2 in [6] for file identifiers and directory structures of USIM. The snippet showing the Home Node B information is copied in here for reference.

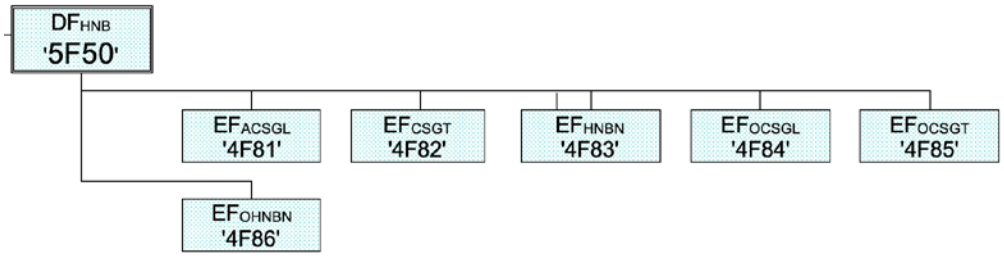

Figure 9-1: HNB relevant EF in USIM

See Section 4.4.6 in [6] for the contents of files at the DF HNB level including the relevant EFs.

It is recommended that *Service n°90* "*Operator CSG Lists and corresponding indications*" is used to specify the CSG information. EF_{OCSGL} (*Operator CSG Lists*), EF_{OCSGT} (*Operator CSG Type*), and EF_{OHNBN} (*Operator Home NodeB Name*) are used by *Service n°90* and is recommended these three EFs be used to configure the CSG information.

Details of DF_{HNB} provisioning is provided below:

- EF_{OCSGL} (See 4.4.6.5 in [6]) :
  - PLMN Tag (e.g., set to the SHNI (315-010)) {Only one PLMN ID is allowed}
  - A single CSG-ID is included. 'CSG ID' is set to the 'CBRS NID' that will be purchased for each Enterprise entity. CSG-ID must be defined as per 3GPP TS 23.003: it must be fix length 27 bit value.
  - This EF has tags to EF_{OCSGT} and EF_{OHNBN} that need to be mandatorily specified.
- EF_{OCSGT} (See 4.4.6.6 in [6]) :
  - Allows for including a custom type information. Include a text string "Private ENT" in this field.
- EF_{OHNBN} (See 4.4.6.6 in [6]) :
  - Allows for including a home node B name. Include a text string converting the CSG-ID field to text and include it in this field. The information is intended to be matched with the CBSD SIB9 broadcast by the UE.

9.2 VendorSpecificExtension definition in the SIM credential

For eSIMs , content of Vendor Specific extension within eSIM Metadata may be used as specified by GSMA SGP.22 [9] as -

```
serviceSpecificDataStoredInEuicc [34] VendorSpecificExtension OPTIONAL, -- Tag 'BF22'
```

If the eSIM Metadata is used , the following data structure shall be used to configure the Enterprise and network information.

9.2.1 ASN.1 Definition of VendorSpecificExtension

The tag 'BF22' VendorSpecificExtension in the eSIM metadata shall be implemented using following ASN.1 data structure, if it is included.

```
-- ASN1START
CBRSNetworkInfo ::= SEQUENCE
{
    cbrsNid             [0] OCTET STRING (SIZE (1..20)), -- Tag '80'
    enterpriseName      [1] OCTET STRING (SIZE (1..20)) OPTIONAL, -- Tag '81'
    proprietaryData     [2] OCTET STRING (SIZE (1..32)) OPTIONAL -- Tag '82'
}
PrivateNetworkInfo ::= SEQUENCE OF CBRSNetworkInfo
    VendorSpecificExtension ::= [34] SEQUENCE OF SEQUENCE { -- Tag 'BF22'
    vendorOid           [0] OBJECT IDENTIFIER, -- OID of OnGo Alliance Or Network/Service
Provider Tag '80'
    vendorSpecificData [1] SEQUENCE
    {
        privateNetworkInfo PrivateNetworkInfo
    }
}
-- ASN1STOP
```

Note:

1. VendorSpecificExtension is recommended to use sequence of size 1.
2. OnGoA OID is not available at this time, rather the use of Network/Service Provider OID is recommended.

