

1 An X-KISS Extension for Digital 2 Signature Verification

3 1 Introduction

4 This submission defines an extension to the XKMS X-KISS protocol that supports the verification
5 of digital signatures.

6 2 Terminology

7 The key words *must*, *must not*, *required*, *shall*, *shall not*, *should*, *should not*, *recommended*, *may*,
8 and *optional* in this document are to be interpreted as described in [RFC2119].

9 3 Protocol Elements

10 3.1 Schema Header and Namespace Declarations

11 The following schema fragment defines the XML namespaces and other header information for
12 the digital signature verification schema:

```
13 <?xml version="1.0" encoding="UTF-8"?>  
14 <xs:schema targetNamespace="sigver"  
15 xmlns:ds="http://www.w3.org/2000/09/xmldsig#"  
16 xmlns:xs="http://www.w3.org/2001/XMLSchema"  
17 xmlns:xkms="http://www.w3.org/2002/03/xkms#"  
18 elementFormDefault="qualified" attributeFormDefault="unqualified">  
19 <xs:import namespace="http://www.w3.org/2002/03/xkms#"  
20 schemaLocation="xkms.xsd"/>  
21 <xs:import namespace="http://www.w3.org/2000/09/xmldsig#"  
22 schemaLocation="http://www.w3.org/TR/2002/REC-xmldsig-core-  
23 20020212/xmldsig-core-schema.xsd"/>
```

24 3.2 <ToBeVerifiedSignature> Element

25 The <ToBeVerifiedSignature> element specifies the signature to be verified by the X-KISS
26 server. It is included as a child of a <xkms:QueryKeyBinding> or <xkms:KeyBinding>
27 element in a signature verification request or response. It includes one of the following elements
28 and attributes:

29 <EnvelopingSignature>

30 This element is used when verification of an encapsulating signature is required. It is of
31 type `<SignatureType>` and contains the encapsulating signature to be verified.

32 `<EnvelopedSignature>`

33 This element is used when verification of an encapsulated signature is required. It is of
34 type `<ObjectType>` and contains the encapsulated signature to be verified.

35 `<DetachedSignature>`

36 This element is used when verification of a detached signature is required. It is a
37 sequence of a `<ds:Signature>` element, which contains the detached signature and a
38 `<ds:Object>` element which contains the object that is signed.

39 `<SignatureAndHash>`

40 This element is used to convey just a signature and the message digest, or hash, or the
41 data that was signed. It consists of a sequence of the `<ds:SignatureValue>` which is
42 the actual signature computed, the `<ds:SignatureMethod>` which indicates the type
43 of signature, the `<ds:KeyInfo>` which can be used to verify the signature, and a
44 `<ds:DigestValue>` element, which contains the hash (usually of a
45 `<ds:SignedInfo>` element) that is used as input to the signature generation algorithm.
46 Use of the `<ds:SignatureAndHash>` element would support constrained environments
47 where submitting the entire signed data is not appropriate, or allow signatures to be
48 verified on private data that should not be disclosed to third parties.

49 `<SignatureReference>`

50 This element is used when the signature is external to this element. It is of type
51 `<RetrievalMethodType>` and includes the URI of the signature to be retrieved and
52 verified.

53 `<NonXMLSignature>`

54 This element is used when verification of signature that is not an XML Signature is
55 required (e.g. CMS signature). It contains a sequence of `<ds:Object>` which will
56 contain the signature and data to be verified.

57 `SignaturePath`

58 This attribute contains a URI which points to (usually using Xpath/Xpointer) the signature
59 to be verified. This optional attribute only needs to be used when either the
60 `<xkms:KeyInfo>` element or the `<xkms:UseKeyWith>` element within the
61 `<xkms:ValidateRequest>` message cannot be used to uniquely identify the signature
62 to be verified.

63 `VerificationTime`

64 When used in a request, this attribute, if present, indicates the time that the server should
65 use as the signing time in the signature verification algorithm. When used in a response,
66 it indicates the time that was used in the signature verification algorithm.

