**3GPP TSG-SA WG6 Meeting #42-bis-e S6-210844**

**e-meeting, 12th – 20th April 2021 (revision of S6-21xxxx)**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **23.434** | **CR** | **51** | **rev** | **1** | **Current version:** | **17.1.0** |  |
|  |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* |
|  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME | **x** | Radio Access Network |  | Core Network | **x** |

|  |
| --- |
|  |
| ***Title:***  | SEAL support for CoAP |
|  |  |
| ***Source to WG:*** | Ericsson |
| ***Source to TSG:*** | S6 |
|  |  |
| ***Work item code:*** | eSEAL |  | ***Date:*** | 2021-04-12 |
|  |  |  |  |  |
| ***Category:*** | **B** |  | ***Release:*** | Rel-17 |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(mirror corresponding to a change in an earlier release)****B*** *(addition of feature),* ***C*** *(functional modification of feature)****D*** *(editorial modification)*Detailed explanations of the above categories canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)…Rel-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | Enhancement of SEAL signalling plane by is required to support constrained devices, e.g. devices that are battery-driven, have limited CPU, memory or communication capabalities. The proposed enhancements are described in TR 23.745 clause 7.20.SEAL-UU is a generic reference point for interactions between a SEAL client and a corresponding SEAL server. Each SEAL service specifies its SEAL-UU reference point and the protocol(s) used in that reference point. The present SEAL services make a choice of using HTTP and/or SIP in the SEAL-UU reference point. Clause 6.2 specifies the functional model of the SEAL signalling control plane, which is based on SIP and HTTP. While these protocols are well established and performant for non-constrained devices, they are problematic for constrained devices.The Constrained Application Protocol (CoAP) is a protocol defined by IETF in RFC 7252 and designed specifically for application layer communication for constrained devices. CoAP provides a request/response interaction model between application endpoints, supports built-in discovery of services and resources, and includes key concepts of the Web such as URIs and Internet media types. CoAP is designed to easily interface with HTTP for integration with the Web while meeting specialized requirements such as multicast support, very low overhead, and simplicity for constrained environments. RFC 7252 specifies bindings to UDP and DTLS. IETF RFC 8323 specifies bindings to TCP, WebSocket and TLS. |
|  |  |
| ***Summary of change:*** | In summary:1. SEAL is enhanced to support CoAP as an additional signalling protocol for use by SEAL services over SEAL-UU reference point.
2. SEAL functional model for signalling control plane is enhanced with CoAP entities.
 |
|  |  |
| ***Consequences if not approved:*** | SEAL does not provide support for constrained devices in the signalling control plane. |
|  |  |
| ***Clauses affected:*** | 2, 6.2, (new) Annex X |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **X** |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  | **X** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **X** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

\* \* \* First Change \* \* \* \*

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 22.104: "Service requirements for cyber-physical control applications in vertical domains".

[3] 3GPP TS 23.379: "Functional architecture and information flows to support Mission Critical Push To Talk (MCPTT); Stage 2".

[4] 3GPP TS 23.280: "Common functional architecture to support mission critical services; Stage 2".

[5] 3GPP TS 23.281: "Functional architecture and information flows to support Mission Critical Video (MCVideo); Stage 2".

[6] 3GPP TS 23.282: "Functional architecture and information flows to support Mission Critical Data (MCData); Stage 2".

[7] 3GPP TS 23.286: "Application layer support for V2X services; Functional architecture and information flows".

[8] 3GPP TS 23.222: "Functional architecture and information flows to support Common API Framework for 3GPP Northbound APIs; Stage 2".

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

[10] 3GPP TS 23.501: "System Architecture for the 5G System; Stage 2".

[11] 3GPP TS 23.502: "Procedures for the 5G System; Stage 2".

[12] 3GPP TS 23.303: "Proximity-based services (ProSe); Stage 2".

[13] 3GPP TS 23.682: "Architecture enhancements to facilitate communications with packet data networks and applications".

[14] 3GPP TS 23.002: "Network Architecture".

[15] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[16] 3GPP TS 23.468: "Group Communication System Enablers for LTE (GCSE\_LTE); Stage 2".

[17] 3GPP TS 23.246: "Multimedia Broadcast/Multicast Service (MBMS); Architecture and functional description".

[18] 3GPP TS 23.203: "Policy and charging control architecture".

[19] 3GPP TS 23.503: "Policy and Charging Control Framework for the 5G System; Stage 2".