Example:

```
BF 22 32 30 30 80 07 2B 06 01 04 01 DC 0F A1 25 A0 23 30 21 80 04 00 00 05 BF 81 12
43 65 6C 6F 6E 61 20 50 72 69 76 61 74 65 20 4C 54 45 82 05 12 34 56 78 90
```

ASN.1 Parsed data:

PDU Name/Identifier	Value	Typereference	Built-in Type	Default Val	Constraints	Offset	Length
VendorSpecificExtension	1	VendorSpecificExtension	SEQUENCE OF			0	53
1			SEQUENCE			3	50
vendorOid	{ 1 3 6 1 4 1 11791 }		OBJECT IDENTIFIER			5	9
vendorSpecificData			SEQUENCE			14	39
privateNetworkInfo	1	PrivateNetworkInfo	SEQUENCE OF			16	37
CBRSNetworkInfo 1		CBRSNetworkInfo	SEQUENCE			18	35
cbrsNid	'000005BF'H		OCTET STRING		(SIZE(1..20))	20	6
enterpriseName	'43656C6F6E61205072697...		OCTET STRING		(SIZE(1..20))	26	20
proprietaryData	'1234567890'H		OCTET STRING		(SIZE(1..32))	46	7

Figure 9-2: ASN.1 Parsed Data

9.2.2 VendorSpecificExtension definition in the SIM credential

LPA per GSMA SGP.22 [9] application hosted on UE should execute GetProfilesinfo per GSMA SGP.22[9] as and when needed to fetch the metadata information about eSIM(s). Upon detection of VendorSpecificExtension, LPA may parse and pass information appropriate UE component for further processing of NID , Enterprise Name and Enterprise Additional Data.

9.2.3 Conditions of when eSIM Metadata is used –

If UE does not support eUICC i.e pluggable SIM only with no eSIM supported, use of CSG-ID per Section 9.1 is recommended.

If the eSIM Metadata option is used by the operator, then the SMDP+ per GSMA SGP.22 [9] shall support the metadata-data structure when enterprise identifier is included as part of the Private CBRS / Non-Public Network subscription.

9.3 Coexistence of CSG-ID and vendor specific option

The CSG-ID support with LTE in the SIM credential definition will need to be continued for legacy UE implementations. This approach of enterprise identifier association with the credential is employed for LTE/EPC operations.

The VendorSpecificExtension providing enterprise identifier may be employed as an alternative method for delivering the same information. At some point in the future, when LTE/EPC operations is phased out and only NR / 5GC operations is required to be supported, the CSG-ID provisioning is no longer required.

If UE supports eUICC according to GSMA SGP.22 [9] and also implements handing of CSG-ID per TS 1004, for eSIM use cases, UE/LPA may consider VendorSpecificExtension from metadata and discard CSG-ID.

10 UE and Network based solutions for Tracking Area Code(TAC) collisions

10.1 Introduction

CBRSA-TS-1002 Section 5.3.7 [3] provides the recommended TAC ranges to be employed based on the acquired IBNs when using the SHNI. The Tracking Area Code used for deployments is selected by the operator and is not monitored by the CBRS Alliance. To avoid denial of service scenarios, nearby LTE networks using the SHNI require unique TACs.

A denial of service scenario for the UE can occur when it visits two LTE networks that employ the same TAC, one without valid credentials and other with valid credentials, is visited by the UE in a short duration of time. It is possible for a UE to attempt to register in a tracking area in which its not authorized for services given the use of SHNI for system camping purposes. This would lead to a rejection of the registration attempt with EMM cause#15 (Section 5.5.3.1 of CBRSA TS-1002 [3]). Upon receiving the rejection with EMM cause#15, the UE would include the TAI in its list of forbidden TAIs and not enter any networks including the preferred enterprise networks that match with the forbidden list. The relevant UE procedures for forbidden TAI are defined in 3GPP TS 24.301 [4], Section 5.3.2.These TAC collision scenarios leading to UE experiencing a denial of service are difficult to detect and troubleshoot.

