**3GPP TSG-CT WG1 Meeting #133e-bisC1-220xxx**

**E-meeting, 17-21 January 2022 (was C1-220053)**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **24.109** | **CR** | **0070** | **rev** | **1** | **Current version:** | **17.0.0** |  |
|  | | | | | | | | |
| *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:*** | Adding profiles of TLS to use AKMA keys | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Qualcomm Incorporated, Nokia, Nokia Shanghai Bell | | | | | | | | | |
| ***Source to TSG:*** | C1 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | AKMA\_TLS | | | | |  | ***Date:*** | | | 2022-01-18 |
|  |  | | | |  | |  | | |  |
| ***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 can be 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:*** | | SA3 specified the use of TLS with AKMA keys (see SA3 WID in S3-212352 and SA3 CRs in S3-212353 & S3-214132). CT1 needs to specify the corresponding stage 3 details. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | An Annex was added to TS 24.109 to contain profiles of TLS using AKMA keys based on the use of TLS wth GBA keys. The main change is specifying an AKMA identifier for use instead of the GBA ones. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | The stage 3 for the use of TLS with AKMA keys will remain unspecified, leading to differing implementations and interoperability issues. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 1, 2, 3.2, Annex X (New) | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 \*\*\*

# 1 Scope

The present document defines stage 3 for the HTTP Digest AKA as specified in RFC 3310 [6] based implementation of Ub interface (UE-BSF), the Disposable-Ks model based implementation of Upa interface (NAF-UE) and the HTTP Digest as specified in RFC 7616 [36] and the PSK TLS based implementation of bootstrapped security association usage over Ua interface (UE-NAF) in Generic Authentication Architecture (GAA) as specified in 3GPP TS 33.220 [1]. The purpose of the Ub interface is to create a security association between UE and BSF for further usage in GAA applications. The purpose of the Upa interface is to provide a push mechanism to created a bootstrapped security association between the UE and NAF for secure communication of pushed messages. The purpose of the Ua interface is to use the so created bootstrapped security association between UE and NAF for secure communication.

The present document also defines stage 3 for the Authentication Proxy usage as specified in 3GPP TS 33.222 [5].

The present document also defines stage 3 for the subscriber certificate enrolment as specified in 3GPP TS 33.221 [4] which is one realization of the Ua interface. The subscriber certificate enrolment uses the HTTP Digest based implementation of bootstrapped security association usage to enrol a subscriber certificate and the delivery of a CA certificate.

The present document also defines stage 3 for TLS using AKMA (Authentication and Key Management for Applications) keys over the Ua\* interface (AKMA AF-UE) as described in 3GPP TS 33.535 [xx].

# 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 TS 33.220: "Generic Authentication Architecture (GAA); Generic bootstrapping architecture".

[2] 3GPP TR 33.919: "Generic Authentication Architecture (GAA); System description".

[3] 3GPP TS 29.109: "Generic Authentication Architecture (GAA); Zh and Zn Interfaces based on the Diameter protocol; Protocol details".

[4] 3GPP TS 33.221: "Generic Authentication Architecture (GAA); Support for Subscriber Certificates".

[5] 3GPP TS 33.222: "Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)".

[6] IETF RFC 3310: "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)".

[7] 3GPP TS 23.003: "Numbering, addressing and identification".

[8] IETF RFC 3023: "XML Media Types".

[9] Void.

[10] Void.

[11] Void.

[12] IETF RFC 2818: "HTTP over TLS".

[13] 3GPP TS 24.228 Release 5: "Signalling flows for the IP multimedia call control based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[14] Void.

[15] Void.

[16] PKCS#10 v1.7: "Certification Request Syntax Standard".

NOTE: <ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-10/pkcs-10v1_7.pdf>

[17] WAP Forum: "WPKI: Wireless Application Protocol; Public Key Infrastructure Definition"

NOTE: <http://www1.wapforum.org/tech/documents/WAP-217-WPKI-20010424-a.pdf>.

[18] Void.

