The Consultative Committee for Space Data Systems

Draft Recommendation for
Space Data System Standards

# SPACECRAFT ONBOARD INTERFACE SERVICES— HIGH DATA RATE WIRELESS PROXIMITY NETWORK COMMUNICATIONS

## DRAFT RECOMMENDED STANDARD

## CCSDS 883.0-P-1.1

## PINK SHEETS

**September 2022**

The Consultative Committee for Space Data Systems

**Draft Recommendation for**
**Space Data System Standards**

# SPACECRAFT ONBOARD INTERFACE SERVICES— HIGH DATA RATE WIRELESS PROXIMITY NETWORK COMMUNICATIONS

## DRAFT RECOMMENDED STANDARD

## CCSDS 883.0-P-1.1

## PINK SHEETS

**September 2022**

# PREFACE

This document is a draft CCSDS Recommended Standard. Its 'Pink Sheet' status indicates that the CCSDS believes the document to be technically mature and has released it for formal review by appropriate technical organizations. As such, its technical contents are not stable, and several iterations of it may occur in response to comments received during the review process.

Implementers are cautioned **not** to fabricate any final equipment in accordance with this document's technical content.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

# DOCUMENT CONTROL

| Document | Title | Date | Status |
|---|---|---|---|
| CCSDS 883.0-B-1 | Spacecraft Onboard Interface Services—High Data Rate 3GPP and Wi-Fi Local Area Communications, Recommended Standard, Issue 1 | February 2022 | Original issue |
| CCSDS 883.0-P-1.1 | Spacecraft Onboard Interface Services—High Data Rate Wireless Proximity Network Communications, Draft Recommended Standard, Issue 1.1 | September 2022 | Current draft update |

NOTES

1 Only pages affected by the current draft update are included in this review document.

2 Substantive changes from the original issue are indicated by markup and change bars.

[33] Communication Frequency Allocations and Sharing in the Lunar Region. Space Frequency Coordination Group Recommendation, SFCG 32-2R3. Darmstadt, Germany: SFCG, 10 December 2021.

[34] Preferred Frequency Bands for Radio Astronomical Measurements. RA Series, ITU-R RA.314-10. Geneva: ITU, June 2020.

[35] 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Requirements for Evolved UTRA (E-UTRA) and Evolved UTRAN (E-UTRAN). Release 9. 3GPP Technical Report, 3GPP TR 25.913 V9.0.0. Sophia Antipolis: 3GPP, December 2009.

[36] 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Study on Channel Model for Frequencies from 0.5 to 100 GHz. Release 16. 3GPP Technical Report, 3GPP TR 38.901 V16.1.0. Sophia Antipolis: 3GPP, December 2019.

[37] "Radio Regulations 2020." 2020. ITU. https://www.itu.int/en/myitu/Publications/2020/09/02/14/23/Radio-Regulations-2020.

[38] Protection of Frequencies for Radioastronomical Measurements in the Shielded Zone of the Moon. RA Series, ITU-R RA.479-5. Geneva: ITU, 2003.

[39] "Radio Astronomy in the Shielded Zone of the Moon." Article 22, Section V in Articles. Vol. 1 of Radio Regulations. Edition of 2020. 4 vols. Geneva: ITU, 2020.

[40] LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) Conformance Specification; Radio Transmission and Reception; Part 1: Conformance Testing. ETSI TS 136 521-1 V15.2.0 (2018-10). Sophia-Antipolis: ETSI, 2018.

[41] 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) Conformance Specification; Radio Transmission and Reception; Part 1: Conformance Testing. Release 16. 3GPP Technical Specification, 3GPP TS 36.521-1 V16.9.0 (2021-06). Sophia Antipolis: 3GPP, June 2021.

[42] Frequency Assignment Guidelines for Communications in the Mars Region. Space Frequency Coordination Group Recommendation, SFCG 22-1R4. Darmstadt, Germany: SFCG, 10 December 2021.

[43] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) Access. Release 17. 3GPP Technical Specification, 3GPP TS 23.401 V17.5.0 (2022-06). Sophia Antipolis: 3GPP, June 2022.

[44] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Architecture Enhancements for Non-3GPP Accesses. Release 17. 3GPP Technical Specification, 3GPP 3GPP TS 23.402 V17.0.0 (2021-03). Sophia Antipolis: 3GPP, March 2021.

[45] L. Daigle and A. Newton. Domain-Based Application Service Location Using SRV RRs and the Dynamic Delegation Discovery Service (DDDS). RFC 3958. Reston, Virginia: ISOC, January 2005.

[46] M. Mealling. *Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database*. RFC 3403. Reston, Virginia: ISOC, October 2002.

[47] M. Jones, J. Korhonen, and L. Morand. *Diameter Straightforward-Naming Authority Pointer (S-NAPTR) Usage*. RFC 6408. Reston, Virginia: ISOC, November 2011.

[48] *DNS/ENUM Guidelines for Service Providers & GRX/IPX Providers*. Version 6.0. GSMA IR.67. London: GSMA, December 2011.

[49] *3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Domain Name System Procedures; Stage 3*. Release 17. 3GPP Technical Specification, 3GPP 3GPP TS 29.303 V17.3.0 (2022-03). Sophia Antipolis: 3GPP, March 2022.

[50] D. Pinkas, N. Pope, and J. Ross. *CMS Advanced Electronic Signatures (CAdES)*. RFC 5126. Reston, Virginia: ISOC, February 2008.

[51] *Series X: Data Networks, Open System Communications and Security – Directory: Information Technology – Open Systems Interconnection – The Directory: Public-Key and Attribute Certificate Frameworks*. ITU-T X.509. Geneva: ITU, 2019.

[52] *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates*. Version 1.8.1. San Francisco: CA/Browser Forum, December 2021.

[53] *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; System architecture for the 5G System (5GS); Stage 2*. Release 17. 3GPP Technical Specification, 3GPP 3GPP TS 23.501 V17.5.0 (2022-06). Sophia Antipolis: 3GPP, June 2022.

[54] *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Procedures for the 5G System (5GS); Stage 2*. Release 17. 3GPP Technical Specification, 3GPP 3GPP TS 23.502 V17.5.0 (2022-06). Sophia Antipolis: 3GPP, June 2022.

[55] *3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Non-Access-Stratum (NAS) Functions Related to Mobile Station (MS) in Idle Mode*. Release 17. 3GPP Technical Specification, 3GPP 3GPP TS 23.122 V17.7.1 (2022-06). Sophia Antipolis: 3GPP, June 2022.

single standard. The recommendations of requiring a given standard include considering all of those standards subsequent to that standard, in the same path, for potential evolution. Current Wi-Fi path sequences are as follows:

a) IEEE 802.11n/802.11ax;

b) IEEE 802.11ac/802.11ax/802.11be Extremely High Throughput (EHT);

c) IEEE 802.11ad/802.11ay; and

d) IEEE 802.11ah.