10.2 TAC Collision: Mitigation and resolution proposals

The information associated with a given private network including geofencing and deployment related aspects provided to the UE to optimally find and attempt camping only on preferred networks is addressed in the other early sections of this specification. This section addresses UE procedures to enable find the preferred networks using the deployment information provided and avoid other networks, which minimizes / prevent the denial of service issues from occurring.

The deployment information currently optionally includes enterprise name and eNB ID and the UE procedures to leverage this provisioned information is discussed in the sections below.

10.2.1 Enterprise name UE based solution

See Section 9 for details on Enterprise Name provisioned along with the SIM credential.

The enterprise deployed eNBs should be deployed as Hybrid CSG Cells as per 3GPP TS 36.331 [10] with the Enterprise Name populated as the Home eNodeB name. This allows for the UE to obtain the Enterprise Name from the enterprise deployed eNBs through SIB broadcast.

During cell selection/re-selection procedures the UE may use the Enterprise Name if provided to determine whether a registration attempt could be performed. The UE may attempt registration if both the conditions below are fulfilled:

- Combination of TAC and Enterprise Name are not part of forbidden TAI list.

  And

- CBRS network Name provided (received over SIB9) matches the CBRS Network Name the UE is provisioned for.

Note: UE enhancements are required to perform the matching with the provisioned Enterprise Name with the SIM credential and eNB SIB broadcasts prior to camping.

10.2.2 Macro eNB ID UE based solution

UE is provisioned with an allowed list of ECGIs that are employed in the enterprise campus where the UE has valid subscriptions as part of the Enterprise Information. The ECGI is composed of the SHNI, a Macro eNB ID and Cell-Identity. The Cell-Identity is freely assigned by the individual operator while the Macro eNB ID(20bits) is allocated by the CBRSA [1]. The UE may also learn the information of the preferred ECGIs for camping on its own and use that as the allowed set of ECGIs.

During cell selection/re-selection procedures the UE may use the allowed set of ECGI provisioned with the SIM credential and match it with the information broadcasted from the enterprise network prior to attempting registering with the network.

Note: UE enhancements are required to perform the matching with the provisioned ECGIs associated with the SIM credential and eNB SIB broadcasts prior to camping.

Appendix A (Informative): Method of geofencing information population in the Enterprise Information Server

Geofencing information supported in the Enterprise Information for enterprises enable the UE to optimally find and camp on Enterprise Networks. Allowing for most if not all enterprises to provide its geofencing information allows for ensuring the ecosystem of vendors support available for market deployments. To enable this, a simple approach of deriving the geofence information based on the GPS information of the deployed CBSD on the enterprise campus is suggested – see Method 1A below. A more sophisticated approaches with Method 1B and Method 2 are suggested as well.

In order to minimize the amount of the information provided to the UE, one of more of the below identified methods can be employed.

For enterprises with multiple sites, the information can be recorded on a site basis and the information made available to the UE. The UE can be provided all the information associated with the enterprise or optimized to have information associated with specific locales. The UE can provide its current location, which can be used to optimize the Enterprise Information provided to the UE.

Method 1A

- Use the GPS information of the deployed CBSDs to determine a combined representation of a set of {center, radius} - ideally a single entry OR as a segmented linear polygon
- Note that CBSDs are allowed a +/- 50m horizontal and +/- 3m vertical error in the GPS location. Most deployments are much finer in defining the CBSD GPS location. A number representing the expected error in the GPS information is also provided as part of the deployment and used to manage this geofence definition

Method 1B

- Collect the GPS locations of the campus extremities and unify them into a set of segmented linear polygons.

Method 2

- As part of the enterprise deployment process, collect the Radio Footprint of the SP networks' set of channels and Cell-IDs and optionally include the RSRP range of the individual cells.
- There are several points on campus where this information is collected, ideally along the extremities / entry points of the campus. This information is unified to have a set of SP network pilots along with their RSRP ranges

Appendix B (Informative): Sample flow chart of UE search and camping behavior for an enterprise system

Figure A-1 addresses Sample flow chart describing UEs behavior scanning for Enterprise Networks. The actual realization is left to the UE implementation.

