|  |
| --- |
|  |

|  |  |
| --- | --- |
| CHANGE REQUEST | |
| Meeting ID:\* | SEC#31 |
| Source:\* | Saïd GHAROUT, Orange, said.gharout@orange.com |
| Date:\* | 2017-09-20 |
| Reason for Change/s:\* | Mirror version for the agreed SEC-2017-140R02 CR for Rel3 |
| CR against: Release\* | 2 |
| CR against: WI\* | Active <Work Item number>  MNT maintenance / < Work Item number(optional)>  Is this a mirror CR? Yes  No  mirror CR number: (Note to Rapporteur - use latest agreed revision)  STE Small Technical Enhancements  Only ONE of the above shall be ticked |
| CR against: TS/TR\* | TS-0003 v2.10.0 |
| Clauses \* | 2.1, 8.5.3.3 |
| Type of change: \* | Editorial change  Bug Fix or Correction  Change to existing feature or functionality  New feature or functionality  Only ONE of the above shall be ticked |
| Impacted other TS/TR(s) |  |
| Post Freeze checking:\* | This CR contains only essential changes and corrections? YES  NO  This CR may break backwards compatibility with the last approved version of the TS? YES  NO |
| Template Version: January 2017 (Do not modify) | |

**oneM2M Notice**

The document to which this cover statement is attached is submitted to oneM2M. Participation in, or attendance at, any activity of oneM2M, constitutes acceptance of and agreement to be bound by terms of the Working Procedures and the Partnership Agreement, including the Intellectual Property Rights (IPR) Principles Governing oneM2M Work found in Annex 1 of the Partnership Agreement.

## Introduction

To accommodate different regulations, it is necessary to support different elliptic curves, in addition to the existing ones.

### -----------------------Start of change 1-------------------------------------------

# 2 References

## 2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non‑specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

The following referenced documents are necessary for the application of the present document.

[1] oneM2M TS-0001: "Functional Architecture".

[2] oneM2M TS-0011: "Common Terminology".

[3] Void.

[4] oneM2M TS-0004: "Service Layer Core Protocol Specification".

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

[6] IETF RFC 6347: "Datagram Transport Layer Security Version 1.2".

[7] ETSI TS 102 225 (V11.0.0): "Smart Cards; Secured packet structure for UICC based applications (Release 11)".

[8] ETSI TS 102 226 (V11.0.0): "Smart Cards; Remote APDU structure for UICC based applications (Release 11)".

[9] 3GPP TS 31.115 (V10.1.0): "Remote APDU Structure for (U)SIM Toolkit applications (Release 10)".

[10] 3GPP TS 31.116 (V10.2.0): "Remote APDU Structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications (Release 10)".

[11] 3GPP2 C.S0078-0 (V1.0): "Secured packet structure for CDMA Card Application Toolkit (CCAT) applications".

[12] 3GPP2 C.S0079-0 (V1.0): "Remote APDU Structure for CDMA Card Application Toolkit (CCAT) applications".

[13] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)".

[14] 3GPP2 S.S0109-A: "Generic Bootstrapping Architecture (GBA) Framework".

[15] IETF RFC 4279: "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)".

[16] Void.

[17] Void.

[18] IETF RFC 5705: "Keying Material Exporters for Transport Layer Security (TLS)".

[19] IETF RFC 3629: "UTF-8, a transformation format of ISO 10646".

[20] "Unicode Standard Annex #15; Unicode Normalization Forms", Unicode 5.1.0, March 2008.

NOTE: Available at <http://www.unicode.org>.

[21] GlobalPlatform Device Technology TEE Administration framework, DRAFT.

[22] GlobalPlatform Device Technology TEE System Architecture, Version 1.0.

[23] ETSI TS 102 671: "Smart Cards; Machine to Machine UICC; Physical and logical characteristics".

[24] ETSI TS 102 221: "Smart Cards; UICC-Terminal interface; Physical and logical characteristics".

[25] ETSI TS 102 484: "Smart Cards; Secure channel between a UICC and an end-point terminal".

[26] ISO/IEC 7816-4: "Identification cards - Integrated circuit cards - Part 4: Organization, security and commands for interchange".

[27] ETSI TS 101 220: "Smart Cards; ETSI numbering system for telecommunication application providers".

[28] Void.

[29] Void.

[30] Void.

[31] IETF RFC 6655: "AES-CCM Cipher Suites for Transport Layer Security (TLS)".

[32] IETF RFC 5289: "TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)".

[33] IETF RFC 2104: "HMAC: Keyed-Hashing for Message Authentication".

[34] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[35] IETF RFC 6960: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".

[36] IETF RFC 6961: "The Transport Layer Security (TLS) Multiple Certificate Status Request Extension".

[37] IETF RFC 7250: "Using Raw Public Keys in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)".

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

[39] National Institute of Standards and Technology (July 1999): "Recommended Elliptic Curves for Federal Government user".

NOTE: Available at <http://csrc.nist.gov/groups/ST/toolkit/documents/dss/NISTReCur.pdf>.

[40] IETF RFC 6920: "Naming Things with Hashes".

[41] IETF RFC 3548: "The Base16, Base32, and Base64 Data Encodings".

[42] IETF RFC 5487: "Pre-Shared Key Cipher Suites for TLS with SHA-256/384 and AES Galois Counter Mode".

[43] IETF RFC 4492: "Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)".

[44] IETF RFC 6066: "Transport Layer Security (TLS) Extensions: Extension Definitions".

