ETSI TS 103 816-1 V1.1.1 (2021-07)

Publicly Available Specification (PAS);
CYBER;
Connecting Products based on MIKEY-SAKKE;
Part 1: KMS Certificate Definition

CAUTION

The present document has been submitted to ETSI as a PAS produced by Secure Chorus and approved by the ETSI Technical Committee Cyber Security (CYBER).

Reference
DTS/CYBER-0065-1

Keywords
cyber security, mobile, PAS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Cyber Security (CYBER).

The present document is part 1 of a multi-part deliverable covering Connecting Products based on MIKEY-SAKKE, as identified below:

Part 1: "KMS Certificate Definition";

Part 2: "One-to-One Voice Communication";

Part 3: "One-to-One Messaging";

Part 4: "Group Voice Communication";

Part 5: "Discovery".

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document is intended to specify the Key Management Server (KMS) Certificate used for sharing security credentials between KMS domains. It is intended for use in connecting domains of products based on Multimedia Internet Keying Sakai-Kasahara Key Encryption (MIKEY-SAKKE) using separate KMSs.

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 referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference/.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

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

[1] IETF RFC 6507 (February 2012): "Elliptic Curve-Based Certificateless Signatures for Identity-Based Encryption (ECCSI)", M. Groves.

[2] IETF RFC 6508 (February 2012): "Sakai-Kasahara Key Encryption (SAKKE)"; M. Groves.

[3] IETF RFC 6509 (February 2012): "MIKEY-SAKKE: Sakai-Kasahara Key Encryption in Multimedia Internet KEYing (MIKEY), M. Groves.

[4] IETF RFC 5480 (March 2009): "Elliptic Curve Cryptography Subject Public Key Information", S. Turner, D. Brown, K. Yiu, R. Housley, T. Polk.

[5] ETSI TS 133 179 (V13.1.0): "LTE; Security of Mission Critical Push To Talk (MCPTT) over LTE (3GPP TS 33.179 version 13.1.0 Release 13)".

[6] IETF RFC 3987 (January 2005): "Internationalized Resource Identifiers (IRIs)", M. Duerst, M. Suignard.

2.2 Informative 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 referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

Not applicable.

3 Definition of terms, symbols and abbreviations

3.1 Terms

Void.

3.2 Symbols

Void.

3.3 Abbreviations

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

3GPP	3rd Generation Partnership Project
ECCSI	Elliptic Curve-based Certificateless Signatures for Identity-based encryption
IETF	Internet Engineering Task Force
KMS	Key Management Server
KPAK	KMS Public Authentication Key
LTE	Long-Term Evolution
MCPTT	Mission-Critical Push-To-Talk
MIKEY	Multimedia Internet Keying
RFC	Request For Comments
SAKKE	Sakai-Kasahara Key Encryption
UE	User Equipment
UID	Unique Identifier
URI	Uniform Resource Identifier
UTF	Unicode Transformation Format
XML	eXtensible Markup Language

4 MIKEY-SAKKE KMS Certificate

4.1 Description

A KMS Certificate is a certificate that applies to an entire domain of users. A Certificate consists of eXtensible Markup Language (XML) containing the information necessary to encrypt messages to a domain of users and verify signatures from the domain of users.

It is assumed that the User Equipment (UE) is managed by a single KMS, the UE's Root KMS. This Root KMS is the only KMS which provisions the UE. The KMS certificate of the Root KMS is known as the Root KMS certificate. This certificate is necessary to encrypt to the UE, and verify signatures of UE (as well as others within the domain).

The Root KMS may also provision a number of external KMS certificates to allow inter-domain communications.

4.2 Fields

The KMS Certificate shall be named a 'KmsCertificate' within the XML. This type shall have the following subfields:

Name	Description
Version	(Attribute) The version number of the certificate type (1.0.0).
Role	(Attribute) This indicates whether the certificate is a "Root" or "External" certificate.
CertUri	The URI of the Certificate (this object).
KmsUri	The URI of the KMS which issued the Certificate.
Issuer	String describing the issuing entity.
ValidFrom	Date from which the Certificate may be used.

