ETSI TS 103 816-5 V1.1.1 (2021-07)

Publicly Available Specification (PAS);
CYBER;
Connecting Products based on MIKEY-SAKKE;
Part 5: Discovery

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-0065-5

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 5 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 method and computer interface used for secure communication between two users of products based on Multimedia Internet Keying Sakai-Kasahara Key Encryption (MIKEY-SAKKE). It is intended for ensuring a Key Management Server (KMS) is able to securely query other KMSs, with the aim of discovering which KMS a given user - known by its UserID as defined in ETSI TS 103 816-2 [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 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] ETSI TS 103 816-2: "Publicly Available Specification (PAS); CYBER; Connecting Products based on MIKEY-SAKKE; Part 2: One-to-One Voice Communication".

[2] ETSI TS 103 816-1: "Publicly Available Specification (PAS); CYBER; Connecting Products based on MIKEY-SAKKE; Part 1: KMS Certificate Definition".

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

[4] ETSI TS 133 180 (V15.2.0): "LTE; Security of the mission critical service (3GPP TS 33.180 version 15.2.0 Release 15)".

[5] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2". T. Dierks, E. Rescorla. August 2008.

[6] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3". E. Rescorla. August 2018.

[7] IETF RFC 4279: "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)". P. Eronen, Ed. H. Tschofenig, Ed. December 2005.

[8] BCP106: "Randomness Requirements for Security". D. Eastlake, 3rd, J. Schiller, S. Crocker. June 2005.

[9] IETF RFC 3275: "(Extensible Markup Language) XML-Signature Syntax and Processing". D. Eastlake 3rd, J. Reagle, D. Solo. March 2002.

[10] ETSI TS 133 220: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) (3GPP TS 33.220)".

[11] ISO 8601:2004(E): "Data elements and interchange formats - Information interchange - Representation of dates and times". December 2004.

NOTE: ISO 8601:2004 has been updated by ISO 8601-1:2019 and ISO 8601-2:2019.

[12] W3C® Recommendation 15 March 2001: "Canonical XML Version 1.0".

NOTE: Available at http://www.w3.org/TR/2001/REC-xml-c14n-20010315.

[13] W3C® Recommendation 10 December 2002: "XML Encryption Syntax and Processing".

NOTE: Available at https://www.w3.org/TR/2002/REC-xmlenc-core-20021210/Overview.html#sha256.

[14] IETF RFC 4051: "Additional XML Security Uniform Resource Identifiers (URIs)".

NOTE: https://www.w3.org/2001/04/xmldsig-more#hmac-sha256.

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
GAA	Generic Authentication Architecture
GBA	Generic Bootstrapping Architecture
HMAC	Hash-based Message Authentication Code
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
KDF	Key Derivation Function
KLF	KMS Lookup Function
KMS	Key Management Server

NOTE: The system distributing keys to users or other vendors.

MC	Mission Critical
MCX	Mission Critical Services
MIKEY	Multimedia Internet KEYing
RFC	Request For Comments
SAKKE	SAkai-Kasahara Key Encryption
SIP	Session Initiation Protocol

SPK	Signalling Protection Key
TLS	Transport Layer Security
UE	User Equipment
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
XML	eXtensible Markup Language
XPK	XML Protection Key
XPK-ID	XML Protection Key IDentifier

4 Overview

Any given user of a Vendor Product is managed by one or more KMSs. As defined in IETF RFC 6509 [3] such a KMS acts as a root of trust and distributor of key material, providing the user with its unique private keys, and all the information it requires to ensure it is able to encrypt data for other users managed by this KMS.

While it may be the case that two users wishing to communicate with one another belong to the same KMS, there may also be scenarios where those separate user groups of Vendor Products are managed by separate KMSs. For further information about the protocols and technologies used to enable connectivity between separate networks of Vendor Products where users are managed by separate KMSs, please refer to the following documents: ETSI TS 103 816-2 [1] and the ETSI TS 103 816-1 [2].

ETSI TS 103 816-2 [1] and the ETSI TS 103 816-2 [1] make the assumption that an initiating client has knowledge of the user's identity that is trying to reach and the details of that user's KMS. Both the user's identity on the responding client and the details of its KMS, together form the essential knowledge required to encrypt data for a given user of a Vendor Product.