Distinguishing performance characteristics for the IEEE Wi-Fi wireless standards are concisely summarized below (see reference [E20] for IEEE 802.11 standardization timelines):

– IEEE 802.11n (2009 standard): 2.4 GHz and 5.8 GHz short-range contention-based PHY/MAC with primarily best-effort performance, with support of up to 600 Mb/s in extreme multi-antenna configurations;

– IEEE 802.11ac (2013 standard): 5.8 GHz short-range contention-based PHY/MAC with primarily best-effort performance, with support of up to 2.34 Gb/s in present (Wave2), with potential for up to 6.77 Gb/s in extreme multi-antenna configurations;

– IEEE 802.11ax (2020 standard—see reference [E20], ~~2019 certification program, 2021 planned certification program for extended band~~Wi-Fi CERTIFIED 6™): Short-range time, space, and frequency-scheduled non-contention MAC for high efficiency and reliability. Initial operation at 2.4 GHz and 5.8 GHz but with extension to channels in 6 to 7 GHz, capable of 9.6 Gb/s. IEEE 802.11ax, marketed as Wi-Fi 6™ by the Wi-Fi Alliance, is the current generation Wi-Fi specification standard, and the successor to Wi-Fi 5™. The 802.11ax standard is designed to operate between 2 and 7 GHz as bands become available for 802.11 use. All Wi-Fi 6 devices work over the previously allocated 2.4 and 5 GHz bands. The Wi-Fi 6E™ designation is for products that also support the 6-7 GHz;

– IEEE 802.11be EHT (TBD availability): recently (2019) approved study group for a new standard for an extremely high-speed data rate improvement on IEEE 802.ax, full standardization targeted for 2024 (see reference [E20]), with large bandwidths and hence high operating frequencies. This standard would have even higher reliability than IEEE 802.11ax through the use of simultaneous coverage from multiple base stations;

– IEEE 802.11ah (2016 standard—see reference [E20], ~~planned 2021 certification program~~Wi-Fi CERTIFIED HaLow™): 900 MHz medium-range contention-based PHY/MAC, based on pre-IEEE 802.11n standards with improvements for reduced power and meshing. Maximum performance of 347 Mb/s in extreme configurations, at several times the range of IEEE 802.11n and IEEE 802.11ac;

– IEEE 802.11ad (2012 standard—see reference [E20]): 60 GHz very short-range and medium-range beamformed contention-based PHY/MAC, capable of functioning at

For the 3GPP Recommendation path, there are the following limitations and expected evolution:

The present network sharing Recommendations in this document use either (1) two networks running on the same RAN, via Multi-Operator Core Networking (MOCN)~~,~~; ~~or~~ (2) an interoperability connection outside the network core, using Access Point Name (APN) routing; or (3) true international roaming via an LTE Gateway Core Network. These are Mobile Virtual Network Operator (MVNO) approaches usually used inside a single nation between network operators with common heritage and tight partnerships and are optimized for such scenarios. ~~However, internationally,~~International roaming is the primary technology used for international operator interoperability across differing RAN technology networks with independent management, usually implemented in LTE via Gateway Core Networking (GWCN) using the LTE S8 and S6a interfaces, with further evolution planned in 5G (annex subsection C3, 3GPP Evolution)~~, and there will be a need for future near-term Recommendations in this area to support flexible international interoperability between space agency and commercial provider networks~~.

– The present network interface Recommendations in this document only specify the general combined control- and user-plane version of each interface and corresponding network function. However, as a step toward 5G, modern LTE commercial production networks are now implementing Control User Plane Separation (CUPS), in which most interfaces and functions are replaced by separate control- and user-plane variants, as described in annex subsection C3.6, Core Evolution to Control User Plane Separation. For both improved QoS and 5G integration, CUPS is required in future near-term Recommendations.

For the IEEE 802.11 Recommendation path, there are the following limitations and expected evolution:

As this document is being published, several IEEE standards and Wi-Fi Alliance certification programs are nearing completion. This document cannot recommend those standards because products cannot yet be evaluated. However these next-generation standards are likely to be applicable candidates offering performance increases and maintaining interoperability with past generations. Wireless interfaces anticipated in the ~~year 2021~~next few years (2022 forward) include ~~Wi-Fi CERTIFIED 6E™ products implementing features in IEEE 802.11ax,~~ Wi-Fi CERTIFIED HaLow™ products implementing features in IEEE 802.11ah~~,~~ and Wi-Fi CERTIFIED WiGig™ products implementing features in IEEE 802.11ay.

### 3.2.2 IEEE 802.11 CHANNEL PLAN

This Recommended Standard intends that infrastructures operating in space should support commercially available terrestrial client devices. However, all infrastructure implementations shall use channel assignments, or a subset of channel assignments, compatible with the respective IEEE 802.11 standards and respect all SFCG spectrum allocations and other applicable frequency band constraints [33]. The channel assignments (carrier frequencies, main spectral lobes) selected by the adopter when a SFCG wireless band is used for Wi-Fi shall not be outside the said wireless band currently allocated by SFCG (references [33] and [42]).

### 3.2.3 3GPP LTE CHANNEL PLAN

This Recommended Standard intends that infrastructures operating in space should support commercially available terrestrial 3GPP client/UE devices. However, all infrastructure implementations shall use channel assignments conforming, or a subset of channel assignments, compatible with the respective 3GPP LTE frequency band standards in 3GPP TS 36.101 (reference [7]) and respect all SFCG spectrum allocations and other applicable frequency band constraints. The channel assignments (carrier frequencies, main spectral lobes) selected by the adopter when a SFCG wireless band is used for Wi-Fi shall not be outside the said wireless band currently allocated by SFCG (references [33] and [42]).

## 3.3 IEEE 802.11 STANDARDS

### 3.3.1 GENERAL

Space exploration vehicles, gateways, and planetary surface elements shall incorporate Wi-Fi infrastructure to support internal and external, low-mobility, short-range, non-critical, wireless-extended network interoperable communications.

### 3.3.2 IEEE 802.11 WI-FI

**3.3.2.1** Infrastructure shall be compliant with Wi-Fi CERTIFIED 6™.

NOTE – Rationale: IEEE 802.11-based products are widely utilized terrestrially with a large COTS provider base and attendant reliability. IEEE 802.11ax offers very high data rates, higher quality of service, increased interference resilience, increased range, addresses hidden and exposed node issues, can be operated at 2.4 GHz or 5 GHz, and Wi-Fi CERTIFIED 6™ products have been increasingly available since late 2019.

**3.3.2.2** For 5 GHz implementations where Wi-Fi CERTIFIED 6™ is not possible, infrastructure may be compliant with Wi-Fi CERTIFIED ac.

NOTE – Rationale: IEEE 802.11-based products are widely utilized terrestrially with a large COTS provider base and attendant reliability. IEEE 802.11ac has replaced IEEE 802.11n as the most available 5 GHz variant currently on the market supporting high-rate data communications.

~~**3.3.2.3** Infrastructure may be compliant with Wi-Fi CERTIFIED n.~~

**3.3.2.3** Where Wi-Fi CERTIFIED 6™ is not possible and 2.4 GHz implementations are required, infrastructure may be compliant with Wi-Fi CERTIFIED n.

NOTES

1 Rationale: IEEE 802.11-based products are widely utilized terrestrially with a large COTS provider base and attendant reliability. IEEE 802.11n was recently the most advanced 2.4 GHz variant on the market supporting mid-rate data communications and has significant space heritage.

2 IEEE 802.11n (Wi-Fi 4) products will quickly become obsolete and deprecated in the wireless market. Mission designers should only consider IEEE 802.11n products for legacy system maintenance and operational support.