Name	Description
ValidTo	Date at which the Certificate expires.
Revoked	A Boolean value defining whether this Certificate has been revoked.
UserIDFormat	A string denoting how MIKEY-SAKKE UserIDs should be constructed. This shall be '1' where Tel-URIs are used as defined in IETF RFC 6509 [3].
PubEncKey	The SAKKE Public Key, 'Z', as defined in IETF RFC 6508 [2]. This is an OCTET STRING encoding of an elliptic curve point as defined in section 2.2 of IETF RFC 5480 [4].
PubAuthKey	The ECCSI Public Key, 'KPAK' as defined in IETF RFC 6507 [1]. This is an OCTET STRING encoding of an elliptic curve point as defined in section 2.2 of IETF RFC 5480 [4].
KmsDomainList	(OPTIONAL) List of domains which the KMS manages.
ParameterSet	(OPTIONAL) The ParameterSet supported by the KMS Certificate. If not present, shall be assumed to be '1'.
NOTE 1: The fields above are defined for consistency with The 3rd Generation Partnership Project (3GPP) specification (clause D.3.2.2 of ETSI TS 133 179 [5]), but fields listed as "optional" may be blank. NOTE 2: ETSI TS 133 179 [5] extends the certificate for UserIDFormat 2 and the extended subfields provided in ETSI TS 133 179 [5] may be included in the KMS Certificate but may be ignored by Vendor Product clients.	

The *KmsUri* shall be unique per logical KMS and in the format <unique string>.<vendor domain>/<display community name>.

The *KmsUri* shall support UTF-8 characters as defined in IETF RFC 3987 [6] to allow meaningful display names, e.g. de453f5ffdd.vendor.org/User%20Group.

The unique string element is vendor implementation specific, but is unique to the KMS, and should therefore change when the master secret changes, e.g. random number, hash(Z || KPAK).

4.3 MIKEY-SAKKE User IDs

To secure communications with a specific user, the initiator shall compose the MIKEY-SAKKE User Identifier (UID) to which the message will be encrypted. Clients shall support MIKEY-SAKKE RFC [3] identifier format, denoted by the value '1'.

ETSI TS 133 179 [5] defines an identifier format for URIs. Clients may support the identifier format defined in ETSI TS 133 179 [5], denoted by the value '2'. Where the identifier format defined in ETSI TS 133 179 [5] is used, clients shall use KMS certificate version "1.1" defined in ETSI TS 133 179 [5].

4.4 XML Schema for KMS Certificate

```
<xsd:element name = "SignedKmsCertificate" type = "SignedKmsCertificateType"/>
<xsd:complexType name = "SignedKmsCertificateType">
    <xsd:sequence>
        <xsd:element name = "KmsCertificate" type = "KmsCertificateType"/>
        <xsd:element ref = "ds:Signature" minOccurs = "0"/>
    </xsd:sequence>
    <xsd:anyAttribute namespace = "##other" processContents = "lax"/>
</xsd:complexType>

<xsd:element name = "KmsCertificate" type = "KmsCertificateType"/>
<xsd:complexType name = "KmsCertificateType">
    <xsd:sequence>
        <xsd:element type = "xsd:anyURI" name = "CertUri" maxOccurs = "1"/>
        <xsd:element type = "xsd:anyURI" name = "KmsUri" maxOccurs = "1"/>
        <xsd:element type = "xsd:string" name = "Issuer" maxOccurs = "1" />
        <xsd:element type = "xsd:dateTime" name = "ValidFrom" maxOccurs = "1"/>
        <xsd:element type = "xsd:dateTime" name = "ValidTo" maxOccurs = "1"/>
        <xsd:element type = "xsd:boolean" name = "Revoked" maxOccurs = "1"/>
        <xsd:element type = "xsd:positiveInteger" name = "UserIdFormat" maxOccurs = "1"/>
        <xsd:element type = "xsd:hexBinary" name = "PubEncKey" maxOccurs = "1"/>
        <xsd:element type = "xsd:hexBinary" name = "PubAuthKey" maxOccurs = "1"/>
        <xsd:element name = "KmsDomainList" maxOccurs = "1">
            <xsd:complexType>
                <xsd:sequence>
                    <xsd:element type = "xsd:anyURI" name = "KmsDomain" maxOccurs = "unbounded"/>
                </xsd:sequence>
            </xsd:complexType>
        </xsd:element>
```

```
        <xsd:element type = "xsd:positiveInteger" name = "ParameterSet" maxOccurs = "1" minOccurs =
"0"/>
        <xsd:any namespace = "##other" processContents = "lax" minOccurs = "0" maxOccurs =
"unbounded"/>
    </xsd:sequence>
    <xsd:attribute name = "Id" type = "xsd:string"/>
    <xsd:attribute name = "Version" type = "xsd:string" fixed="1.0.2"/>
    <xsd:attribute name = "Role" type = "RoleType"/>
    <xsd:anyAttribute namespace = "##other" processContents = "lax"/>
</xsd:complexType>

<xsd:simpleType name = "RoleType">
    <xsd:restriction base = "xsd:string">
        <xsd:enumeration value = "Root"/>
        <xsd:enumeration value = "External"/>
    </xsd:restriction>
</xsd:simpleType>
```

History

Document history		
V1.1.1	July 2021	Publication