A discovery process is shall however be used in the scenario where the initiating client and the responding client are managed by separate KMSs and the initiating client has access to the user identity on the responding client (which was derived by prior knowledge of a phone number, for example), however has no information relating to which KMS manages the responding client. In practice, such a process would entail the initiating client's KMS securely querying all other known and trusted KMSs to discover which KMS manages the responding client.

Once the initiating client obtains knowledge of the responding client's KMS, the KMS Certificates that were previously exchanged can be used to provide the initiating client with all required detail to encrypt data for the responding client. Please further note that the KMS Certificates are defined in ETSI TS 103 816-1 [2]

In order for a KMS to query all known KMSs securely, the following methodologies shall be used:

1) how to query a KMS; and

2) how to secure any KMS to KMS communication.

Both methodologies have recently been investigated by the 3rd Generation Partnership Project (3GPP) for the purposes of Mission Critical Services (MCX), detailed in ETSI TS 133 180 [4]. The present document references the following approaches provided in ETSI TS 133 180 [4].

Clause 5.3.3 of ETSI TS 133 180 [4] provides procedures whereby certain messages can be sent and received to a KMS via HyperText Transfer Protocol (HTTP) requests. The process defined in ETSI TS 133 180 [4], clause 5.3.3 provides a type of message entitled "KMS Lookup" defined as follows:

> *KMS Lookup: This message is to lookup the external KMS that should be used for a provided Session Initialisation Protocol (SIP) Uniform Resource Identifier (URI).*

This type of request is to be used when a user queries its own KMS to discover which KMS should be used for a given SIP URI. An example of this message is provided in clause D.2.7 of ETSI TS 133 180 [4], where the HyperText Transfer Protocol (HTTP) request Uniform Resource Locator (URL) includes the identity of the SIP URI, and is provided as:

> *…/keymanagement/identity/v1/lookup/user%40example.org*

The protection of such messages is further defined in ETSI TS 133 180 [4], clause 4.3.3, where the communication is secured via Transport Layer Security (TLS):

> *the UE connection to the KMS is over HTTP and hence is secured using TLS directly between the Mission Critical (MC) client and KMS or between the MC client and the HTTP proxy or directly to the KMS. When the HTTP proxy is in the path between the MC client and the KMS, key material is wrapped using a Transport Key (TrK) distributed out-of-band (reference clause 5.3.2). The TrK or a shared Integrity Key (InK) may be used to sign the key material.*

ETSI TS 133 180 [4] also provides a mechanism for securing communication between MCX signalling servers, for the purposes of call signalling, where a Signalling Protection Key (SPK) has been previously, and manually, provisioned. This is provided in ETSI TS 133 180 [4], clause 5.5.

An eXtensible Markup Language (XML) Protection Key (XPK) is further defined in ETSI TS 133 180 [4] clause 9.3.3. The SPK can be used to encrypt and sign XML data, providing confidentiality and integrity in the communication of XML data between servers. When the SPK is used for this purpose, the term "XPK" is used. This XPK itself is not directly a signing key or an encryption key. A key derivation function is used to obtain the signing and encryption key from the XPK. This key derivation function is provided in clause 9.2.3 of ETSI TS 133 180 [4].

The present document specifies an "HTTP interface" which allow certain secure requests from one KMS to another via HTTP protected with TLS. The present document is limited to specifying the interface between two KMSs. The present document does not however specify the interface between a given user and its KMS, as this is not required to archive interoperability between Vendor Products. The interface is however specified in a way that is compliant with the "KMS Lookup interface" defined in 3GPP and which specifies the communication between a user with its KMS in MCX. This was done in order to maximize possible future interoperability between a Vendor Product KMS and a MCX KMS.

The present document also provides the mechanism for assuring the integrity of the data being exchanged between Vendor Product KMSs. It does so by referring to the 3GPP approach for securing XML databetween signalling servers in MCX. This is to ensure compliance with common industry approaches to providing integrity to XML data, as well as to maximize possible future interoperability between a Vendor Product KMS and a MCX KMS.

5 Inter-domain communication

5.1 HTTP Interface

A Vendor Product KMS shall provide an HTTP endpoint which shall be secured via TLS 1.2 as defined by IETF RFC 5246 [5]

The endpoint may implement TLS 1.3 as defined in IETF RFC 8446 [6]. The KMS may also support TLS Pre-Shared Keys (TLS-PSK) in accordance to IETF RFC 4279 [7].