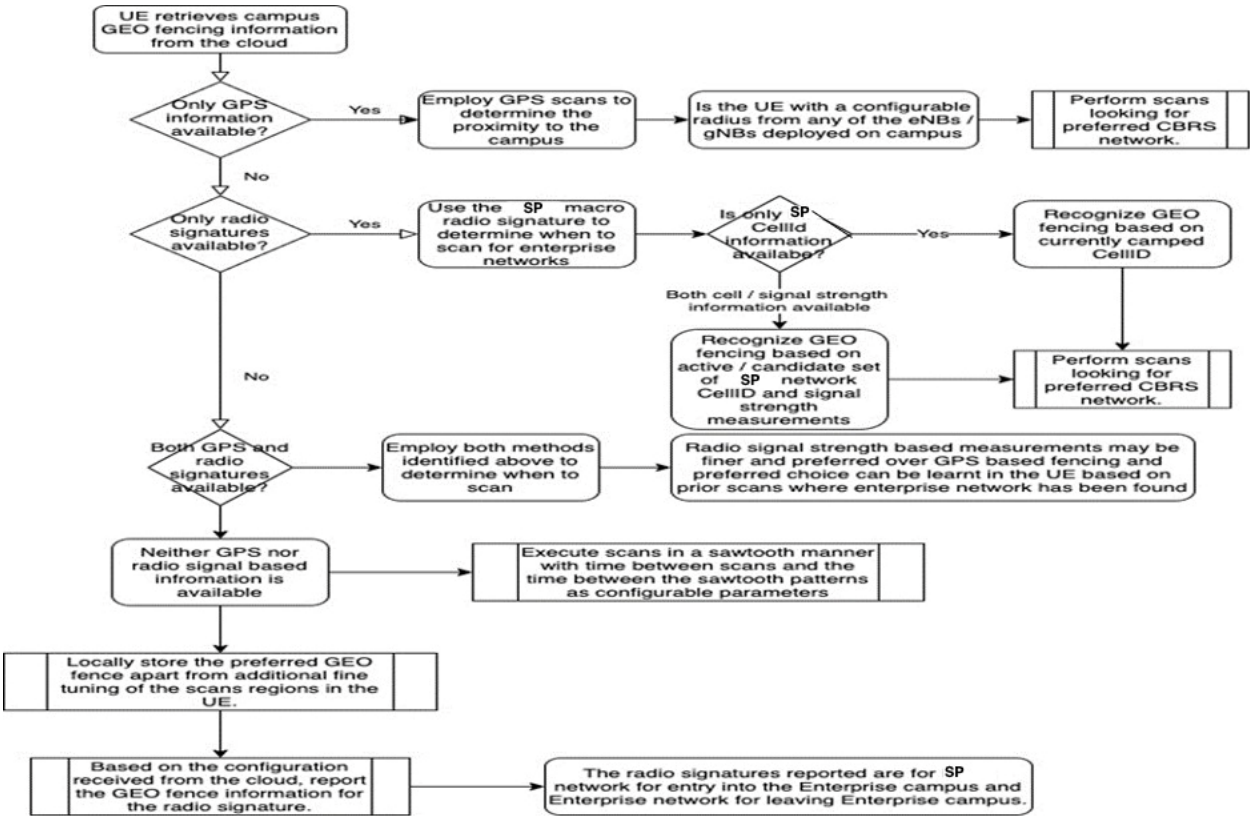

Figure A-1: Sample flow chart describing UEs behavior scanning for Enterprise Networks

Appendix C (Informative): Enterprise Information provisioning on the UE

This appendix provides potential methods that can be employed to deliver the Enterprise Information to the UE.

C.1 Mobile Device Management (MDM)

For CYOD (Choose your own device) managed by the enterprise IT, the device provisioning is managed through MDM procedure. There are several vendors that provide MDM solutions for enterprise device management supplied to the enterprise IT. These solutions are further catered to specialized procedures that are custom defined by each UE OEM. MDM solutions allow for the enterprise IT to configure the individual devices with the required operational configurations including the device subscription to access connectivity to the enterprise deployed network.

As part of the credential provisioning, the Enterprise Information object including the geofencing information as defined by the specification could be optionally provisioned on to the device and associated with the enterprise access connectivity subscription. The information could be stored any secure location on the device including the SIM provisioning platform. This procedure could also employ the procedures defined in Section C.2 using OTA Update procedures to provision the UE with the Enterprise Information.

