**3GPP TSG-CT WG1 Meeting #132-eC1-215680\_r1**

**E-meeting, 11-15 October 2021**

**3GPP TSG-CT WG3 Meeting #118-eC3-215046\_r1**

**E-Meeting, 11th – 15th October 2021**

**3GPP TSG-CT WG4 Meeting #106-eC4-215154\_r1**

**E-Meeting, 11th – 15th October 2021**

(revision of CP-yyxxxx)

**Source: Ericsson**

**Title: New WID on Enhancements of 3GPP profiles for cryptographic algorithms and security protocols**

**Document for: Approval**

**Agenda Item: 17.1.1 (CT1, CT3) / 5 (CT4)**

3GPP™ Work Item Description

Information on Work Items can be found at <http://www.3gpp.org/Work-Items>   
See also the [3GPP Working Procedures](http://www.3gpp.org/specifications-groups/working-procedures), article 39 and the TSG Working Methods in [3GPP TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm)

# Title: Enhancements of 3GPP profiles for cryptographic algorithms and security protocols

## Acronym: eCryptPr

## Unique identifier:

Potential target Release: Rel-17

## 1 Impacts

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Affects:** | UICC apps | ME | AN | CN | Others (specify) |
| **Yes** |  | X |  | X |  |
| **No** | X |  | X |  | X |
| **Don't know** |  |  |  |  |  |

## 2 Classification of the Work Item and linked work items

### 2.1 Primary classification

|  |  |
| --- | --- |
|  | Feature |
| X | Building Block |
|  | *Work Task* |
|  | Study Item |

### 2.2 Parent Work Item

|  |  |  |  |
| --- | --- | --- | --- |
| Parent Work / Study Items | | | |
| Acronym | Working Group | Unique ID | Title (as in 3GPP Work Plan) |
| eCryptPr | SA3 | 910024 | Enhancements of 3GPP profiles for cryptographic algorithms and security protocols |

### 2.3 Other related Work Items and dependencies

|  |  |  |
| --- | --- | --- |
| Other related Work Items (if any) | | |
| Unique ID | Title | Nature of relationship |
| 860017 | 3GPP profiles for cryptographic algorithms and security protocols | SA3 Work Item in Release 16 which updated the 3GPP security protocol profiles for security algorithms to:   * remove support for non-recommended TLS cipher suites; * remove references to deprecated protocols (including TLS 1.1) in 3GPP specifications; * follow minimum requirements and best practice on TLS extensions. |

**Dependency on non-3GPP (draft) specification**:

- Internet draft draft-ietf-tls-dtls13: " The Datagram Transport Layer Security (DTLS) Protocol Version 1.3".

## 3 Justification

3GPP specifications use several security protocols from other standards bodies. For each of these protocols, the 3GPP security protocol profiles specify which version, options, extensions, and cryptographic algorithms to support and use. In addition to updates from IETF, attacks and recommendations on how to use these protocols are published by academia and other organizations. The 3GPP security protocol profiles need to be regularly updated to stay up to date and remain secure.

The IMS specifications make use of algorithms such as MD5, SHA-1, and key exchange without Diffie-Hellman, which are weak and no longer recommended to use.

TLS 1.0 and TLS 1.1 do not support any secure cipher suites and has several weaknesses. IETF published RFC 8996 which forbids negotiation and use of TLS 1.0 and TLS 1.1 everywhere. RFC 8996 also deprecates DTLS 1.0. SA3 deprecated TLS 1.0 and 1.1, and DTLS 1.0.

The eCryptPr WID in SA3, specifies the update of cryptographic algorithms and the 3GPP security protocol profiles for security algorithms, considering the following:

- Update the usage of (D)TLS according to other standards bodies' works, e.g., new IETF works.

- Add new strong and recommended algorithms in the IMS specifications and deprecate cryptographic algorithms considered weak where possible.

- Add default certificate profiles to the 3GPP security protocol profiles. Add statement that the 3GPP security profile apply for all uses of (D)TLS to protect 3GPP interfaces unless otherwise stated.