3 It is the responsibility of wireless communication system planners to follow the specific Wi-Fi channel plan specified by the mission infrastructure for multi-agency interoperable wireless communications.

4 In support of interoperable 802-11-based Wi-Fi communications, the CCSDS leverages the interoperability test suite of the Wi-Fi Alliance. Adherence to the attendant Wi-Fi certifications and sub-certifications for Wi-Fi 4 (802.11n), Wi-Fi 5 (802.11ac), and Wi-Fi 6 (802.11ax) provides the basis for multi-agency interoperable Wi-Fi wireless communication systems. ~~For highly mobile clients it is recommended that Wi-Fi clients support the Wi-Fi Alliance Request-to-send/Clear-to-send (RTS/CTS) certification.~~

**3.3.2.4** For highly mobile clients using 802.11n or ac, Wi-Fi clients and infrastructure should support the Wi-Fi Alliance 'RTS with BW Signaling' certification and the Request-to-send/Clear-to-send (RTS/CTS) protocol defined in IEEE 802.11-2020 subclauses 9.3.1 and 10.3.2.

### 3.3.3 IEEE 802.11 SECURITY

~~**3.3.3.1** For all implementations, security shall be compliant with Wi-Fi CERTIFIED WPA2-Enterprise™.~~

~~NOTE Rationale: IEEE 802.11 based products are widely utilized terrestrially with a large COTS provider base and attendant reliability. WPA2 is recommended for backward compatibility. WPA2 is recommended to be disabled unless necessary to support legacy designs.~~

~~**3.3.3.2** For all implementations, security should be compliant with Wi-Fi CERTIFIED WPA2-Personal™.~~

~~NOTE – Rationale: IEEE 802.11-based products are widely utilized terrestrially with a large COTS provider base and attendant reliability. WPA3 is recommended for all new designs (reference [27]).~~

**3.3.3.1** The order of preference for WPA security capabilities of IEEE 802.11 Wi-Fi networks is (best is first, or highest-ranked):

a) WPA3™-Enterprise 192-bit, when restricted to EAP-TLS/certificates;

b) WPA3™-Enterprise Only mode, when restricted to EAP-TLS/certificates;

c) WPA3™-Enterprise Only mode, when restricted to [EAP-PEAP] user/password;

d) WPA3™-Personal/WPA3™-SAE (global password/key).

NOTE – WPA3™-Enterprise Only = WPA2™ Enterprise + Protected Management Frames (PMF) and Authentication and Key Management (AKM) suite selector 5.

**3.3.3.2** New infrastructure and clients should strive to support the newest wireless security protocols whenever available. Low-ranked protocols may be operationally disabled. For all non-shared key implementations, security shall be compliant with WPA3™-Enterprise Only mode.

NOTE – Rationale: IEEE 802.11-based products are widely utilized terrestrially with a large COTS provider base and attendant reliability. Forward compatibility with WPA3™-Enterprise 192-bit mode EAP-TLS is recommended for all new designs (reference [27]) while supporting multiple authentication techniques. However, WPA3™-Enterprise 192-bit mode client hardware might be less readily available, and use of this standard requires evaluation to determine required backwards compatibility. It is recommended that new client designs implement WPA3™ so that networks can tighten security as infrastructure is modernized. It is recommended that new infrastructure designs implement WPA3™ Personal or Enterprise so that networks can tighten security as legacy clients are retired.

**3.3.3.3** For all shared-key implementations, security shall be compliant with WPA3™-Personal.

NOTE – Rationale: IEEE 802.11 based products are widely utilized terrestrially with a large COTS provider base and attendant reliability. User device compatibility with WPA3™-Enterprise 192-bit mode EAP-TLS is recommended for all new designs. Shared password security is difficult to manage but can be made secure using the WPA3™-SAE mode in WPA3™-Personal. WPA3™ is required for all new certifications. WPA3™ Personal presently is supported by many more devices than is WPA3™ Enterprise.

**3.3.3.4** For all implementations that do not use a single shared network key, security should be compliant with WPA3™-Enterprise with EAP-TLS security.

NOTE – Rationale: IEEE 802.11-based products are widely utilized terrestrially with a large COTS provider base and attendant reliability. WPA3™-Enterprise Only mode with EAP-TLS security, with client devices and credentials compatible with WPA3™-Enterprise 192-bit mode, is recommended for all new designs (reference [27]). WPA3™ 192-bit mode implements more protection than WPA3™-Enterprise Only and requires EAP-TLS authentication. However, WPA3™-Enterprise with 192-bit Mode client hardware might be less available, and use of this standard requires evaluation to determine required backwards compatibility.

**3.3.3.5** For all implementations not using a shared key, security should be implemented by EAP-TLS using self-signed certificates compliant with IETF RFC 5126 (reference [50]).

NOTE – Rationale: EAP-TLS is based on signed ITU X.509 (reference [51]) certificates for both infrastructure and clients and provides significantly more protection than other EAP-based methods. Self-signed Certificate Authority (CA) root and client certificates can be used to allow the wireless network to operate without requiring low-latency network connections to Earth-based CA signing infrastructure. EAP-TLS is implemented by the use of a local Authentication Server (AS) (RADIUS, for example) and WPA2™-Enterprise or WPA3™-Enterprise.

**3.3.3.6** For all implementations of EAP-TLS, certificates shall be renewed on all hardware on an ongoing basis.

NOTE – Rationale: Security keys need to be changed with enough regularity to ensure that large-scale probing of clients and/or capture of traffic does not allow determination of key value. Self-signed CA root certificates will generally last as long as 10 years. CA root certificate changes can result in problems with key distribution and are best not be updated unless responding to security compromise. Client certificates cannot be generated to last more than 825 days under CA/Browser Baseline Requirements (reference [52]). RADIUS certificates also ought to be renewed. If certificate renewal is possible in a mission, EAP-TLS 1.2 or above is the preferred level of authentication in an IEEE 802.11 network.

**3.3.3.7** All implementations not using a shared key should use SHA384 and 3072-bit (i.e., RSA 3K) signing size for signing WPA2™/WPA3™ credentials (keys and certificates).

NOTE – Rationale: WPA3™-Enterprise 192-bit mode security networks require 384-bit security signing and use of these keys provides future protection.

**3.3.3.8** All implementations not using shared keys should use an AS capable of implementing one of the following:

a) 192-bit security RSA 3K with the TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 cipher suite: ECDHE and RSA using the 384-bit prime modulus curve P-384, or

b) 192-bit security RSA 3K with the TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 cipher suite: DHE and RSA using ≥ 3072-bit modulus

NOTE – Rationale: These cipher suites are needed for simultaneous compatibility with both TLS 1.3 and Wi-Fi CERTIFIED WPA3™-Enterprise 192-bit mode networks and provide future protection (reference [22]).

**3.3.3.9** WPA3™-Enterprise Only mode and WPA3™-Enterprise 192-bit mode networks shall use TLS 1.2 and above.

NOTE – Rationale: TLS 1.2 is presently the minimum level of network security in modern wired and wireless network, with TLS 1.3 providing significant benefits on security and ability to handle network latency.

**3.3.3.10** If WPA3™-Enterprise and WPA3™-Personal are not possible, security may be compliant with Wi-Fi CERTIFIED WPA2™-Personal.

