Raw XML Messaging
A Proposal to P1619.3

THE KEY TO ENCRYPTION IS HOW YOU MANAGE IT™

Bob Lockhart
Senior Solutions Architect
October 2008

Raw XML Messaging

- Keeps messaging to a minimum for lightweight clients
  - No overhead from SOAP
- Extensible for heavyweight client
- Security provided by encrypted transport
- Message Authentication can be made optional on a per KM Client basis
- Converts easily to binary formatted messages
- Still uses of XML Schema Definition files

Minimum Generate Key Request

Full message shown to right

Required Fields:

- XML Version
- Protocol Version
- Message Timestamp
- Session ID
- Key Type

Easily mapped to binary

- Small TLV package
- Low overhead clients
  - Hardware Clients

```
<?xml version="1.0" encoding="UTF-8"?>
<kms_request>
 <protocol_version>1.0</protocol_version>
 <timestamp>1903-07-01T00:00:00Z</timestamp>
 <kms_request_parameters>
   <kms_generatekey_request>
     <session_id>32 byte HEX String</session_id>
     <key_request>
       <key_type>XTS-AES-256</key_type>
     </key_request>
   </kms_generatekey_request>
 </kms_request_parameters>
</kms_request>
```

Minimum Generate Key Reply

Full message shown to right

Required Items:

- XML Version
- Protocol Version
- Message Timestamp
- Session ID
- Identifiers
  - SO_Family
  - SO_Domain
  - SO_Context
  - SO_Handle
  - SO_Record_ID
- Creation Timestamp
- Key Blob

```
<?xml version="1.0" encoding="UTF-8" ?>
<kms_reply xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:noNamespaceSchemaLocation="kms_reply_def.xsd">
 <protocol_version>1.0</protocol_version>
 <timestamp>1903-07-01T00:00:00Z</timestamp>
 <kms_reply_parameters>
  <kms_generatekey_reply>
   <session_id>32 byte HEX String</session_id>
   <key_reply>
    <identifiers>
     <so_object_id>
      <so_family>km</so_family>
      <so_domain>example.com</so_domain>
      <so_context>
       <so_object_space>key</so_object_space>
       <so_path>/some/directory/</so_path>
      </so_context>
      <so_handle>736f6d652068616e646c65</so_handle>
      <so_record_id>164F1C617DBDB87C6F67FC3E</so_record_id>
     </so_object_id>
    </identifiers>
    <timestamps>
     <key_created_time_stamp>1903-07-01T00:05:00Z</key_created_time_stamp>
    </timestamps>
    <key_value>
     <raw_data>Base 64 Encoded Key Data</raw_data>
    </key_value>
   </key_reply>
  </kms_generatekey_reply>
 </kms_reply_parameters>
</kms_reply>
```

Extended Generate Key Request

Full message shown to right

Concepts:

- Do Not Return
  - Should be first
- Return
- Client assigned GUID
  - SO_Family
  - SO_Domain
  - SO_Context
  - SO_Handle
- Key Use
  - Disk
  - LTO4
  - etc…

```
<?xml version="1.0" encoding="UTF-8"?>
<kms_request>
 <protocol_version>1.0</protocol_version>
 <timestamp>2008-10-06T12:34:56Z</timestamp>
 <kms_request_parameters>
  <kms_generatekey_request>
   <session_id>32 byte HEX String</session_id>
   <do_not_return>
    <attribute_name>so_record_id</attribute_name>
    <attribute_name>key_value</attribute_name>
    <attribute_name>timestamps</attribute_name>
   </do_not_return>
   <return>
    <attribute_name>key_state</attribute_name>
   </return>
   <key_request>
    <so_object_id>
     <so_family>km</so_family>
     <so_domain>bigbank.com</so_domain>
     <so_context>
       <so_object_space>key</so_object_space>
       <so_path>/some/directory/</so_path>
     </so_context>
     <subdirectory>vt1/</subdirectory>
     <so_handle>ab6f6d442b68613e948c6a</so_handle>
    </so_object_id>
    <key_use>tape</key_use>
    <key_type>CBC-AES-256-HMAC-SHA1</key_type>
   </key_request>
  </kms_generatekey_request>
 </kms_request_parameters>
</kms_request>
```

Extended Generate Key Reply

Full message shown to right

Extended Return:

- Original Identifier
  - SO_Family
  - SO_Domain
  - SO_Context
  - SO_Handle
  - SO_Record_ID
- No Key Timestamps
- Disable Timestamp
- No Key Blob
- Additional Attributes
  - Key Use
  - Key State

```
<?xml version="1.0" encoding="UTF-8"?>
<kms_reply>
 <protocol_version>1.0</protocol_version>
 <timestamp>2008-10-06T12:35:00Z</timestamp>
 <kms_reply_parameters>
  <kms_generatekey_reply>
   <session_id>32 byte Hex String</session_id>
   <key_reply>
    <identifiers>
     <so_object_id>
      <so_family>km</so_family>
      <so_domain>bigbank.com</so_domain>
      <so_context>
       <so_object_space>key</so_object_space>
       <so_path>/some/directory/</so_path>
      </so_context>
      <subdirectory>vt1/</subdirectory>
      <so_handle>ab6f6d442b68613e948c6a</so_handle>
     </so_object_id>
    </identifiers>
    <timestamps>
     <disable_timestamp>2010-10-06T12:34:55Z</disable_timestamp>
    </timestamps>
    <attributes>
     <key_use>tape</key_use>
     <key_state>preactivation</key_state>
    </attributes>
   </key_reply>
  </kms_generatekey_reply>
 </kms_reply_parameters>
</kms_reply>
```

Minimum Generate Key Reply

Full XSD shown to right

Need for Base XSD

- Provides common items between messages that use same attributes
  - Generate Key
  - Store Key
  - Retrieve Key
    - (Get Key)
- Needed for:
  - Key functions
  - Policy functions
  - Events & Alerts
  - Others???

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">
 <xs:annotation>
  <xs:documentation>definition of complex type elements</xs:documentation>
 </xs:annotation>
 <xs:complexType name="kms_generatekey_request_type">
  <xs:complexContent>
   <xs:extension base="kms_key_request_base">
    <xs:sequence>
     <xs:element name="key_request">
      <xs:complexType>
       <xs:complexContent>
        <xs:extension base="kms_key_request_with_attributes">
         <xs:sequence>
          <xs:element name="key_type">
           <xs:simpleType>
            <xs:restriction base="xs:string">
             <xs:enumeration value="see attached XSD file for list" />
            </xs:restriction>
           </xs:simpleType>
          </xs:element>
         </xs:sequence>
        </xs:extension>
       </xs:complexContent>
      </xs:complexType>
     </xs:element>
    </xs:sequence>
   </xs:extension>
  </xs:complexContent>
 </xs:complexType>
</xs:schema>
```