The TLS Certificate shall be signed. It may be signed by a root authority, or it may be self-signed.

Where the HTTP endpoint is provided as https://domain:port/keymanagement/identity/v1/lookup it shall resolve a query to https://domain:port/keymanagement/identity/v1/lookup/userid, where "userid" is the URL-encoded "tel URI" of the user as defined in IETF RFC 6509 [3].

NOTE: For example for the user uniquely identified as tel:+123, a responding KMS would respond to https://domain:port/keymanagement/identity/v1/lookup/tel:%2B123.

5.2 XML Protection Key

A Vendor Product KMS shall generate a 128-bit key, the XPK. The KMS shall generate a separate XPK for each of the KMSs it desires to establish a secure communication channel with (each KMS if "federates" with). The XPK shall be generated by the Vendor Product KMS using a cryptographically secure random number generator. Guidance on random number generation can be found in BCP106 [8].

A Vendor Product KMS shall also generate a 32-bit XPK-ID. The 4 most significant bits (the purpose tag) of the XPK-ID shall be set to "3". The 28 least significant bits of the XPK-ID shall be a 28-bit randomly generated number.

All XML Data shall be signed using SHA-256 HMAC as defined in IETF RFC 3275 [9], with a HMAC length of 128 bits. The HMAC input key shall be derived from the XPK using the Key Derivation Function (KDF) provided in ETSI TS 133 220 [10], annex B, with the following parameters.

- FC = 0x52 (for signalling plane integrity).
- P0 = Originating KMS URI.
- L0 = length of above, expressed in number of bytes.
- P1 = XPK-ID.
- L1 = length of above, expressed in number of bytes (i.e. 0x00 0x20).

5.3 Setup

To enable secure communication between Vendor Products, each Vendor Product KMS shall provide the following set of data ("credentials") to any external KMS with which it wishes to federate:

- KMS Certificate [2]
- TLS certificate for the KMS Server and TLS-PSK keys if desired
- KMS lookup domain, port and address of the endpoint, where the domain shall match the domain provided in the TLS certificate
- SIP Server Address and Port
- SIP Domain of the users of the KMS
- XPK
- XPK-ID

The exchange of this information is performed manually by administrators of each KMS. The process of exchanging the above information is outside the scope of the present document.

Once the data listed above is exchanged, a KMS shall attempt a TLS connection to the endpoint of the federated KMS, in order to ensure the validity of the TLS certificate.