- Specify a profile of TLS 1.3 to use with GBA.

Within the eCryptPr WID SA3 specified support of HTTP Digest Access Authentication according to RFC 7616 and RFC 7235 instead of obsoleted RFC 2617; and also specified support of HTTP/1.1 according to RFC 7230 instead of obsoleted RFC 2616. As consequence, SIP Digest Access Authentication should be supported according to RFC 8760 instead of RFC 3261 and RFC 2617.

In light of these, impacts on protocols and interfaces under CT WGs' responsibilities are foreseen and need to be specified.

NOTE: Changes from HTTP/1.1 according to the obsoleted RFC 2616 are not related to security aspects only and are available from:

<https://datatracker.ietf.org/doc/html/rfc7230#appendix-A.2>

<https://datatracker.ietf.org/doc/html/rfc7231#appendix-B>

<https://datatracker.ietf.org/doc/html/rfc7232#appendix-A>

<https://datatracker.ietf.org/doc/html/rfc7233#appendix-B>

<https://datatracker.ietf.org/doc/html/rfc7234#appendix-A>

<https://datatracker.ietf.org/doc/html/rfc7235#appendix-A>

## 4 Objective

The objective of this work item is to update the specifications under remit of CT WGs to align with the requirements agreed under the SA3 work item eCryptPr.

For CT1, the expected work includes:

- Remove references to deprecated protocols TLS 1.0 which is forbidden to support in 3GPP.

- Align support of TLS with SA3 agreed TLS profile.

- Specify support of HTTP Digest according to RFC 7616 and RFC 7235 instead of RFC 2617.

- Specify support of SIP Digest according to RFC 8760 instead of RFC 2617.

- Specify support of base encoding of data according to RFC 4648 instead of RFC 3548.

- Specify support of HTTP/1.1 according to RFC 7230 and RFC 7231 instead of RFC 2616.

NOTE 1: Support of HTTP/1.1 according to RFC 7230 is already specified in some CT1 TSs (e.g. TS 24.334, 24.282).

For CT3, the expected work includes:

- Align support of TLS with SA3 agreed TLS profile.

- Update support of HTTP Digest according to RFC 7616 and RFC 7235 instead of RFC 2617.

NOTE 2: In CT3 TSs support of HTTP/1.1 is specified only according to RFC 7230 and associated RFCs 7231 – 7235.

For CT4, the expected work includes:

- Remove references to deprecated protocols TLS 1.0 which is forbidden to support in 3GPP.

- Align support of TLS with SA3 agreed TLS profile.

- Update support of SIP Digest according to RFC 8760 instead of RFC 2617.

- Specify support of base encoding of data according to RFC 4648 instead of RFC 3548.

- Specify support of HTTP/1.1 according to RFC 7230 instead of RFC 2616.