[20] 3GPP TS 26.348: "Northbound Application Programming Interface (API) for Multimedia Broadcast/Multicast Service (MBMS) at the xMB reference point".

[21] 3GPP TS 29.214: "Policy and charging control over Rx reference point".

[22] 3GPP TS 29.468: "Group Communication System Enablers for LTE (GCSE\_LTE); MB2 Reference Point; Stage 3".

[23] 3GPP TS 36.300: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2".

[24] IETF RFC 6733 (October 2012): "Diameter Base Protocol".

[25] ETSI TS 102 894-2 (V1.2.1): "Intelligent Transport Systems (ITS); Users and applications requirements; Part 2: Applications and facilities layer common data dictionaryMultimedia Broadcast/Multicast Service (MBMS); Protocols and codecs".

[26] ETSI TS 102 965 (V1.4.1): "Intelligent Transport Systems (ITS); Application Object Identifier (ITS-AID); Registration".

[27] ISO TS 17419: "Intelligent Transport Systems - Cooperative systems - Classification and management of ITS applications in a global context".

[28] 3GPP TS 26.346: "Multimedia Broadcast/Multicast Service (MBMS); Protocols and codecs".

[29] 3GPP TS 33.434: "Service Enabler Architecture Layer (SEAL); Security aspects for Verticals".

[30] 3GPP TS 29.549: "Service Enabler Architecture Layer for Verticals (SEAL); Application Programming Interface (API) specification; Stage3".

[31] 3GPP TS 23.285: "Architecture enhancements for V2X services".

[refX] IETF RFC 7252: "The Constrained Application Protocol (CoAP)".

[refY] IETF RFC 8323: "CoAP (Constrained Application Protocol) over TCP, TLS, and WebSockets".

\* \* \* Next Change \* \* \* \*

## 6.2 On-network functional model description

Figure 6.2-1 illustrates the generic on-network functional model for SEAL.



Figure 6.2-1: Generic on-network functional model

In the vertical application layer, the VAL client communicates with the VAL server over VAL-UU reference point. VAL-UU supports both unicast and multicast delivery modes.

NOTE 1: The VAL-UU reference point is out of scope of the present document.

The SEAL functional entities on the UE and the server are grouped into SEAL client(s) and SEAL server(s) respectively. The SEAL consists of a common set of services (e.g. group management, location management) and reference points. The SEAL offers its services to the vertical application layer (VAL).

NOTE 2: The functionalities and reference points of the vertical application layer are out of scope of the present document.

NOTE 3: The vertical application layer may further consist of vertical application enabler layer functionalities (specified by 3GPP) and application specific functionalities, which is out of scope of the present document.

The SEAL client(s) communicates with the SEAL server(s) over the SEAL-UU reference points. SEAL-UU supports both unicast and multicast delivery modes. The SEAL client(s) provides the service enabler layer support functions to the VAL client(s) over SEAL-C reference points. The VAL server(s) communicate with the SEAL server(s) over the SEAL-S reference points. The SEAL server(s) may communicate with the underlying 3GPP network systems using the respective 3GPP interfaces specified by the 3GPP network system.

Editor's Note: SEAL-UU support for multicast delivery is FFS.

The specific SEAL client(s) and the SEAL server(s) along with their specific SEAL-UU reference points and the specific network interfaces of 3GPP network system used are described in the respective on-network functional model for each SEAL service.

Figure 6.2-2 illustrates the functional model for interconnection between SEAL servers.



Figure 6.2-2: Interconnection between SEAL servers

To support distributed SEAL server deployments, the SEAL server interacts with another SEAL server for the same SEAL service over SEAL-E reference point.

Figure 6.2-3 illustrates the functional model for inter-service communication between SEAL servers.



Figure 6.2-3: Inter-service communication between SEAL servers

The SEAL server interacts with another SEAL server for inter-service communication over SEAL-X reference point.

Figure 6.2-4 illustrates the functional model for communication between SEAL server and VAL user database.



Figure 6.2-4: Communication between SEAL server and VAL user database

The SEAL server interacts with the VAL user database for storing and retrieving user profile over VAL-UDB reference point.

Figure 6.2-5 shows the functional model for the signalling control plane.



Figure 6.2-5: Functional model for signalling control plane

NOTE: The Light-weight Protocol (LWP) functional entities and reference points are a generic representation of protocol entities and reference points for use in constrained environments. Specilizations to a particular transport protocol are defined in the annexes of this specification.

