Encoding Options for Key Wrap of Un-structured Data

Proposal to OASIS KMIP TC

Stan Feather and Indra Fitzgerald
Hewlett-Packard Co.

26 October, 2010

Key Wrap for un-structured data

Reason for proposed change

- Current key wrap specification may require all wrapped keys to be TTLV-encoded

- TTLV encoding could be a problem in the following example use case:
  - A KMIP proxy client requests a wrapped key on behalf of another device
  - The proxy is KMIP aware, but can't unwrap the key
  - The device using the key is not KMIP-aware
  - End-device unwraps the key, but doesn't understand the TTLV data

- KMIP 1.0 spec (section 2.1.4) requires the Key Value Byte String to be TTLV-encoded
  - Even if the string only includes Key Material
  - Example of Key Value Byte String, containing Key Material and encoding, before wrapping

```
420045  01  00000018 420043  08 00000010 0123456789ABCDEF0123456789ABCDEF
  Key                    Key    Byte
 Value   Struct   Len    Mat'l  String   Len    Key material
```

Proposal Description

Proposal description, for KMIP 1.1 spec

- Provide a method (an Encoding Option) to choose between un-encoded or encoded wrapping of un-structured keys
  - Un-structured is defined as Key Values with unstructured Key Material, and no attributes.
  - If Key Value data is structured (i.e., includes attributes), then server will always encode. TTLV-encoding is the only encoding option currently specified.
  - Default behavior is to encode, even if Key Value is un-structured (1.0 behavior)
  - Example of an unstructured Key Value, with no encoding, before wrapping into a Key Value Byte String:

```
0123456789ABCDEF0123456789ABCDEF
Key material
```

- Related request
  - Include a key wrapping use case in the KMIP 1.1 Use Case document
  - Include an Encoding Option example in the KMIP 1.1 Usage Guide

Proposal Detail

Proposed specification changes
reference: KMIP spec CD 12 (PDF), on 28 May,2010

2.1.4 Key value. Change line 248 to say

The *Key Value* is only used inside a Key Block. For plaintext keys, Key Value SHALL be a Key Value structure (see Table 6). For wrapped keys, Key Value is a Byte String containing, at minimum, the wrapped key material. This Byte String MAY also contain a wrapped Key Value structure.

2.1.4 Key value. Change line 254 to say

The Key Value Byte String is the wrapped contents of a Key Value structure. If the Key Value structure consists only of a Key Material byte string, the client MAY choose to request the Key Value Byte String to be un-encoded. Otherwise, the Key Value Byte String SHALL be a wrapped, TTLV encoded (see Section 9.1) Key Value structure.

Proposal Detail

Proposed specification changes
reference: KMIP spec CD 12 (PDF), on 28 May,2010

2.1.5 Key Wrapping Data. Insertion, following line 267, to say

• An *Encoding Option*, specifying whether the wrapped Key Value Byte String contains encoding. Only a Key Value containing no attributes MAY be un-encoded.

2.1.5 Key Wrapping Data. append a row to Table 7

Encoding Option	Enumeration, see 9.1.3.2.31	No. Specifies whether the Key Value Byte String was encoded. If not present, the wrapped Key Value SHALL be TTLV encoded. Only a wrapped Key Value with no attributes MAY be un-encoded.

Proposal Detail

Proposed specification changes

reference: KMIP 1.0 spec CD 12 (PDF), on 28 May,2010

2.1.6 Key Wrapping Specification. insertion, following line 305, to say

• An Encoding Option, specifying whether the Key Value will be encoded before wrapping. Only a Key Value structure with no attributes may be un-encoded.

2.1.6 Key Wrapping Specification. append a row to Table 10

Encoding Option	Enumeration, see 9.1.3.2.31	No. If Encoding Option is not present, the wrapped Key Value SHALL be TTLV encoded. If 1 or more attribute names are included the server SHALL return an error.