[45] IETF RFC 7251: "AES-CCM Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)".

[46] IETF RFC 5480: "Elliptic Curve Cryptography Subject Public Key Information".

[47] GlobalPlatform Device Technology Secure Element Remote Application Management v1.0 GPD\_SPE\_008.

[48] IETF RFC 5869: HMAC-based Extract-and-Expand Key Derivation Function (HKDF).

[49] IETF RFC 7518 (2015): "JSON Web Algorithms (JWA)".

[50] IETF RFC 7516: "JSON Web Encryption (JWE)", 2015.

[51] IETF RFC 7515: "JSON Web Signature (JWS)", 2015.

[52] W3C Recommendation: "XML Signature Syntax and Processing v1.1", 2013.

NOTE: Available at <http://www.w3.org/TR/xmlsig-core1/>.

[53] IETF RFC 7519: "JSON Web Token (JWT)", 2015.

[54] OpenID Foundation: "OpenID Connect Core 1.0", 2014.

[55] W3C Recommendation: "XML Encryption Syntax and Processing v1.1", 2013.

NOTE: Available at <http://www.w3.org/TR/xmlenc-core1/>.

[56] IETF RFC 5652: "Cryptographic Message Syntax (CMS)", September 2009.

[57] oneM2M TS-0022: "Field Device Configuration”.

[58] oneM2M TS-0032: "MAF and MEF Interface Specification”.

[59] IETF RFC 7030, “Enrollment over Secure Transport”.

[60] IETF Historic draft: “Simple Certificate Enrollment Protocol”, draft-nourse-scep-23

NOTE: Available at <https://tools.ietf.org/html/draft-nourse-scep-23>

[61] IETF Historic draft: “Simple Certificate Enrollment Protocol”, draft-gutmann-scep-05

NOTE: Available at: <https://www.ietf.org/id/draft-gutmann-scep-05.txt>.

[X] SOG-IS: “SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms”, Version 1.0, May 2016.

[Y] RFC 5639 . Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation.

### -----------------------End of change 1---------------------------------------------

### -----------------------Start of change 2-------------------------------------------

#### 8.5.3.3 Signature-Only ESData Security Class Protocol Details

To maintain consistency, signature types are provided which are available in both XML-Signature [52] and JSON Web Signature (JWS) [51].

* HMAC using SHA-256, SHA-384 or SHA-512.
* RSA signature using PKCS1-v1.5 and MGF1with SHA-256, SHA-384 or SHA-512.
* ECDSA signature using P-256, P-384 or P-512 with SHA-256, SHA-284 or SHA-512 respectively.
* ECDSA signature using FRP256v1 or brainpoolP256r1 curves [X] with SHA-256 for both curves.

Table 8.5.3.3-1 identifies the algorithms that are supported in XML-SIG for Signature-only ESData Security Class.

Table 8.5.3.3-1: Algorithms that are supported in XML-Signature for  
Signature-only ESData Security Class

|  |  |  |  |
| --- | --- | --- | --- |
| Signature Type | Algorithm | | <SignatureMethod Algorithm=".."> |
| HMAC | SHA-256 | | <http://www.w3.org/2001/04/xmldsigmore#hmacsha256> |
| SHA-384 | | <http://www.w3.org/2001/04/xmldsigmore#hmacsha384> |
| SHA-512 | | <http://www.w3.org/2001/04/xmldsigmore#hmacsha512> |
| RSA | RSA PKCS1-v1.5 and MGF1 with: | SHA-256 | <http://www.w3.org/2001/04/xmldsigmore#rsasha256> |
| SHA-384 | <http://www.w3.org/2001/04/xmldsigmore#rsasha384> |
| SHA-512 | <http://www.w3.org/2001/04/xmldsigmore#rsasha512> |
| ECDSA | P-256 and SHA-256 | | http://www.w3.org/2001/04/xmldsigmore#ecdsasha256 |
| P-384and SHA-384 | | http://www.w3.org/2001/04/xmldsigmore#ecdsasha384 |
| P-512 and SHA-512 | | http://www.w3.org/2001/04/xmldsigmore#ecdsasha512 |
| FRP256v1 and SHA-256 | | See |X] |
| brainpoolP256r1 and SHA-256 | | See [Y] |

The XML-Signature object may be transported "plain" - with no encoding, or may be encoded in base64.

Table 8.5.3.3-2 identifies the algorithms that are supported in JWS for Signature-only ESData Security Class.

Table 8.5.3.3-2: Algorithms that are supported in JSON Web Signature (JWS) for  
Signature-only ESData Security Class

|  |  |  |  |
| --- | --- | --- | --- |
| Signature Type | Algorithm | | "alg":".." |
| HMAC | SHA-256 | | HS256 |
| SHA-384 | | HS384 |
| SHA-512 | | HS512 |
| RSA | RSA PKCS1-v1.5 and MGF1 with: | SHA-256 | RS256 |
| SHA-384 | RS384 |
| SHA-512 | RS512 |
| ECDSA | P-256 and SHA-256 | | ES256 |
| P-384and SHA-384 | | ES384 |
| P-512 and SHA-512 | | ES512 |

The output generated by JWS conforms to either the JWS JSON Serialization or a URI-safe JWS Compact Serialization. The JWS JSON Serialization may be transported "plain" – with no encoding, or may be encoded in base64. oneM2M TS-0004 [4] defines the datatype m2m:e2eCompactJWS for the JWS Compact Serialization.

### -----------------------End of change 2---------------------------------------------