NOTE – Rationale: IEEE 802.11-based products are widely utilized terrestrially with a large COTS provider base and attendant reliability. WPA3 is recommended for all new designs (reference [27]); if WPA3™-Enterprise is not possible, utilization of WPA2™-Personal, which is less secure, is recommended.

**WARNING**: WPA-2™ Personal security is difficult to manage and will be deprecated; however, a significant pool of product choices exists today, and capability to accommodate a limited number of devices remains desirable.

**3.3.3.11** For all implementations, security shall be compliant with Wi-Fi CERTIFIED™ Protected Management Frames.

NOTE – Rationale: IEEE 802.11-based products are widely utilized terrestrially with a large COTS provider base and attendant reliability. Protected management frames preclude simple exploits such as spoofing or disconnection. Infrastructure without PMF would be entirely vulnerable. Clients without PMF are individually vulnerable. Over 24000 products have received this certification. This requirement does not apply to WPA2-Personal (see WARNING, above).

### 3.3.4 IEEE 802.11 WIRELESS PROFILES

All client implementations should be configurable with multiple profiles (reference [29]).

**3.4.3.2** The LTE Network RAN shall operate with a Physical Layer restricted to channel parameters, including RF frequency, bandwidth, and transmit power, listed in 3GPP TS 36.101 Radio Transmission and Reception specifications (reference [7]).

NOTE – Rationale: Modern UE and eNodeB devices are extensively tested for interoperability on these bands and with these parameters. Furthermore, signaling protocol specifications and user hardware settings use band numbers and other parameters in 3GPP TS 36.101 (reference [7]), and not direct reference to frequency and power, to specify behavior in a dynamic radio environment.

**3.4.3.3** If multi-cell operation is possible, eNodeB hardware should support S1-based HandOver (HO) according to 3GPP TS 36.413 S1 Application Protocol (reference [12]).

NOTE – Rationale: Multi-cellular operation provides an avenue for growth in capacity and coverage to allow communication over large terrains with complex line-of-sight requirements. S1-based handover is the most basic form of interoperable handover capable of ensuring that TCP/IP connections are not reset during the move from one eNodeB cell to another.

### 3.4.4 3GPP LTE NETWORK – ROAMING INTEROPERABILITY

#### 3.4.4.1 Discussion

Roaming in 3GPP LTE is supported by the 3GPP Gateway Core Networking (GWCN) architecture (references [3], [11], [43], [44], [53], and [54]).

#### 3.4.4.2 3GPP LTE Network—Differentiated S-GW and P-GW

All LTE networks requiring inter-agency/user roaming shall implement differentiated P-GW and S-GW functions (see option (b) in 3.4.11).

#### 3.4.4.3 3GPP LTE Network—GWCN Routing via S6a and S8

All LTE networks requiring inter-agency/user roaming shall be able to route S6a and S8 interface network traffic to and from other agency/user (home and visited) cores via Gateway Core Networking (GWCN) as described in 3GPP TS 23.401 (reference [43]) and 3GPP TS 23.402 (reference [44]).

#### 3.4.4.4 3GPP LTE Network—Visiting UE IMSI Authentication

All LTE networks requiring inter-agency/user roaming shall implement a method in the visited MME that allows home HSSes to be used for IMSIs from visiting UEs.

#### 3.4.4.5 3GPP LTE Network—Visiting UE Visited MME Home P-GW Selection

All LTE networks requiring inter-agency/user roaming shall implement a mechanism in the visited MME to select the correct home P-GW for a roaming (visiting) user for a given APN.

#### 3.4.4.6 3GPP LTE Network—DNS Requirements for LTE Roaming

All LTE networks requiring inter-agency/user roaming should implement local DNS servers describing their network via the S-NAPTR mechanism in the IETF RFC 3958 (reference [45]), IETF RFC 3403 (reference [46]), IETF RFC 6408 (reference [47]), GSMA PRD IR.88 (reference [11]), and GSMA PRD IR.67 (reference [48]) standards, using fully qualified domain names (FQDNs) and APN-FQDNs described in these standards and DNS procedures described in 3GPP TS 29.303 (reference [49]).

#### 3.4.4.7 3GPP LTE Network—User Roaming Home P-GW Selection

All LTE networks requiring inter-agency/user roaming should implement home P-GW selection in the visited MME from the visiting UE PLMN-ID and APN via the S-NAPTR mechanism described in 3GPP TS 29.303 (reference [49]) and IR.88 (reference [11]).

NOTES

1 Rationale: Roaming provides for agency LTE networks to provide network connectivity to other agencies'/users' UEs back to their home networks via their own cores using network connectivity requiring lower latency and performance than MOCN.

2 Rationale: GSMA PRD IR.88-specified roaming allows for dynamic delegation in a visited LTE network of visiting UEs to the home P-GWs corresponding to their APNs without requiring manual update of all MME configurations in all interoperating agencies when a single agency adds or modifies an APN and/or P-GW.

### 3.4.5 3GPP LTE NETWORK – RAN AND MULTI-OPERATOR CORE NETWORK

If direct sharing of the LTE RAN without further direct network interoperation is required, more than one EPC should be connected to the RAN in a Multi-Operator Core Network (MOCN) architecture, in accordance with 3GPP TS 23.251 Network Sharing (reference [13]).

NOTE – Rationale: MOCN allows supporting more than one agency directly using the shared RAN infrastructure if the corresponding eNodeB hardware is capable of supporting multiple S1 interface connections to different cores. Agencies retain full control of their networks with maximum isolation of those networks. Other techniques and infrastructure are required for agencies wishing to use lower SWaP hardware and/or deeper interoperability between their networks.

### A2.1.6 SD-WAN Configuration (Optional)

| SD-WAN | |
|---|---|
| Implementation Agency | |
| Special configuration | |
| Other information | |

| SD-WAN | |
|---|---|
| Implementation Agency | |
| Special configuration | |
| Other information | |

### A2.1.7 Identification of Specification

| CCSDS 883.0-P-1.1 | |
|---|---|
| Have any exceptions been required?<br><br>NOTE – A YES answer means that the implementation does not conform to the Recommended Standard. Non-supported mandatory capabilities are to be identified in the PICS, with an explanation of why the implementation is nonconforming. | Yes [ ] No [ ] |

| Item Number | Item Description | Reference | Status Value | Support | | Protocol Status Value | Profile Status Value |
|---|---|---|---|---|---|---|---|
| 1 | 3GPP LTE EPC & RAN (non-ISM) | 3.4.1 | M | | | | |
| 2 | 3GPP LTE EPC and RAN | 3.4.2 | M | | | | |
| 3 | 3GPP LTE EPC and UE LTE PHY | 3.4.3 | M | | | | |
| 4 | 3GPP LTE EPC and UE S1-based HO | 3.4.3 | M/O | | | | |
| 5 | 3GPP LTE Different S-GW & P-GW | 3.4.4.2 | M | | | | |