\* \* \* Next Change \* \* \* \*

#### 6.4.3.X LWP entities

##### 6.4.3.X.1 LWP client

This functional entity acts as the light-weight protocol client for all transactions of the SEAL client executing in a constrained UE. A SEAL client executing in an unconstrained UE may choose to use the LWP client if it is available.

##### 6.4.3.X.2 LWP proxy

This functional entity acts as a proxy for transactions between the LWP client and one or more LWP servers. The LWP proxy typically terminates a secure transport protocol (e.g. DTLS, TLS or secure WebSocket) session on LWP-1 reference point with the LWP client of the VAL UE allowing the LWP client to establish a single secure session for transactions with multiple LWP servers that are reachable by the LWP proxy.

The LWP proxy can act as a cross-protocol LWP-HTTP proxy to enable LWP clients to access resources on HTTP servers via the LWP-HTTP-2 reference point.

The LWP proxy terminates LWP-3 reference point that lies between different LWP proxies. It may provide a topology hiding function from LWP entities outside the trust domain of the VAL system.

The LWP proxy can also terminate LWP-HTTP-3 reference point for interworking with another HTTP proxy. In this role it provides cross-protocol mapping and may provide a topology hiding function from HTTP entities outside the trust domain of the VAL system.

The LWP proxy shall be in the same trust domain as the LWP clients and LWP servers that are located within a VAL service provider's network. There can be multiple instances of a LWP proxy e.g. one per trust domain.

##### 6.4.3.X.3 LWP server

This functional entity acts as the LWP server for all LWP transactions of the SEAL server.

NOTE: A SEAL client can act as LWP server for certain transactions as required by the SEAL service.

#### 6.4.3.Y LWP usage

LWP is a generic representation of a light-weight protocol for use in constrained environments. Specializations of the light-weight protocol (LWP) functional entities and reference points to a particular protocol are defined in the annexes of this specification.

LWP is a representation of a protocol to be used by the SEAL service enablers on their respective SEAL-UU reference points when the SEAL client is executing in a constrained UE. In this case the SEAL client should use the LWP-1 reference point with the LWP proxy and should use either the LWP-2 or the LWP-HTTP-2 reference point for transport and routing of the related signalling with the SEAL server.

Editor’s note: Which procedures of a SEAL service enabler are not necessary to be supported for a constrained UE is FFS.

A SEAL client executing in a non-constrained UE may choose to use the LWP-1 reference point with the LWP proxy and may use either the LWP-2 or the LWP-HTTP-2 reference point for transport and routing of the related signalling with the SEAL server.

LWP may be used for interactions between SEAL servers on their respective SEAL-E reference points. For this usage the SEAL-E reference point shall use the LWP-1 and either the LWP-2 or the LWP-3 reference point depending on the trust relationship between the interacting SEAL servers.

\* \* \* Next Change \* \* \* \*

#### 6.5.3.X1 Reference point LWP-1 (between the LWP client and the LWP proxy)

The LWP-1 reference point exists between the LWP client and the LWP proxy.

#### 6.5.3.X2 Reference point LWP-2 (between the LWP proxy and the LWP server)

The LWP-2 reference point exists between the LWP proxy and the LWP server.

#### 6.5.3.X3 Reference point LWP-3 (between the LWP proxy and LWP proxy)

The LWP-3 reference point exists between the LWP proxy and another LWP proxy in a different network.

#### 6.5.3.X4 Reference point LWP-HTTP-2 (between the LWP proxy and the HTTP server)

The LWP-HTTP-2 reference point exists between the LWP proxy and the HTTP server.

#### 6.5.3.X5 Reference point LWP-HTTP-3 (between the LWP proxy and the HTTP proxy)

The LWP-HTTP-3 reference point exists between the LWP proxy and another HTTP proxy in a different network.

\* \* \* Next Change \* \* \* \*

Annex X (normative):
Usage of CoAP as the LWP in the signalling control plane

# X.1 General

This annex specifies the CoAP protocol as the light-weight protocol in the signalling control plane.

The Constrained Application Protocol (CoAP) is a light-weight protocol defined by IETF in RFC 7252 [refX] and designed specifically for application layer communication for constrained devices. CoAP provides a request/response interaction model between application endpoints, supports built-in discovery of services and resources, and includes key concepts of the Web such as URIs and Internet media types. CoAP is designed to easily interface with HTTP for integration with the Web while meeting specialized requirements such as multicast support, very low overhead, and simplicity for constrained environments. RFC 7252 [refX] specifies bindings to UDP and DTLS. IETF RFC 8323 [refY] specifies bindings to TCP, WebSocket and TLS.