67 The following schema fragment defines the `<ToBeVerifiedSignature>` element:

```
68 <xs:element name="ToBeVerifiedSignature">  
69   <xs:complexType>  
70     <xs:choice>  
71       <xs:element name="EnvelopingSignature"  
72         type="ds:SignatureType" />
```

```

73 <xs:element name="EnvelopedSignature" base="ds:Object" type="ds:ObjectType" />
74 <xs:element name="DetachedSignature">
75 <xs:complexType>
76 <xs:sequence>
77 <xs:element ref="ds:Signature" />
78 <xs:element ref="ds:Object" />
79 </xs:sequence>
80 </xs:complexType>
81 </xs:element>
82 <xs:element name="SignatureAndHash">
83 <xs:complexType>
84 <xs:sequence>
85 <xs:element ref="ds:SignatureValue" />
86 <xs:element ref="ds:SignatureMethod" />
87 <xs:element ref="ds:KeyInfo" />
88 <xs:element ref="ds:DigestValue" />
89 </xs:sequence>
90 </xs:complexType>
91 </xs:element>
92 <xs:element name="SignatureReference"
93 type="ds:RetrievalMethodType" />
94 <xs:element name="NonXMLSignature">
95 <xs:complexType>
96 <xs:sequence>
97 <xs:element ref="ds:Object" />
98 </xs:sequence>
99 </xs:complexType>
100 </xs:element>
101 </xs:choice>
102 <xs:attribute name="SignaturePath" type="xs:anyURI"
103 use="optional" />
104 <xs:attribute name="VerificationTime" type="xs:dateTime"
105 use="optional" />
106 </xs:complexType>
107 </xs:element>

```

108 4 Request and Response Syntax and Processing

109 These are requirements on the relying party.

110 4.1 Request Syntax and Processing

111 A request to verify an XML Digital Signature consists of a `<xkms:ValidateRequest>` message
112 with the following restrictions.

113 If multiple signatures are present on the object, then either the `<xkms:KeyInfo>` element or the
114 `<xkms:UseKeyWith>` element **MUST** contain sufficient information to uniquely identify one of
115 the signers or the `SignaturePath` attribute **MUST** be used to point to the signature to be
116 verified. The response will then return the status of the signature created by that signer.

117 The `<xkms:KeyUsage>` field **MUST** contain only the value `xkms:Signature`.

118 The `<xkms:QueryKeyBinding>` element **MUST** contain exactly one instance of a
119 `<ToBeVerifiedSignature>` element, which **MUST** contain the signature to be verified.

120 4.2 Response Syntax and Processing

121 A response to a request to verify an XML Digital Signature consists of a <xkms:ValidateResult>
122 message with the following restrictions.

123 Either the <xkms:KeyInfo> and <xkms:UseKeyWith> elements MUST refer to exactly one
124 signature on the object or the *SignaturePath* attribute MUST be used to point to the signature
125 that was verified.

126 The <xkms:KeyUsage> field MUST contain only the value *xkms:Signature*.

127 At least one <xkms:Reason> element MUST include the value *EESignature*. The description
128 of this reason code is "The Signature on signed data provided by the client in the
129 <ToBeVerifiedSignature> element was successfully verified."

130 The <xkms:KeyBinding> element MUST contain exactly one instance of a
131 <ToBeVerifiedSignature> element, which MUST contain the signature that was verified.

132 5 Verification Server Requirements

133 These are requirements on the X-KISS Signature Verification Server.

134 TBD.

135 6 References

136 6.1 Normative

- 137 [RFC2119] S. Bradner, *Key words for use in RFCs to Indicate Requirement Levels*,
138 <http://www.ietf.org/rfc/rfc2119.txt>, IETF RFC 2119, March 1997.
- 139 [RFC3161] C. Adams, P. Cain, D. Pinkas, R. Zuccherato, *Internet X.509 Public Key*
140 *Infrastructure Time Stamp Protocols*, <http://www.ietf.org/rfc/rfc3161.txt>,
141 RFC 3161, August 2001.
- 142 [XKMS] P. Hallam-Baker, XML Key Management Specifications (XKMS 2.0),
143 <http://www.w3.org/2001/XKMS/Drafts/XKMS/xkms-part1.html>.
- 144 [XMLSig] D. Eastlake et al., XML-Signature Syntax and Processing,
145 <http://www.w3.org/TR/xmlsig-core/>, World Wide Web Consortium.
- 146