**3GPP TSG-CT WG3 Meeting #110eC3-203417**

**E-Meeting, 02nd – 11th June 2020** (Revision of C3-203315)

**Source: Samsung**

**Title: Pseudo-CR on Clarification on usage of TLS**

**Spec: 3GPP TS 29.549 v1.2.0**

**Agenda item: 16.27**

**Document for: Decision**

**1. Introduction**

Editor’s note (“*Usage of HTTP over TLS is based on security defined by SA3*”) in clause 6.3 needs to be resolved. SA3 has specified in TS 33.434, the usage of TLS over HTTP and the applicable TLS profiles.

**2. Reason for Change**

This pCR proposes that the usage of TLS over http should be as specified in TS 33.434.

**3. Conclusions**

<Conclusion part (optional)>

**4. Proposal**

It is proposed to agree the following changes to 3GPP TS 29.549 v1.2.0.

\* \* \* 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 23.434: "Service Enabler Architecture Layer for Verticals (SEAL); Functional architecture and information flows".

[3] 3GPP TS 29.122: "T8 reference point for Northbound Application Programming Interfaces (APIs)".

[4] IETF RFC 6455: "The Websocket Protocol".

[5] IETF RFC 7230: "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing".

[6] IETF RFC 7231: "Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content".

[7] IETF RFC 7232: "Hypertext Transfer Protocol (HTTP/1.1): Conditional Requests".

[8] IETF RFC 7233: "Hypertext Transfer Protocol (HTTP/1.1): Range Requests".

[9] IETF RFC 7234: "Hypertext Transfer Protocol (HTTP/1.1): Caching".

[10] IETF RFC 7235: "Hypertext Transfer Protocol (HTTP/1.1): Authentication".

[11] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

[12] IETF RFC 7540: "Hypertext Transfer Protocol Version 2 (HTTP/2)".

[13] IETF RFC 8259: "The JavaScript Object Notation (JSON) Data Interchange Format".

[14] 3GPP TS 29.501: "5G System; Principles and Guidelines for Services Definition; Stage 3".

[15] Open API Initiative, “OpenAPI 3.0.0 Specification”, <https://github.com/OAI/OpenAPI-Specification/blob/master/versions/3.0.0.md>.

[16] 3GPP TS 29.222: "Common API Framework for 3GPP Northbound APIs; Stage 3”.

[17] 3GPP TS 23.222: "Common API Framework for 3GPP Northbound APIs; Stage 2”.

[18] 3GPP TS 33.122: "Security Aspects of Common API Framework for 3GPP Northbound APIs".

[19] IETF RFC 6749: "The OAuth 2.0 Authorization Framework".

[20] 3GPP TS 29.523: "5G System; Policy Control Event Exposure Service; Stage 3".

[21] 3GPP TS 29.571: "5G System; Common Data Types for Service Based Interfaces; Stage 3".

[22] 3GPP TS 29.500: "5G System; Technical Realization of Service Based Architecture; Stage 3".

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

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

## 6.3 Usage of HTTP

For SEAL APIs, support of HTTP/1.1 (IETF RFC 7230 [5], IETF RFC 7231 [6], IETF RFC 7232 [7], IETF RFC 7233 [8], IETF RFC 7234 [9] and IETF RFC 7235 [10]) over TLS (IETF RFC 5246 [11]) is mandatory and support of HTTP/2 (IETF RFC 7540 [12]) over TLS (IETF RFC 5246 [11]) is recommended.

A functional entity desiring to use HTTP/2 shall use the HTTP upgrade mechanism to negotiate applicable HTTP version as described in IETF RFC 7540 [12].

Usage of HTTP over TLS and the TLS profiles shall be as specified in clause 5.1.1.4 of 3GPP TS 33.434 [AA].

\* \* \* End of Changes \* \* \* \*