| Item Number | Item Description | Reference | Status Value | Support | | Protocol Status Value | Profile Status Value |
|---|---|---|---|---|---|---|---|
| 6 | 3GPP LTE GWCN S6a / S8 Routing | 3.4.4.3 | M/O | | | | |
| 7 | 3GPP LTE Visiting UE IMSI authentication | 3.4.4.4 | M/O | | | | |
| 8 | 3GPP LTE Visiting UE P-GW selection | 3.4.4.5 | M/O | | | | |
| 9 | 3GPP LTE DNS for LTE Roaming | 3.4.4.6 | M/O | | | | |
| 10 | 3GPP LTE Roaming Home P-GW selection | 3.4.4.7 | M/O | | | | |
| 11 | 3GPP LTE RAN and MOCN | 3.4.4 | O | | | | |
| 12 | 3GPP LTE RAN, Core, UE Security | 3.4.6 | M | | | | |
| 13 | 3GPP LTE RAN PLMN ID | 3.4.7 | M | | | | |
| 14 | 3GPP LTE UE IMSI | 3.4.8 | M | | | | |
| 15 | 3GPP LTE UE USIM ICCID | 3.4.9 | M | | | | |
| 16 | 3GPP LTE Core MME and HSS | 3.4.10 | M | | | | |
| 17 | 3GPP LTE Core S-GW and P-GW | 3.4.11 | M | | | | |
| 18 | 3GPP LTE Core S1-MME and S1-U | 3.4.12 | M | | | | |
| 19 | 3GPP LTE Core S6a and S11 | 3.4.13 | M | | | | |
| 20 | 3GPP LTE Core SGi | 3.4.14 | M | | | | |
| 21 | 3GPP LTE Core SGi for Ext-PDN | 3.4.15 | M | | | | |

### A3.1.6 Identification of Specification

| CCSDS 883.0-P-1.1 | |
|---|---|
| Have any exceptions been required?<br><br>NOTE – A YES answer means that the implementation does not conform to the Recommended Standard. Non-supported mandatory capabilities are to be identified in the PICS, with an explanation of why the implementation is nonconforming. | Yes [ ] No [ ] |

| ~~Item Number~~ | ~~Item Description~~ | ~~Reference~~ | ~~Status Value~~ | ~~Support~~ | | ~~Protocol Status Value~~ | ~~Profile Status Value~~ |
|---|---|---|---|---|---|---|---|
| ~~1~~ | ~~IEEE 802.11ax Wi-Fi 6~~ | ~~3.3.2~~ | ~~M~~ | | | | |
| ~~2~~ | ~~IEEE 802.11ax Wi-Fi 5~~ | ~~3.3.2~~ | ~~O~~ | | | | |
| ~~3~~ | ~~IEEE 802.11ax Wi-Fi 4~~ | ~~3.3.2~~ | ~~O~~ | | | | |
| ~~4~~ | ~~WPA2™~~ | ~~3.3.3~~ | ~~O~~ | | | | |
| ~~5~~ | ~~WPA3™~~ | ~~3.3.3~~ | ~~M~~ | | | | |
| ~~6~~ | ~~IEEE 802.11 Profiles~~ | ~~3.3.3.1~~ | ~~M~~ | | | | |

| Item Number | Item Description | Reference | Status Value | Requires Optional Item | Support | | Protocol Status Value | Profile Status Value |
|---|---|---|---|---|---|---|---|---|
| 1 | IEEE 802.11ax Wi-Fi 6 | 3.3.2 | M | | | | | |
| 2 | IEEE 802.11ax Wi-Fi 5 | 3.3.2 | O | | | | | |
| 3 | IEEE 802.11ax Wi-Fi 4 | 3.3.2 | O | | | | | |
| 4 | WPA3™-Enterprise | 3.3.3.2 | M | 6 | | | | |
| 5 | WPA3™-Personal | 3.3.3.3 | M | | | | | |

| Item Number | Item Description | Reference | Status Value | Requires Optional Item | Support | | Protocol Status Value | Profile Status Value |
|---|---|---|---|---|---|---|---|---|
| 6 | WPA3™-Enterprise with EAP-TLS | 3.3.3.4 | O | 7, 8, 9, 10, 11 | | | | |
| 7 | EAP-TLS Self-Signed Certificates | 3.3.3.5 | M | | | | | |
| 8 | EAP-TLS certificate renewal | 3.3.3.6 | M | | | | | |
| 9 | SHA384 & 3072-bit signing | 3.3.3.7 | O | | | | | |
| 10 | Authentication server cipher | 3.3.3.8 | O | | | | | |
| 11 | TLS minimum specification | 3.3.3.9 | O | | | | | |
| 12 | Access Point WPA2™ Personal | 3.3.3.10 | O | | | | | |
| 13 | Protected Management Frames (PMF) | 3.3.3.11 | M | | | | | |
| 14 | IEEE 802.11 Profiles | 3.3.3.1 | M | | | | | |

## A4 TEST ARTIFACT GENERATION FOR 3GPP INTEROPERABILITY TESTING

This document describes the procedure for the following:

a) 3GPP LTE Network connectivity verification;

b) 3GPP LTE Network performance characterization;

c) 3GPP LTE QoS verification;

d) 3GPP LTE Mobility verification.

| Testing Notes | |
|---|---|
| **Test Note 01** | iPerf test is applicable only to Wi-Fi, since LTE core does not allow UEs to directly ping each other. |
| **Test Note 02** | The test procedure for every interop scenario needs to be performed. |
| **Test Note 03** | Handover output is shown by recording the screen during video conference. Video conference is used for live streaming, which is used to avoid background video prefetching (i.e., caching). |

## A5 TEST ARTIFACT GENERATION FOR IEEE 802.11

### ExWC Wi-Fi Connectivity and Roaming Test Procedure

This document describes the Wi-Fi roaming test procedure as follows:

a) Network connectivity verification;

b) Network performance verification.

Once a UE has been connected to a Wi-Fi network, the Wi-Fi network credentials, Service Set Identifier (SSID), which are the network's name and the network's password, will be stored in the UE. The UE can then connect to any Wi-Fi network with the same credentials irrespective of the network location or vendor, thereby allowing roaming.

| Network Connectivity Verification Procedure | |
|---|---|
| **Test Description** | **Test documentation** |
| **Wi-Fi saved networks** | – Go to settings.<br>– Go to Wi-Fi.<br>– Go to Saved networks.<br>– Verify that the list of saved networks includes the Wi-Fi network of interest. |
| **Connecting to the Wi-Fi network** | – The UE automatically connects to the previously known Wi-Fi network.<br>– UE can also be manually connected to the Wi-Fi by going to Settings -> Wi-Fi and selecting the Wi-Fi network of interest. |
| ~~**UE access to the Internet**~~ | ~~Access can be verified by clicking on the browser and going to a website (e.g., www.nasa.gov).~~ |
| **UE access to the IP network** | – Demonstrate network access such as by browsing web site or pinging a network host. |

| | |
|---|---|
| **Enterprise Security Verification** | For Enterprise networks only, verification of A3.1.6<br>– Capture AS logs for TLS version and TLS Session Cipher Suite (at least TLS 1.2 and SHA256 or SHA384 in cipher suite)<br>– Capture Wireless traffic or AS logs for AKM Suite Selector (at least Suite Selector/OID 00:0F:AC 5 for WPA3-Enterprise)<br>– Capture Wireless traffic for PFM flag status (AP must send MFPR: 1) |

| **Network Performance Verification Procedure** | |
|---|---|
| **Test Description** | **Test documentation** |
| **iPerf test** | – Download PingTools Network Utilities (version 4.35 and above) from the app/play store.<br>Link: https://play.google.com/store/apps/details?id=ua.com.streamsoft.pingtools&hl=en_US<br>– Open the PingTools application on the UE.<br>– Click the tab on the top-left and select iPerf.<br>– Enter the iPerf server IP address and click start.<br>Signature: |

| **Testing Notes** | |
|---|---|
| **Test Note 01** | A UE with Android OS is used as an example in the procedure. |