[19] Open Mobile Alliance: "ECMAScript Crypto Object"

NOTE: <http://www.openmobilealliance.org>.

[20] Open Mobile Alliance: "WPKI"

NOTE: <http://member.openmobilealliance.org/ftp/public_documents/SEC/Permanent_documents/>.

[21] 3GPP TS 33.203: "3G security; Access security for IP-based services".

[22] IETF RFC 2234: "Augmented BNF for Syntax Specifications: ABNF".

[23] Void.

[24] 3GPP TS 33.223: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) Push function".

[25] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[26] Open Mobile Alliance Push Enabler Release v2.2: "Push Over the Air".

NOTE: <http://www.openmobilealliance.org/Technical/release_program/push_v2_2.aspx>.

[27] Open Mobile Alliance Push Enabler Releasev 2.2: "Push Message Specification".

NOTE: <http://www.openmobilealliance.org/Technical/release_program/push_v2_2.aspx>.

[28] Open Mobile Alliance Device Management Enabler Release v1.2: "Enabler Release Definition for OMA Device Management".

NOTE: <http://www.openmobilealliance.org/Technical/release_program/dm_v1_2.aspx>.

[29] 3GPP TS 33.303: "Proximity-based Services (ProSe); Security aspects".

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

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

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

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

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

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

[36] IETF RFC 7616: "HTTP Digest Access Authentication".

[37] IETF RFC 4648: "The Base16, Base32, and Base64 Data Encodings".

[xx] 3GPP TS 33.535: "Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS)".

\*\*\* Next change \*\*\*

## 3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

A-KID AKMA Key IDentifier

AKA Authentication and Key Agreement

AKMA Authentication and Key Management for Applications

AP Authentication Proxy

AS Application Server

AUTN Authentication Token

AUTS Re-synchronisation Token

AV Authentication Vector

BSF BootStrapping Function

B-TID Bootstrapping - Transaction IDentifier

CA Certification Authority

CK Confidentiality Key

DER Distinquished Encoding Rules

FQDN Fully Qualified Domain Name

GAA Generic Authentication Architecture

GBA Generic Bootstrapping Architecture

GBA\_ME ME-based GBA

GBA\_U GBA with UICC-based enhancements

GPI GBA Push Info

GUSS GBA User Security Settings

HSS Home Subscriber System

HTTP Hypertext Transfer Protocol

HTTPS HTTP over TLS

IK Integrity Key

IMPI IP Multimedia Private Identity

IMPU IP Multimedia PUblic identity

Ks Key material

Ks\_NAF NAF specific key material

MAC Message Authentication Code

ME Mobile Equipment

NAF Network Application Function

PKCS Public-Key Cryptography Standards

PKI Public Key Infrastructure

PSK Pre-Shared Secret

RAND RANDom challenge

RES authentication Response

SA Security Association

SQN SeQuence Number

TLS Transport Layer Security

TMPI Temporary IP Multimedia Private Identity

UE User Equipment

UICC Universal Integrated Circuit Card

URI Uniform Resource Identifier

URN Uniform Resource Name

USIM User Service Identity Module

USS User Security Settings

UTC Coordinated Universal Time

WIM Wireless Identity Module

WPKI Wireless PKI

WTLS Wireless Transport Layer Security

XRES Expected authentication response

\*\*\* Next change \*\*\*

Annex X (normative):  
TLS with AKMA profiles

# X.1 General

This Annex provides the details of how to apply TLS with AKMA keys (see 3GPP TS 33.535 [xx]) based on the procedures in clauses 5.3.2 and 5.3.3.