## 5 Expected Output and Time scale

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| New specifications | | | | | |
| Type | TS/TR number | Title | For info  at TSG# | For approval at TSG# | Rapporteur |
|  |  |  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Impacted existing TS/TR | | | |
| TS/TR No. | Description of change | Target completion plenary# | Remarks |
| 24.109 | Update to:   * specify support of HTTP Digest according to RFC 7616 and RFC 7235 instead of RFC 2617; * specify support of base encoding of data according to RFC 4648 instead of RFC 3548; * specify support of HTTP/1.1 according to RFC 7230 instead of RFC 2616. | TSG CT#95 (March 2022) | CT1 responsibility |
| 24.141 | Update to:   * specify support of HTTP Digest according to RFC 7616 and RFC 7235 instead of RFC 2617; * specify support of HTTP/1.1 according to RFC 7230 instead of RFC 2616. | TSG CT#95 (March 2022) | CT1 responsibility |
| 24.229 | Update to:   * specify support of SIP Digest according to RFC 8760 instead of RFC 2617; * specify support of HTTP/1.1 according to RFC 7230 instead of RFC 2616. | TSG CT#95 (March 2022) | CT1 responsibility |
| 24.481 | Update to:   * specify support of HTTP/1.1 according to RFC 7230 instead of RFC 2616. | TSG CT#95 (March 2022) | CT1 responsibility |
| 24.482 | Update to:   * specify support of HTTP/1.1 according to RFC 7230 instead of RFC 2616. | TSG CT#95 (March 2022) | CT1 responsibility |
| 24.486 | Update to:   * specify support of HTTP/1.1 according to RFC 7230 instead of RFC 2616. | TSG CT#95 (March 2022) | CT1 responsibility |
| 24.545 | Update to:   * specify support of HTTP/1.1 according to RFC 7230 instead of RFC 2616. | TSG CT#95 (March 2022) | CT1 responsibility |
| 24.547 | Update to:   * specify support of HTTP/1.1 according to RFC 7230 instead of RFC 2616. | TSG CT#95 (March 2022) | CT1 responsibility |
| 24.548 | Update to:   * specify support of HTTP/1.1 according to RFC 7230 instead of RFC 2616. | TSG CT#95 (March 2022) | CT1 responsibility |
| 24.623 | Update to:   * remove reference to TLS 1.0 (RFC 2246;) * specify support of HTTP Digest according to RFC 7616 and RFC 7235 instead of RFC 2617; * specify support of HTTP/1.1 according to RFC 7230 instead of RFC 2616. | TSG CT#95 (March 2022) | CT1 responsibility |
| 29.079 | Update to:   * remove RFC 2617. | TSG CT#95 (March 2022) | CT3 responsibility |
| 29.122 | Align support of TLS with SA3 agreed TLS profiles. | TSG CT#95 (March 2022) | CT3 responsibility |
| 29.222 | Update to:   * specify support of HTTP Digest according to RFC 7616 and RFC 7235 instead of RFC 2617. * Align support of TLS with SA3 agreed TLS profiles. | TSG CT#95 (March 2022) | CT3 responsibility |
| 29.486 | Align support of TLS with SA3 agreed TLS profiles. | TSG CT#95 (March 2022) | CT3 responsibility |
| 29.517 | Align support of TLS with SA3 agreed TLS profiles. | TSG CT#95 (March 2022) | CT3 responsibility |
| 23.008 | Update to:   * specify support of SIP Digest according to RFC 8760 instead of RFC 2617; * specify support of base encoding of data according to RFC 4648 instead of RFC 3548. | TSG CT#95 (March 2022) | CT4 responsibility |
| 29.228 | Update to:  specify support of SIP Digest according to RFC 8760 instead of RFC 2617. | TSG CT#95 (March 2022) | CT4 responsibility |
| 29.229 | Update to:  specify support of SIP Digest according to RFC 8760 instead of RFC 2617. | TSG CT#95 (March 2022) | CT4 responsibility |
| 29.240 | Update to:   * remove reference to TLS 1.0 (RFC 2246;) * specify support of HTTP/1.1 according to RFC 7230 instead of RFC 2616. | TSG CT#95 (March 2022) | CT4 responsibility |
| 23.333 | Align support of TLS with SA3 agreed TLS profiles. | TSG CT#95 (March 2022) | CT4 responsibility |
| 29.333 | Align support of TLS with SA3 agreed TLS profiles. | TSG CT#95 (March 2022) | CT4 responsibility |
| 29.334 | Align support of TLS with SA3 agreed TLS profiles. | TSG CT#95 (March 2022) | CT4 responsibility |

## 6 Work item Rapporteur(s)

Biondic, Nevenka, Ericsson, nevenka.biondic@ericsson.com

## 7 Work item leadership

CT1

## 8 Aspects that involve other WGs

None

## 9 Supporting Individual Members

|  |
| --- |
| Supporting IM name |
| Ericsson |
| NCSC |
| NTT DOCOMO |
| Nokia |
| Nokia Shanghai Bell |
|  |