## C2.10 IEEE 802.11AH-2016 WI-FI HALOW

An offshoot of the older IEEE 802.11-2007 standards, which precede IEEE 802.11n, the 2016 Wi-Fi HaLow standard (reference [2]) is designed to support longer range and lower electrical power communications by use of bands in the vicinity of 900 MHz, for Internet-of-Things (IoT) applications. Communication is based on the IEEE 802.11a and IEEE 802.11g protocols, with some modifications. To fit within the narrow bandwidths available at 900 MHz, the standard works on a sub-sampled variant of the IEEE 802.11-2007 standards. Only 26 OFDM sub-channels are used, down from 52, but in a 16 MHz total channel width, compared to 22 MHz for IEEE 802.11g. Unlike IEEE 802.11a and IEEE 802.11g, IEEE 802.11ah allows 4 MIMO streams, allows up to 347 Mb/s data rates, and can operate at ranges above 1 kilometer. IEEE 802.11ah HaLow will support WPA3™ security.

## C2.11 IEEE 802.11 NETWORK AUTHENTICATION

Wi-Fi network access can be controlled and administered via IEEE 802.1x port-based Network Access Control. IEEE 802.1X (reference [22]) defines the encapsulation of the Extensible Authentication Protocol (EAP) over IEEE 802. With IEEE 802.1x systems, Remote Authentication Dial-In User Service (RADIUS) is often the back-end of choice for authentication. RADIUS is a client/server protocol that runs at the Application Layer utilizing either UDP or TCP for transport, and provides authentication, authorization, and accounting management services. Network access servers, the gateways that control access to a network, usually contain a RADIUS client component that communicates with the RADIUS server. WPA2™ and WPA3™ with IEEE 802.1x authentication are known as WPA2™-Enterprise and WPA3™-Enterprise. Enterprise variants of WPA2™ and WPA3™ do not suffer from the management and security exposure problems of pre-shared keys.

The Protected Extensible Authentication Protocol, also known as Protected EAP or simply PEAP, is a protocol that encapsulates EAP within a potentially encrypted and authenticated Transport Layer Security (TLS) tunnel. The purpose was to correct deficiencies in EAP; EAP assumed a protected communication channel, such as that provided by physical security, so facilities for protection of the EAP conversation were not provided.

PEAP was jointly developed by Cisco Systems, Microsoft, and RSA Security. The protocol only specifies chaining multiple EAP mechanisms and not any specific method. Use of the EAP-MSCHAPv2 and EAP-GTC methods are the most commonly supported.

EAP is an authentication framework frequently used in network and internet connections. It is defined in RFC 3748, which made RFC 2284 obsolete, and is updated by RFC 5247. EAP is an authentication framework for providing the transport and usage of material and parameters generated by EAP methods. There are many methods defined by RFCs, and a number of vendor-specific methods and new proposals exist. EAP is not a wire protocol; instead it only defines the information from the interface and the formats. Each protocol that uses EAP defines a way to encapsulate by the user EAP messages within that protocol's messages.

EAP is in wide use as of publication. For example, in IEEE 802.11 (WiFi) the WPA and WPA2™ standards have adopted IEEE 802.1X (with various EAP types) as the canonical authentication mechanism.

EAP-TLS, defined in RFC 5216, is an IETF open standard that uses the TLS protocol, and is well-supported among wireless vendors. EAP-TLS is the original, standard wireless LAN EAP authentication protocol. EAP-TLS is still considered one of the most secure EAP standards available, although TLS provides strong security only as long as the user understands potential warnings about false credentials, and is universally supported by all manufacturers of wireless LAN hardware and software.

## C3 3GPP EVOLUTION

### C3.1 OVERVIEW

Detailed technical information for 3GPP Long Term Evolution (LTE) is specified in reference [E1]. Additional technical information is contained in Interop Testing Considerations for 3GPP LTE in the associated Yellow Book Interoperability Testing Report (reference [E16]), Interoperability Considerations (SD-WAN) annex in reference [E1], Spectrum Management Concerns in reference [E1], annex D, Network Management in 3GPP Networks annex in reference [E1], and annex G of this document.

The architecture of the 3GPP Long Term Evolution (LTE) proximity wireless communications is shown in figure C-1. The primary LTE functional components that constitute the RAN and the Evolved Packet Core (EPC) are:

– Mobility Management Entity (MME): Supports user equipment context, identity, authentication, and authorization.

– S-GW: Receives and sends packets between the eNodeB and the core network.

– P-GW: Connects the EPC with external networks.

– Home Subscriber Server (HSS): Database of user-related and subscriber-related information.

– Policy and Charging Rules Function (PCRF): Optional function providing QoS rules to P-GW.

NOTE – S-GW and P-GW may be implemented as a single combined gateway for simplified user-plane applications.

– [Required] SGi interface between P-GW and external PDN carrying user-plane traffic flow to external services.

## C3.2 3GPP LTE ROAMING

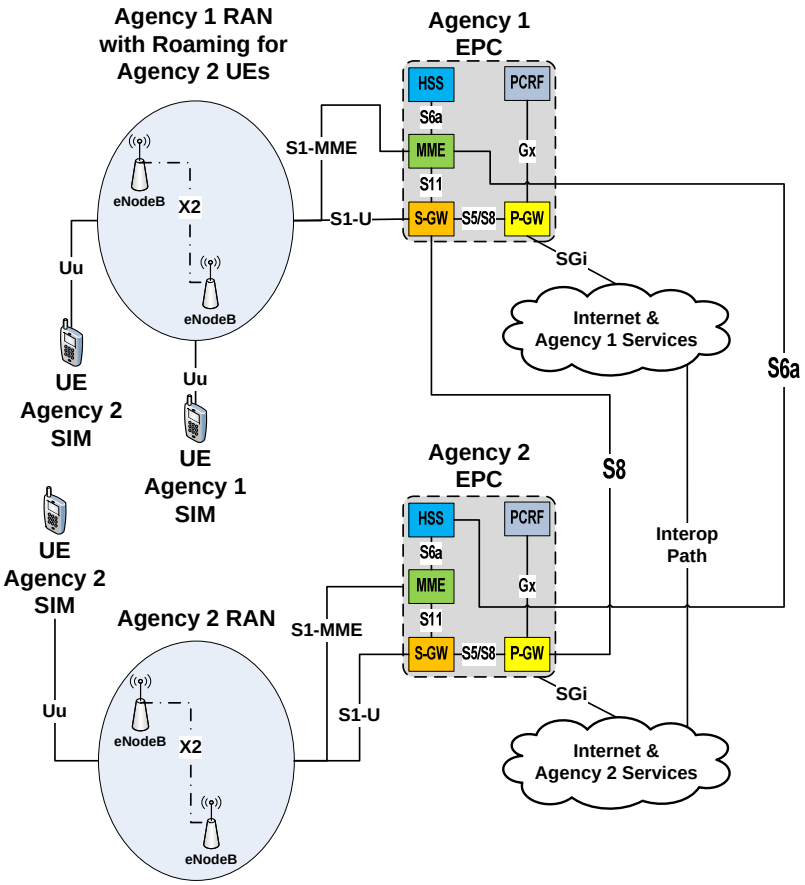


**Figure C-2: 3GPP LTE Roaming (GWCN) Architecture**

3GPP LTE Roaming can be described as follows: The visiting UE checks to see if its home PLMN-ID is available. If not, it looks at an internal list of VPLMs where it has roamed onto its HPLM before. If that doesn't work, it starts to check available PLMNs randomly to see if one allows it to connect. Once that works, it remembers. If the HPLM appears, it switches back to it as described in 3GPP TS 23.122 (reference [55]). Something *could* be added to the block up to say that the UE *shall* implement the PLMN selection processes in TS 23.122 to connect to a visited PLMN RAN. Testing has shown that this only works if the ICCID on the device is such that it will know what regulatory domain to use for channels to scan to find the network. LTE Roaming Interfaces (*roaming is preferred architecture for Agency Interoperability support*) are shown in figure C-2 with the following characteristics:

– RAN networks are owned by different agencies, with fully independent cores and services are allowed.