C.2 OTA Update

OTA Update Server can be leveraged to implement solution which delivers geofencing payload over a secure OTA connection with xUICC using OTA HTTP protocol as specified in Global Platform Amendment B [11] and payload format in ETSI 102.226 [12].

Geofencing Payload can be delivered UICC over RFM (Remote File Management) Or RAM (Remote Applet Management) depending on implementation. A Javacard Applet on the xUICC could be implemented to proactively reach to remote server on different events and request for geofencing payload.

Figure A-2 provides a high level sequence of messages exchanges between the UE and OTA server and Geofencing server.

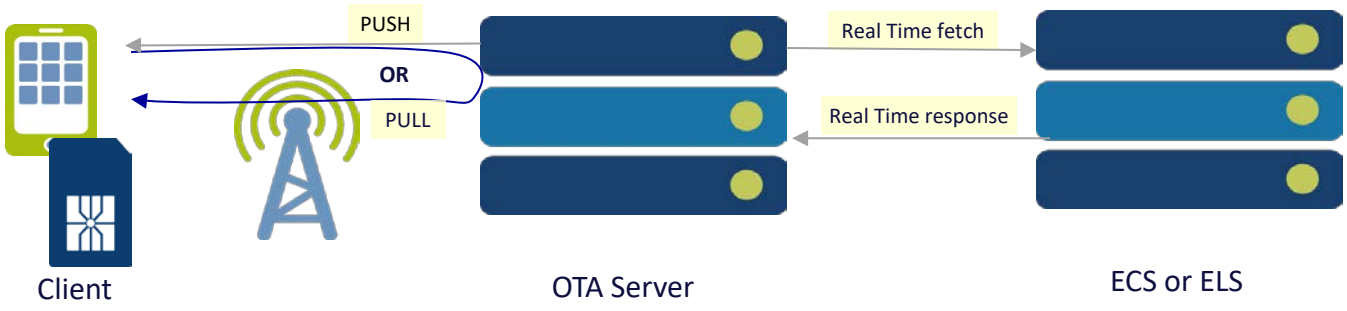

Figure A-2: Message exchanges between the UE and OTA server and Geofencing server.

Appendix D (Informative): MDT based TAC Collision detection

This is an informative annex and proposes the use of 3GPP MDT framework to enable network detection and mitigation of TAC collisions.

The current 3GPP behavior is for the UE to collect information on a PLMN basis and report the collected metric to the same PLMN network when there is information to report.

UEs are provisioned with the capability to collect and report information on the cells along with the associated TAIs where the rejection took place as part of the MDT procedure. The UE is also provided restrictions by indicating the Cell-IDs and TAIs of interest for which the rejection related information needs to be collected. An exemplary call flow is provided in Figure A-3.

The UE reports the information collected each time it successfully reenters the UE's associated enterprise network. The enterprise network employs the retrieved information for TAI re-configuration as needed.