Proposal Detail

Proposed specification changes (continued)
reference: KMIP 1.0 spec CD 12 (PDF), on 28 May,2010

9.1.3.1 Tags. Table 193. Add row
- Encoding Option; 4200A2
- (Reserved); 4200A3 – 42FFFF

9.1.3.2.31 (new). Key Wrap Encoding Option Enumeration
- no encoding; 00001.
- TTLV encoding; 00002
- Extensions; 8XXXXXXX

Appendix B. Table 253. Add row
- Encoding Option 2.1.5, 2.1.6, 9.1.3.2.31 Enumeration

Proposal Detail

Proposed specification changes (continued)
reference: KMIP 1.0 spec CD 12 (PDF), on 28 May,2010

9.1.3.2.28 Result Reason Enumeration. Table 221. Add new value:
"Encoding Option Error"; Value 00000012

11.4. Register Errors. Table 229. Add (1) new Error Definition:
"Encoding Option not permitted when Key Wrapping Specification contains attribute names"; Operation Failed; Encoding Option Error

11.11. Get Errors. Table 236. Add (2) new Error Definitions:
"Object exists but cannot be provided in the desired Encoding Option"; Operation Failed; Encoding Option Error

"Encoding Option not permitted when Key Wrapping Specification contains attribute names"; Operation Failed; Encoding Option Error

Proposed Usage Guide Changes

Insert new paragraph, 3.21.6, following line 792
reference: KMIP Usage Guide 1.0 CD 10 (PDF), on 26 May,2010

3.21.6 Encoding Option for Wrapped Keys
KMIP provides the option to specify the Encoding Option inside the Key Wrapping Specification and Key Wrapping Data. This option allows users to Get or Register the Key Value in a non-TTLV encoded format. This may be desirable in a proxy environment, where the end-client is not KMIP-aware.

The Encoding Option is only available if no attributes are specified inside the Key Value. The server is required to return the Encoding Option Error if both the Encoding Option and Attribute Names are specified inside the Key Wrapping Specification. Similarly, the server is expected to return the Encoding Option Error when registering a wrapped object with attributes inside the Key Value and the Encoding Option is set in the Key Wrapping Data. If no Encoding Option is specified, KMIP assumes that the Key Value is TTLV-encoded. Thus, by default, the complete TTLV-encoded Key Value content, as shown in the example below, is wrapped:

```
Key Material          || Byte String   || Length   || Key Material Value
420043                || 08            || 00000010 || 0123456789ABCDEF0123456789ABCDEF
```

Proposed Usage Guide Changes (cont.)

Insert new paragraph, 3.21.6, following line 792
reference: KMIP Usage Guide 1.0 CD 10 (PDF), on 26 May,2010

Some end-clients may not understand or have the space for anything more than the actual key material (i.e., 0123456789ABCDEF0123456789ABCDEF in the above example). To wrap only the Key Material value during a Get operation, the Encoding Option (00001 for no encoding) should be specified inside the Key Wrapping Specification. The same Encoding Option should be specified in the Key Wrapping Data when returning the non-TTLV encoded wrapped object inside the Get Response or when registering a wrapped object in non-TTLV encoded format.

It is important to be aware of the risks involved when excluding the attributes from the Key Value. Binding the attributes to the key material in certain environments is essential to the security of the end-client. An untrusted proxy could change the attributes (provided separately via the Get Attributes operation) that determine how the key is being used (e.g. Cryptographic Usage). Including the attributes inside the Key Value and cryptographically binding it to the Key Material could prevent potential misuse of the cryptographic object and may prevent a replay attack if, for example, a nonce is included as a custom attribute. The exclusion of attributes and therefore the usage of the Encoding Option are only recommended in at least one of the following scenarios:

Proposed Usage Guide Changes (cont.)

Insert new paragraph, 3.21.6, following line 792
reference: KMIP Usage Guide 1.0 CD 10 (PDF), on 26 May,2010

1. End-clients are registered with the KMIP server and are communicating with the server directly (i.e., the TLS connection is between the server and client).

2. The environment is controlled and non-KMIP-aware end-clients are aware how wrapped cryptographic objects (possibly Raw keys) from the KMIP server should be used without having to rely on the attributes provided by the Get Attributes operation.

3. The wrapped cryptographic object consists of attributes inside the Key Material value. These attributes cannot be interpreted by the KMIP server, but are understood by the end-client. This may be the case if the Key Format Type is opaque or vendor-specific.

4. The proxy communicating with the KMIP server on behalf of the end-client is considered to be trusted and is operating in a secure environment.

Registering a wrapped object without attributes is not recommended in a proxy environment, unless scenario 4 is met