- UEs from different agencies (Home PMN/HPMN) can roam on another network (Visited PMN/VPMN) and connect to their HPMN and corresponding agency network.
- Agency 2 connects on agency 1 RAN; connections in other direction must be established for agency 1 on agency 2 RAN.
- As UEs move between RANs, S-GWs usually change, TCP/IP sockets close/restart.
- Roaming can be addressed with Post-IP and DTN protocols.
- Simple handover between eNodeBs inside the same RAN is not a problem.
- The configuration shown is just GWCN (and some variants possible), but with RANs having RF overlap.
- The configuration is robust to latency issues.
- The configuration needs full S-GW and P-GW with S8, but highly-standardized, if available.
- LTE/5G Interoperation is based on S8:3GPP TS 23.501 (reference [53]), 23.502 (reference [54]), and GSMA NG.113 (reference [3]).

Home Routing, Local breakout, MSISDN, and compatibility:

- As discussed earlier, some interoperation modes require the P-GW of one agency's network to receive information that originates from the HSS of another agency's network, transmitted via the S-GW, which gets it from the MME.
- This requires compatibility between the *contents* of that information from the HSS with what the S-GW expects.
- But some components may be optional, one being MSISDN (generalized phone number), whereas IMSI (subscriber ID) is always required.
- Combining optional and required components can be problematic when vendors implement things differently; in a home-routed (HR) network it is not a problem, since HSS and P-GW are in the same agency's network.
- But HR requires an S-GW/P-GW split and an EPC that can provide for this via S8.
- Local breakout (LBO, P-GW local to agency RAN) avoids S8, but cannot be an HPMN.
- LBO allows for combined gateways and fully local traffic to have low latency and high throughput to local data networks, even if some other core functions (such as HSS) are remote via longer latency or low-throughput backhaul networks.
- Full-blown cores allow mixing both, but reduced cores are useful in many circumstances (albeit more a software development/management issue than computing power).

## C3.3 LTE EVOLUTION TOWARD 5G

Since reference [E1], 3GPP 4th Generation LTE technology has advanced considerably and has become the dominant form of mobile high-speed data communications. However, the first full 3GPP 5th Generation (5G) 3GPP technology standards have been completed, and 5G networks are now being deployed to consumers, having started to become operational in October 2018. Table C-1 details the timeline and capabilities evolution of 3GPP LTE and 5G. This annex subsection describes important advances and changes that are crucial to near-term use of 3GPP standards in spaceflight proximity wireless networks.

**Table C-1: 3GPP LTE and 5G Capabilities by Release**

| Release | Status | Start | End | Capabilities and Services |
|---|---|---|---|---|
| **Rel-18** | Open | 2021-12-15 | 2024-03-01 | 5G-Advanced.machine-learning-based techniques at different levels of the wireless network. Edge computing, evolution of IMS, smart energy and infrastructure, vehicle-mounted relays, low power high accuracy positioning for industrial IoT scenarios, enhanced access to and support of network slice, satellite backhaul in 5G. |
| **Rel-17** | Open | 2018-06-15 | 2022-07-01 | Topics include: Cyber-physical control systems, mission critical services common requirements, critical medical applications, enhancements for UAVs, asset tracking use cases, enhanced relays, future railway mobile communication system, ~~edge computing enhancement for 5G networks, and proximity services enhancements~~evolution of NTN, edge computing enhancement for 5G networks, and V2V and D2D (sidelink) services. |
| **Rel-16** | ~~Open~~Frozen | 2017-03-22 | 2020-07-03 | Topics include: Multimedia Priority Service, Vehicle-to-everything (V2X) Application Layer services, 5G satellite access, Local Area Network support in 5G, wireless and wireline convergence for 5G, terminal positioning and location~~, and novel radio techniques~~. Also security, codecs and streaming services, Local Area Network interworking, network slicing, and the IoT. |
| **Rel-15** | Frozen | 2016-06-01 | 2019-06-07 | First NR ('New Radio') release. Support for 5G Vehicle-to-x service, IP Multimedia Core Network Subsystem (IMS), Future Railway Mobile Communication System. |
| **Rel-14** | Frozen | 2014-09-17 | 2017-06-09 | Energy Efficiency, Location Services (LCS), Mission Critical Data over LTE, Mission Critical Video over LTE, Flexible Mobile Service Steering (FMSS), Multimedia Broadcast Supplement for Public Warning System (MBSP), enhancement for TV service, massive Internet of Things~~, Cell Broadcast Service (CBS)~~. |
| **Rel-13** | Frozen | 2012-09-30 | 2016-03-11 | LTE in non-licensed bands, LTE enhancements for Machine-Type Communication. Elevation Beamforming/Full-Dimension MIMO, Indoor positioning. LTE-Advanced Pro. |

| Release | Status | Start | End | Capabilities and Services |
|---|---|---|---|---|
| **Rel-12** | Frozen | 2011-06-26 | 2015-03-13 | Enhanced Small Cells (higher order modulation, dual connectivity, cell discovery, self-configuration), Carrier aggregation (2 uplink carriers, 3 downlink carriers, FDD/TDD carrier aggregation), MIMO (3D channel modeling, elevation beamforming, massive MIMO), New and Enhanced Services: MTC, D2D comms, eMBMS. |
| **Rel-11** | Frozen | 2010-01-22 | 2013-03-06 | Advanced IP Interconnection of Services. Service layer interconnection between national operators/carriers as well as third party application providers heterogeneous networks (HetNet) improvements, Coordinated Multi-Point operation (CoMP). In-device Co-existence (IDC). |
| **Rel-10** | Frozen | 2009-01-20 | 2011-06-08 | LTE Advanced ~~fulfilling~~ IMT Advanced 4G requirements. Backwards compatible with release 8 (LTE). ~~Multi-Cell HSDPA (4 carriers).~~ |
| **Rel-9** | Frozen | 2008-03-06 | 2010-03-25 | SAES Enhancements, WiMAX and LTE/UMTS interop. Dual-Cell HSDPA with MIMO, Dual-Cell HSUPA. LTE HeNB. |
| **Rel-8** | Frozen | 2006-01-23 | 2009-03-12 | First LTE release. All-IP Network (SAE). New OFDMA, FDE, and MIMO based radio interface, not backwards compatible with previous CDMA interfaces. Dual-Cell HSDPA. UMTS HNB. |

3GPP standards have evolved into their 5$^{th}$ Generation since reference [E1]. 5G standards are defined from 3GPP Release 15, onwards. The 3GPP Release 16 and Release 17 standards have been previously ratified. There are a set of three major capabilities that define 5G and are critical to future spaceflight requirements, as follows:

– Enhanced Mobile Broadband (eMBB): extremely high-speed communications data rate, in the 1-10 Gb/s class;

– Ultra-Reliable Low Latency Communications (URLCC): reaching extremely high-reliability wireless communications for mission-critical command and control and teleoperations, at wire line-class reliability, with latency sub-1 ms;

– Massive Machine-type Communications (mMTC): allowing for extremely dense clients, at densities in the 1 million devices per km$^2$ class.