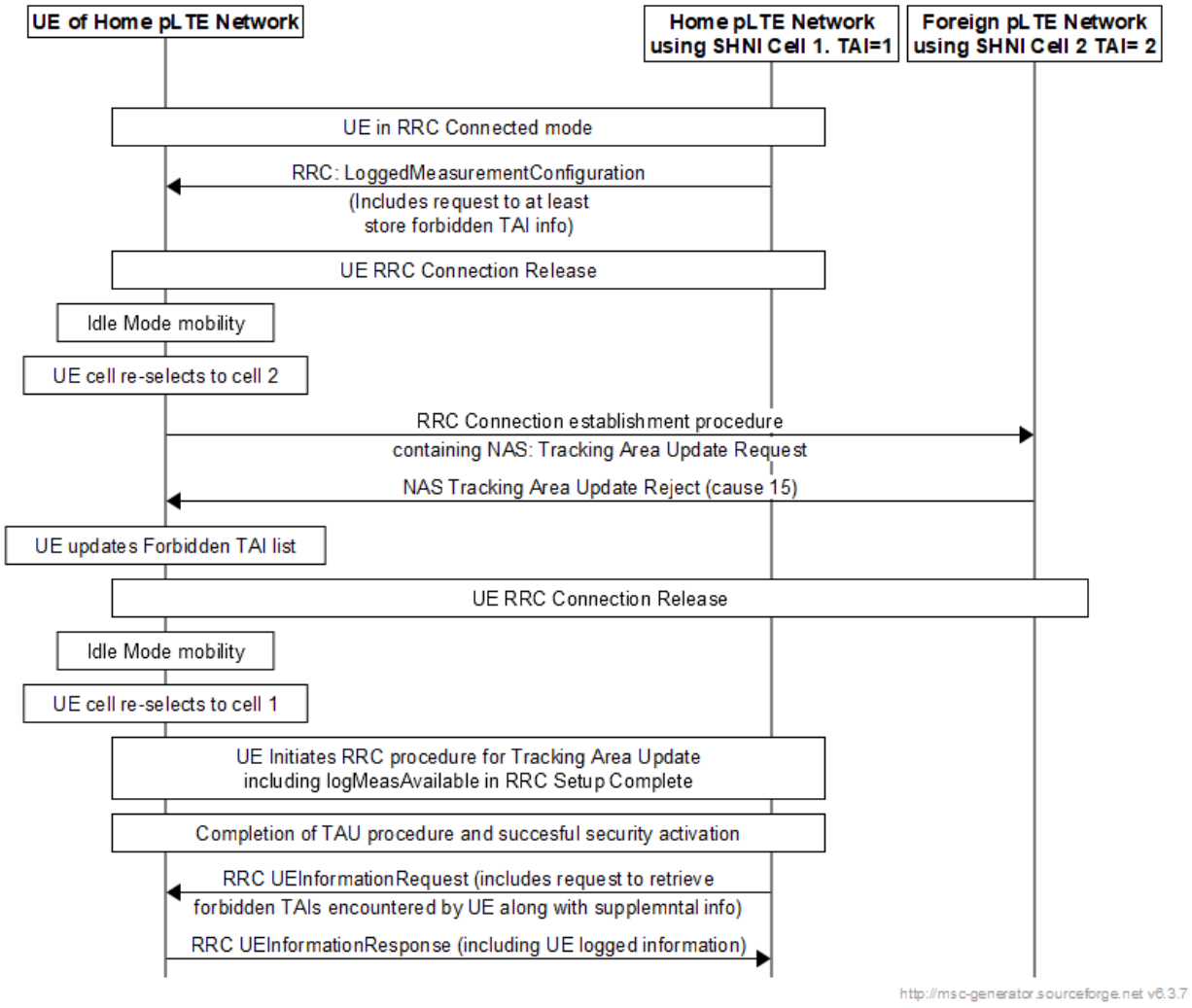

Figure A-3: Exemplary Message Sequence for TAI collision detection

Appendix E: Change History

Table A-1: Change History

Version	Date	Description
V0.0.0	31-03-2021	Initial Draft
V.01.0	31-10-2021	Draft for ballot submission. CRs • NSTG-21-065_r0_2021.07.12_Celona_Technical_TS-1004.docx • NSTG-21-091_r7_2021.09.15_Celona - G&D_Technical_Enterprise Identifier population in the SIM credent.docx • NSTG-21-090_r5_2021.09.15_Celona - G&D_Technical_Enterprise Information Service.docx • NSTG-21-097_r3_2021.09.29_Celona_Technical_TAC Collision Avoidance.docx • NSTG-21-083_r4_2021.08.16_Celona - G&D_Technical_Enterprise credential identification in the UE.docx • NSTG-21-078_r8_2021.08.09_Celona_Technical_Enterprise information message payload and parameter defi.docx • NSTG-21-080_r3_2021.08.09_Celona_Technical_Sample flow chart of UE search and camping behavior for a.docx • NSTG-21-079_r3_2021.08.09_Celona_Technical_Method of geofencing information population in the Enterp.docx • NSTG-21-077_r3_2021.08.09_Celona_Technical_Enterprise Database High Level Schema.docx • Added the definition of Enterprise Information, and comments about “geofence information” or “geofencing information” being encapsulated in “Enterprise Information”.