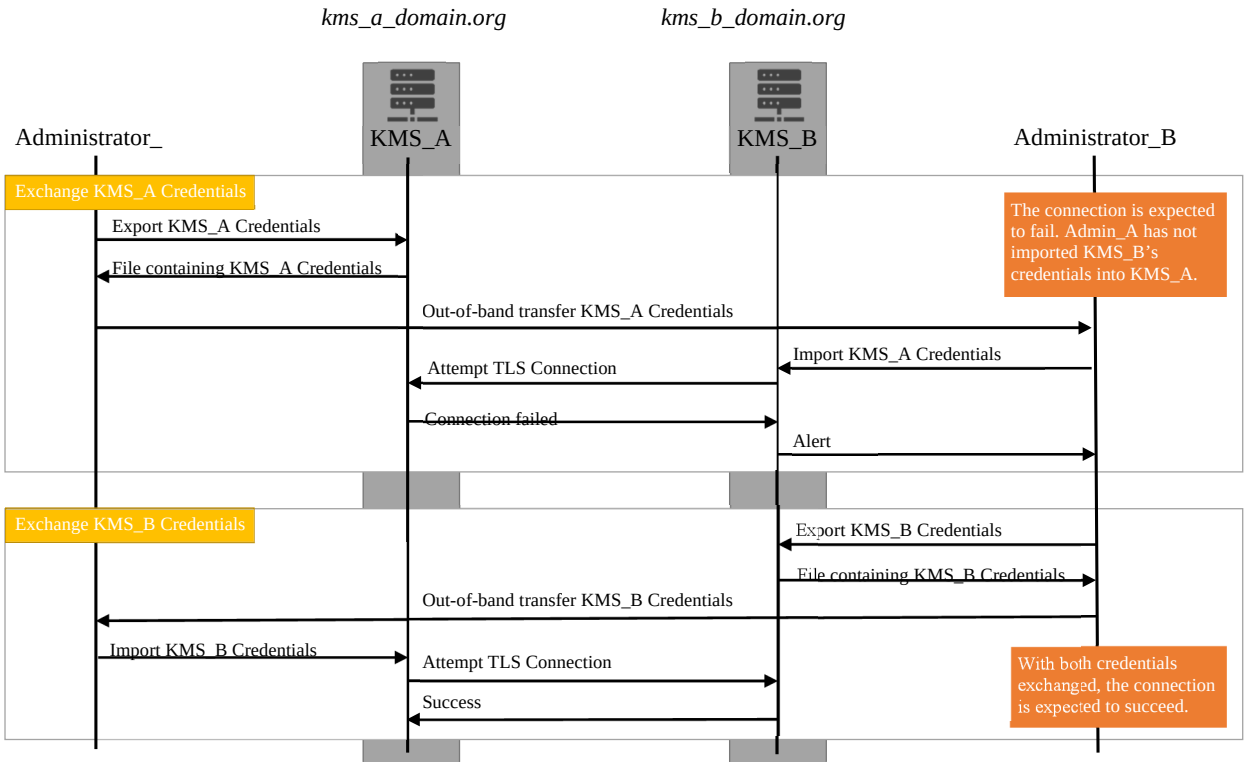

Figure 1: KMS credentials exchange

6 Discovery procedure

6.1 Discovery call flow

In order for an initiating client to obtain the required data to establish a communication session, the initiating client's KMS may need to query one or more trusted KMSs with which it has already setup a secure communication channel.

For example, the initiating client user "Alice" managed by KMS_A wishes to initiate a secure phone call with the responding client user "Bob" known to Alice as "+456" and managed by KMS_B.

In this scenario, Alice's software will query KMS_A for details of the security domain of +456. As +456 is not a user of KMS_A, the KMS will have to undertake the discovery process to identify which KMS, if any, has +456 as a user.

KMS_A has previously setup a communication channel with KMS_B, as it has exchanged credentials with KMS_B.

KMS_A queries KMS_B's Lookup endpoint, thus performing the "KMS Lookup Function" (KLF).

NOTE: The communication mechanism between a user and their KMS is out of scope for the present document.