5G achieves these capabilities by an evolution of the RF interface and an evolution of the network architecture used in 3GPP, compared to 4G LTE. The new radio technology, 5G NR, is based on a scalable OFDM solution, which can expand beyond the 15 kHz OFDM subcarrier spacing in factors of two, while also allowing for more subcarriers in a channel, and more channel aggregation, plus the optional ability to use OFDMA, instead of SC-FDMA, in the uplink. Additionally, allowed frequency bands are expanded above 3 GHz, and up into mmWave bands reaching up to 100 GHz. In the mmWave bands, it is expected that, for example, 500 MHz of bandwidth will be available in 28 GHz, 1 GHz at 38 GHz, and 2 GHz at 72 GHz. These high frequencies allow for beam-forming and massive MIMO in extremely compact antenna array and device sizes. However, starting at 600 MHz, 5G will also use low-band frequencies, and present 4G LTE bands will steadily be replaced by 5G bands, starting in 2020, as has happened in the transition from 2G and 3G to 4G LTE.

[E11] Ankit Bhamri, Kari Hooli, and Timo Lunttila. “Massive Carrier Aggregation in LTE-Advanced Pro: Impact on Uplink Control Information and Corresponding Enhancements.” *IEEE Communications Magazine* 54, no. 5 (May 2016): 92–97.

[E12] CBRS Alliance. https://www.cbrsalliance.org.

[E13] “Mission Critical Services in 3GPP.” June 20, 2017. 3GPP. https://www.3gpp.org/NEWS-EVENTS/3GPP-NEWS/1875-MC_SERVICES.

[E14] “Wi-Fi Direct.” Wi-Fi Alliance. https://www.wi-fi.org/discover-wi-fi/wi-fi-direct.

[E15] LoRa Alliance®. https://lora-alliance.org/.

[E16] *Proximity Wireless Network Communications Interoperability Test Report*. ITR 883x0b1-Y. Forthcoming.

[E17] “Roadmap - IEEE Future Networks.” IEEE. https://futurenetworks.ieee.org/roadmap.

[E18] “5G NR C-V2X Progress Report.” Presented at Meeting of Collaboration on ITS Communication Standards (8 March 2019, Geneva). https://www.itu.int/en/ITU-T/extcoop/cits/Documents/Meeting-20190308-Geneva/14_5GAA-progress_report.pdf

[E19] *ETSI Plugtests Report: 1st ETSI C-V2X Plugtests (2–6 December 2019, Malaga, Spain)*. V1.0.0. Sophia-Antipolis: ETSI, December 2019.

[E20] “Official EEE 802.11 Working Group Project Timelines—2020-12-23.” LMSC, LAN/MAN Standards Committee (Project 802). https://www.ieee802.org/11/Reports/802.11_Timelines.htm. (31 December 2020)

[E21] Youjia Chen, et al. “Dynamic Reuse of Unlicensed Spectrum: An Inter-Working of LTE and WiFi.” *IEEE Wireless Communications* 24, no. 5 (October 2017): 52–59.

[E22] Massimiliano Maule, et al. “Delivering Fairness and QoS Guarantees for LTE/Wi-Fi Coexistence Under LAA Operation.” *IEEE Access* 6 (23 January 2018): 7359–7373.

[E23] Dmitry Chizhik, et al. “Analytic Propagation Approximation over Variable Terrain and Comparison to Data.” In *2020 14th European Conference on Antennas and Propagation (EuCAP) (15–20 March 2020, Copenhagen, Denmark)*, 1–3. Piscataway, New Jersey: IEEE Conference Publications, 2020.

[E24] Chatwin Lansdowne, et al. “Spacecraft Wireless System Performance Degradation Due to Impedance Mismatch in Cables and Connectors.” In *2019 IEEE Topical Workshop on Internet of Space (TWIOS) (20–23 January 2019, Orlando, Florida)*, 1–4. Piscataway, New Jersey: IEEE Conference Publications, 2019.

[E25] “Lunar Surface Propagation Modeling and Effects on Communications.” In *26th International Communications Satellite Systems Conference (ICSSC) (10–12 June 2008, San Diego, CA)*. Reston, Virginia: AIAA, 2008.

[E26] *CCSDS Authentication Credentials*. Issue 1. Recommendation for (Blue Book), CCSDS 357.0-B-1. Washington, D.C.: CCSDS, July 2019.

# ANNEX H

# PROPOSED FUTURE STANDARDIZATION ACTIVITIES

# (INFORMATIVE)

**Table H-1: Roadmap for Future Standardization Activities**

| Activity | Status | Start | End | Capabilities and Services |
|---|---|---|---|---|
| **CCSDS 883.0-B-1** | ~~Open~~Closed | 2020-02-15 | ~~2020-12-31~~2022-02-01 | Topics include: IEEE 802.11 and 3GPP standards for space proximity wireless network communications.<br>IEEE 802.11 (WFA):<br>802.11n 2.4 GHz/5 GHz (Wi-Fi 4)<br>802.11ac 5 GHz (Wi-Fi 5, wave 1 and wave 2)<br>802.11ax 2.4 GHz, 5 GHz (Wi-Fi 6) 6 GHz (Wi-Fi 6E), 802.11be 2.4, 5, 6 GHz (Wi-Fi 7)<br>802.11k-r-v Enterprise Roaming<br>NOTE– IEEE 802.11n (Wi-Fi 4) products are recommended only for legacy system.<br>3GPP<br>LTE: SIM Interop<br>LTE: Multi-RAN<br>LTE: Multi Operator Core Network<br>LTE: APN Routing |
| **CCSDS 883.0-B-2** | Open | 2022-02-01 | 2022-07-01 | Focus is on true 3GPP Roaming for ICSIs, Gateway<br>GWCN<br>CUPS<br>Focus on 802.11 updated standards and hardware<br>Wi-Fi 6E 6 GHz<br>802.11ay 60 GHz<br>802.11ah 900 MHz<br>Focus on 3GPP LTE/5G Rel-16, Rel-17 updates<br>5G RAN and Core interoperability<br>C-V2X, D2D<br>Network Slicing<br>IoT<br>Satellite LTE/5G (backhaul, RAN)<br>Advanced spectrum sharing<br>Dynamic Spectrum Sharing (DSS)<br>Licensed Assist Access (LAA)<br>Licensed Shared Access (LSA) |

The roadmap includes an intersessional SOIS/Wireless-SLS/RFM meeting during every CCSDS meeting, for coordination about frequency band and modulations sets issues.