This annex describes the usage of CoAP in the signalling control plane, in order to enable a SEAL service enabler to use CoAP on the SEAL-UU reference point.

# X.2 Signalling plane architecture including CoAP as LWP

Figure X.2-1 illustrates the functional model for the signalling control plane as shown in figure 6.2-5 when CoAP is used as the LWP.



Figure X.2-1: Functional model for signalling control plane including CoAP entities as LWP entities and reference points

# X.3 CoAP entities

## X.3.1 CoAP client

CoAP client is a specialization of the LWP client. This functional entity acts as the client for all transactions of the SEAL client executing in a constrained UE. A SEAL client executing in an unconstrained UE may choose to use the CoAP client if it is available.

NOTE: A SEAL server can act as CoAP client for certain transactions as required by the SEAL service.

## X.3.2 CoAP proxy

CoAP proxy is a specialization of the LWP proxy. This functional entity acts as a proxy for transactions between the CoAP client and one or more CoAP servers. The CoAP proxy terminates a DTLS, TLS or secure WebSocket session on LWP-1 reference point with the CoAP client of the VAL UE allowing the CoAP client to establish a single secure session for transactions with multiple CoAP servers that are reachable by the CoAP proxy.

The CoAP proxy can act as a cross-protocol CoAP-HTTP proxy to enable CoAP clients to access resources on HTTP servers via LWP-HTTP-2 reference point. HTTP-2 and LWP-HTTP-2 reference points are equivalent.

The CoAP proxy terminates LWP-3 reference point that lies between different CoAP proxies. It may provide a topology hiding function from CoAP entities outside the trust domain of the VAL system.

The CoAP proxy can also terminate LWP-HTTP-3 reference point for interworking with another HTTP proxy. In this role it provides cross-protocol mapping and may provide a topology hiding function from HTTP entities outside the trust domain of the VAL system. HTTP-3 and LWP-HTTP-3 reference points are equivalent.

The CoAP proxy shall be in the same trust domain as the CoAP clients and CoAP servers that are located within a VAL service provider's network. There can be multiple instances of a CoAP proxy e.g. one per trust domain.

NOTE: The number of instances of the CoAP proxy is deployment specific.

## X.3.3 CoAP server

CoAP server is a specialization of the LWP server. This functional entity acts as the CoAP server for all CoAP transactions of the SEAL server.

NOTE: A SEAL client can act as CoAP server for certain transactions as required by the SEAL service.

# X.4 LWP reference points description in relation to CoAP

## X.4.1 Reference point LWP-1 (between the CoAP client and the CoAP proxy)

The LWP-1 reference point in the case of CoAP exists between the CoAP client and the CoAP proxy. The LWP-1 reference point is based on CoAP (which may be secured using DTLS when run on UDP or TLS when run on TCP or WebSocket).

## X.4.2 Reference point LWP-2 (between the CoAP proxy and the CoAP server)

The LWP-2 reference point, which in the case of CoAP exists between the CoAP proxy and the CoAP server, is based on CoAP (which may be secured using DTLS when run on UDP or TLS when run on TLS).

## X.4.3 Reference point LWP-3 (between the CoAP proxy and CoAP proxy)

The LWP-3 reference point, which in the case of CoAP exists between the CoAP proxy and another CoAP proxy in a different network, is based on CoAP (which may be secured using DTLS when run on UDP or TLS when run on TLS).

# X.5 CoAP usage

CoAP is a protocol to be used by the SEAL service enablers on their respective SEAL-UU reference points when the SEAL client is executing in a constrained UE. In this case the SEAL client should use the LWP-1 reference point with the CoAP proxy and should use either the LWP-2 or the LWP-HTTP-2 reference point for transport and routing of the related signalling with the SEAL server.

A SEAL client executing in a non-constrained UE may choose to use the LWP-1 reference point with the CoAP proxy and may use either the LWP-2 or the LWP-HTTP-2 reference point for transport and routing of the related signalling with the SEAL server.

CoAP may be used for interactions between SEAL servers on their respective SEAL-E reference points. For this usage the SEAL-E reference point shall use the LWP-1 and either the LWP-2 or the LWP-3 reference point depending on the trust relationship between the interacting SEAL servers.