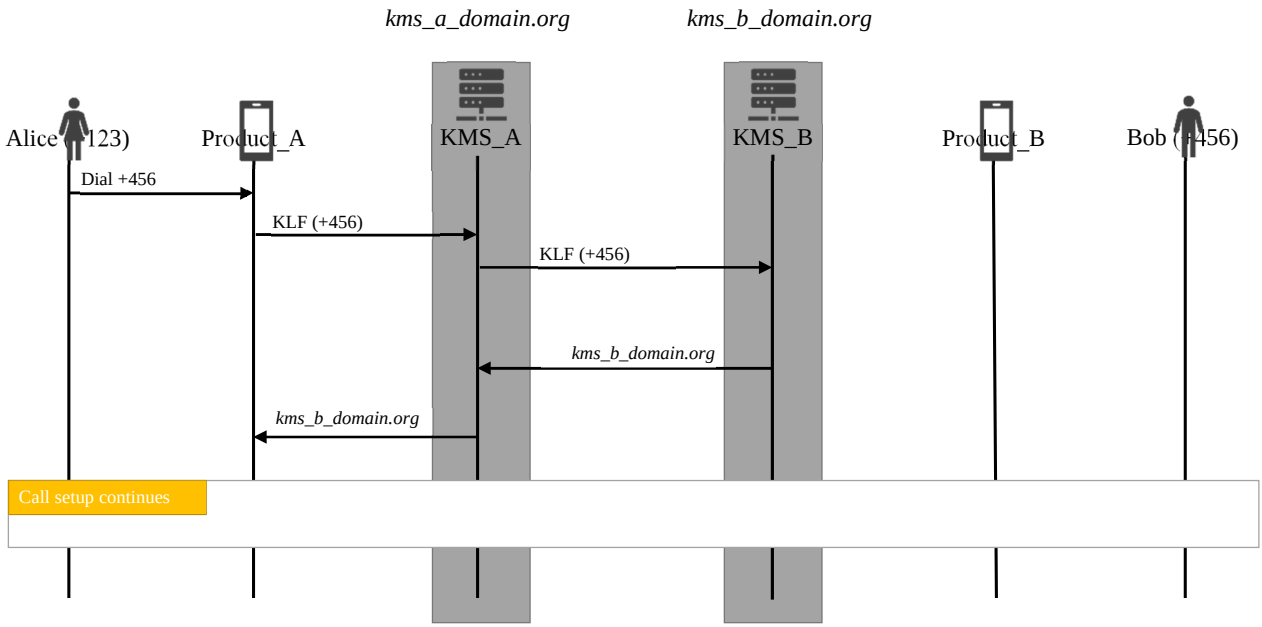

Figure 2: Example discovery call flow

6.2 XML Request

6.2.1 XML Request format

The requesting KMS shall send an HTTPS POST request to the endpoint with a SHA-256 HMAC signed requesting XML document, and include the following HTTP headers:

Content-type: text/xml

6.2.2 Fields

Table 1: KMS Request Certificate Subfields

Name	Description
Version	(Attribute) The version number of the certificate type (1.0.0)
UserUri	The URI of the requesting KMS
KmsUri	The URI of the responding KMS
Time	The time of the request in ISO 8601 format [11]
ClientReqURL	The URL that was queried
CanonicalizationMethod Algorithm	(Attribute) The value http://www.w3.org/TR/2001/REC-xml-c14n-20010315 [12]
Signature Method Algorithm	(Attribute) as defined in [100] http://www.w3.org/2001/04/xmldsig-more#hmac-sha256 [14]
HMACOutputLength	128
DigestMethod Algorithm	http://www.w3.org/2001/04/xmlenc#sha256 [13]
DigestValue	The SHA-256 digest as defined in IETF RFC 3275 [9]
SignatureValue	The HMAC-signed signature as defined in IETF RFC 3275 [9] using the key derived from the XPK, using the KDF
KeyName	The XPK-ID

6.2.3 XML Schema

```
<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
      <xs:element name="UserUri" type="xs:string"/>
      <xs:element name="KmsUri" type="xs:string"/>
      <xs:element name="Time" type="xs:dateTime"/>
      <xs:element name="ClientReqUrl" type="xs:string"/>
```

```
      <xs:element name="KmsRequest">
         <xs:complexType>
            <xs:sequence>
                 <xs:element ref="UserUri"/>
                 <xs:element ref="KmsUri"/>
                 <xs:element ref="Time"/>
                 <xs:element ref="ClientReqUrl"/>
            </xs:sequence>
            <xs:attribute type="xs:string" name="Id"/>
            <xs:attribute type="xs:string" name="Version"/>
         </xs:complexType>
      </xs:element>
      <xs:element name="SignedKmsRequest">
         <xs:complexType>
            <xs:sequence>
                 <xs:element ref="KmsRequest"/>
                 <xs:element ref="xd:Signature"xmlns:xd="http://www.w3.org/2000/09/xmldsig#"/>
            </xs:sequence>
         </xs:complexType>
      </xs:element>
</xs:schema>
```

6.3 XML Response

6.3.1 XML Response format

The responding KMS shall ensure the requesting address matches the KMS endpoint domain provided during the credentials exchange which occurred prior to responding to the POST request. The responding KMS may send a response or it may block incoming connections from other originating address at the network layer (for example through the use of a firewall).

If the responding KMS provides a response, it shall be a 200 OK HTTP response in which case it shall be provided with the following headers.

Content-type: text/xml

The response shall be signed with a SHA-256 HMAC signed payload as defined in clause 5.2 and shall embed one or more KmsLookupResult fields. Each one of these shall correspond to a KMS which manages the user. The subfield "*KmsUri"* shall provide the URI of the KMS which manages the requested user.

In the event the responding KMS does not wish to provide information about a given user, or it has no knowledge of a given user, it may provide a response wherein the "*KmsUri"* subfield is an empty string, in which case the KmsLookupResult field containing the empty KmsUri subfield shall be the single and only instance of the KmsLookupResult field.