# X.2 Shared key-based UE authentication with certificate-based AF authentication

The TLS profile for GBA in clause 5.3.2.1 is modified with the AKMA AF taking the role of the NAF from GBA (see 3GPP TS 33.220 [1]) to support AKMA keys as follows:

- the UE and the AF shall support the TLS version as specified in annex E of 3GPP TS 33.310 [25]. See clause 5.3.1 in 3GPP TS 33.222 [5] for the detailed profiling of TLS.

a) when the UE starts communication via Ua\* reference point with the AF, it shall establish a TLS tunnel with the AF. The AF is authenticated to the UE by means of a public key certificate. The UE shall verify that the server certificate corresponds to the FQDN of the AF with which it established the tunnel. No client authentication is performed as part of TLS (no client certificate necessary).

b) the UE sends an HTTP request to the AF inside the TLS tunnel (HTTPS, i.e. HTTP over TLS) as described in clause 5.2 with the following changes:

1) the UE shall indicate to an AF that it supports AKMA based HTTP Digest authentication by including a "product" token, that is a constant string "3gpp-akma",in the "User-Agent" header (see RFC 7231 [31]) in outgoing HTTP requests; and

2) the AF may decide to authenticate the UE using AKMA-based shared secret by executing the authentication procedure. This is indicated in the "realm" parameter of the WWW-Authenticate header field. The realm attribute shall contain the constant string "3GPP-bootstrapping-akma". If the AF has a choice between GBA\_Digest (see 3GPP TS 33.220 [1]) and AKMA keying, then the AF shall select AKMA over GBA\_Digest.

c) the UE shall generate the HTTP request and the AF shall authenticate the HTTP request using HTTP Digest. HTTP Digest authentication (see RFC 3310 [6]) shall be used with previously bootstrapped security association as follows:

1) the "username" parameter shall be the A-KID;

2) the password used in the digest calculations shall be KAF (AKMA Application Key) with the KAF Base64 encoded as specified in RFC 4648 [37]; and

3) the "realm" parameter shall contain two parts delimited by "@" sign where the first part is the constant string "3gpp-akma" and the latter part shall be the FQDN of the AF (e.g. "[3gpp-akma@af1.operator.com](mailto:3gpp-akma@naf1.operator.com)"); and

d) both the UE and the AF shall verify upon receiving each of the HTTP responses and HTTP requests that the second part of the realm attribute is equal to the FQDN of the AF.

The authentication failures are supported as described in clause 5.3.2.2.

Clauses 5.3.2.3 and 5.3.2.4 are not supported as AKMA does not support deriving a fresh key in the same way as GBA.

NOTE: Key refresh for AKMA requires a new primary authentication and cannot be triggered independently by the application layer.

# X.3 Shared key-based mutual authentication between UE and AF

## X.3.1 General

The TLS profile for GBA in clause 5.3.3.1 is modified with the AKMA AF taking the role of the NAF from GBA (see 3GPP TS 33.220 [1]) to support AKMA keys as follows:

- The profile for TLS and TLS Extensions to be used together with PSK TLS is defined in annex E of 3GPP TS 33.310 [25].

## X.3.2 TLS 1.2

- The PSK TLS handshake shall be used with bootstrapped security association as follows:

a) the ClientHello message shall contain one or more PSK-based ciphersuites;

b) the ClientHello message shall contain the server\_name TLS extension and it shall contain the hostname of the AF;

c) the ServerHello message shall contain a PSK-based ciphersuite selected by the AF;

d) the ServerKeyExchange shall be sent by the server and it shall contain the psk\_identity\_hint field and it shall contain the static string "3GPP-AKMA";

e) the ClientKeyExchange shall contain the psk\_identity field and it shall contain a prefix "3GPP-AKMA" and the A-KID. If the UE has a choice between GBA\_Digest (see 3GPP TS 33.220 [1]) and AKMA keying, then the AF shall select AKMA over GBA\_Digest; and

f) the UE and AF shall derive the TLS premaster secret from KAF (AKMA Application Key).

The authentication failures are supported as described in clause 5.3.3.2.

Clauses 5.3.3.3 and 5.3.3.4 are not supported as AKMA does not support deriving a fresh key in the same way as GBA.

NOTE: Key refresh for AKMA requires a new primary authentication and cannot be triggered independently by the application layer.

## X.3.3 TLS 1.3

Editor's note (WI AKMA\_TLS, CR#0070): The contents of this subclause are FFS and will be added when the use of GBA with TLS 1.3 is specified.

\*\*\* End of changes \*\*\*