The KmsLookupResult also has an attribute "*Id"* which shall match the responding KMS's URI, thereby providing a mechanism whereby a responding KMS may provide a response to the query on behalf of another KMS, should it wish to do so. The requesting KMS may then choose to query that KMS in turn, to avoid querying further KMS, or may choose to trust the responding KMS directly.

6.3.2 Fields

The KMS request shall be named a "SignedKmsResponse" within the XML. This type shall have the following subfields as shown in table 2.

Table 2: KMS Response Certificate Subfields

Name	Description
Version	(Attribute) The version number of the certificate type (1.0.0)
UserUri	The URI of the requesting KMS
KmsUri	The URI of the responding KMS
Time	The time of the response in ISO 8601 format [11]
ClientReqURL	The URL that was queried
KmsMessage Version	(Attribute) 1.0.0
KmsLookup Version	(Attribute) 1.0.0
KMSLookupResult	One or more responses to the request
KmsLookupResult Version	(Attribute) 1.0.0
KmsLookupResult Id	The KMS URI of the responding KMS
UserUri	The URI of the requested user
KmsUri	The URI of the KMS for the requested user (if known) or an empty string
CanonicalizationMethod Algorithm	(Attribute) The value http://www.w3.org/TR/2001/REC-xml-c14n-20010315 [12]
Signature Method Algorithm	(Attribute) As defined in [100] http://www.w3.org/2001/04/xmldsig-more#hmac-sha256 [14]
HMACOutputLength	128
DigestMethod Algorithm	http://www.w3.org/2001/04/xmlenc#sha256 [13]
DigestValue	The SHA-256 digest as defined in IETF RFC 3275 [9]
SignatureValue	The HMAC-signed signature as defined in IETF RFC 3275 [9] using the key derived from the XPK, using the KDF
KeyName	The XPK-ID

6.3.3 XML Schema

```
<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
    <xs:element name="UserUri" type="xs:string"/>
    <xs:element name="KmsUri" type="xs:string"/>
    <xs:element name="KmsLookupResult">
       <xs:complexType>
            <xs:sequence>
                <xs:element ref="UserUri"/>
                <xs:element ref="KmsUri"/>
            </xs:sequence>
            <xs:attribute type="xs:string" name="Version"/>
            <xs:attribute type="xs:string" name="Id"/>
       </xs:complexType>
    </xs:element>
    <xs:element name="KmsLookup">
       <xs:complexType>
            <xs:sequence>
                <xs:element ref="KmsLookupResult"/>
            </xs:sequence>
            <xs:attribute type="xs:string" name="Version"/>
       </xs:complexType>
    </xs:element>
    <xs:element name="Time" type="xs:dateTime"/>
    <xs:element name="ClientReqUrl" type="xs:string"/>
    <xs:element name="KmsMessage">
       <xs:complexType>
            <xs:sequence>
                <xs:element ref="KmsLookup"/>
            </xs:sequence>
            <xs:attribute type="xs:string" name="Version"/>
       </xs:complexType>
    </xs:element>
    <xs:element name="KmsResponse">
       <xs:complexType>
            <xs:sequence>
                <xs:element ref="UserUri"/>
                <xs:element ref="KmsUri"/>
                <xs:element ref="Time"/>
                <xs:element ref="ClientReqUrl"/>
                <xs:element ref="KmsMessage"/>
            </xs:sequence>
            <xs:attribute type="xs:string" name="Id"/>
            <xs:attribute type="xs:string" name="Version"/>
       </xs:complexType>
```

```
    </xs:element>
    <xs:element name="SignedKmsResponse">
       <xs:complexType>
            <xs:sequence>
                <xs:element ref="KmsResponse"/>
                <xs:element ref="xd:Signature" xmlns:xd="http://www.w3.org/2000/09/xmldsig#"/>
            </xs:sequence>
       </xs:complexType>
    </xs:element>
</xs:schema>
```

Annex A (normative): Examples

A.1 Example: XML Request example

```
<?xml version="1.0" encoding="UTF-8"?>
<SignedKmsRequest xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <KmsRequest Id="xmldoc" Version="1.0.0">
    <UserUri>kms.avon.org</UserUri>
    <KmsUri> kms.brent.org</KmsUri>
    <Time>2018-09-17T10:01:19Z</Time>
    <ClientReqUrl>https://kms.brent.org:3000/keymanagement/identity/v1/lookup/tel%3A%2B456</ClientReq
    Url>
  </KmsRequest>
  <Signature
     xmlns="http://www.w3.org/2000/09/xmldsig#">
     <SignedInfo>
        <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
        <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#hmac-sha256">
           <HMACOutputLength>128</HMACOutputLength>
        </SignatureMethod>
        <Reference URI="#xmldoc">
           <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
           <DigestValue>o0P3NgaMyjM+78y4x8oPQVuRQdK1EST2y7FftP1RFbg=</DigestValue>
        </Reference>
     </SignedInfo>
     <SignatureValue>fFxnUUFs2HxoyKqfHd7vGg==</SignatureValue>
     <KeyInfo>
        <KeyName>34fe23ef</KeyName>
     </KeyInfo>
  </Signature>
</SignedKmsRequest>
```

A.2 Example: XML Response

```
<?xml version="1.0" encoding="UTF-8"?>
<SignedKmsResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <KmsResponse Id="xmldoc" Version="1.0.0">
    <UserUri>kms.avon.org</UserUri>
    <KmsUri>kms.brent.org</KmsUri>
    <Time>2017-11-27T13:39:58+00:00</Time>
    <ClientReqUrl>https://kms.brent.org:3000/keymanagement/identity/v1/lookup/tel%3A%2B456</ClientReq
    Url>
    <KmsMessage Version="1.0.0">
  <KmsLookup Version="1.0.0" xsi:type="se:KmsLookupTkType">
      <KmsLookupResult Version="1.0.0" Id="kms.brent.org">
                <UserUri>tel:+456</UserUri>
                <KmsUri>kms.brent.org</KmsUri>
             </KmsLookupResult>
         </KmsLookup>
     </KmsMessage>
  </KmsResponse>
  <Signature
    xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
       <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
       <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#hmac-sha256">
          <HMACOutputLength>128</HMACOutputLength>
       </SignatureMethod>
       <Reference URI="#xmldoc">
          <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
          <DigestValue>o0P3NgaMyjM+78y4x8oPQVuRQdK1EST2y7FftP1RFbg=</DigestValue>
       </Reference>
    </SignedInfo>
    <SignatureValue>fFxnUUFs2HxoyKqfHd7vGg==</SignatureValue>
    <KeyInfo>
       <KeyName>34fe23ef</KeyName>
    </KeyInfo>
```

```
  </Signature>
</SignedKmsResponse>
```

A.3 Example: Key Derivation Function Test Vectors

A.3.1 Introduction

The example provided below shows a key derivation using the key derivation function specified in ETSI TS 133 220 [10], in Annex B. The input to which are the XPK and the string S.

A.3.2 Example input to the Key Derivation Function

A sample string S is constructed as per ETSI TS 133 220 [10] in clause A.2, with the parameters as follows. For this example, an originating KMS URI of "kms.example.org" and a random XPK-ID are used.

REPRESENTATION (XPK-ID)	L1	FC					P0 (KMS DOMAIN)						L0	P1
HEXADECIMAL	52	6B 78 65	6D 61 2E	73 6D 6F	2E 70 72	65 6C 67	00	0F	39	28	73	0C	00	04
NUMERICAL	82	N/A					15		N/A				4	
STRING	N/A	kms.example.org					N/A		N/A				N/A	

Resulting in S with the following value in hexadecimal notation:

526B 6D 73 2E 65 78 61 6D 70 6C 65 2E 6F 72 67 00 0F 39 28 73 0C 00 04

A sample random XPK is provided as follows in hexadecimal notation:

07 36 F2 EA 20 B6 49 11 8D 15 93 01 45 83 CD D4

A.3.3 Expected output from the Key Derivation Function

The derived output of the KDF is as follows in hexadecimal notation:

B3 24 C5 99 08 F1 6A BC 84 80 6C 43 AC 21 2D E7 93 0B E7 61 52 49 3E D4 E5

1C 01 58 7D 9A 00 F9

The derived key is the 128 least significant bits as follows in hexadecimal notation:

93 0B E7 61 52 49 3E D4 E5 1C 01 58 7D 9A 00 F9

History

Document history		
V1.1.1	July 2021	Publication