Relatório de Teste $Kryptus\ kNET$

Lab
SEC - Universidade Federal de Santa Catatina2018-01-29

0.1 Execução

```
--- report/expected.tex 2018-01-29 17:58:33.000000000 -0200
+++ report/results.tex 2018-01-29 17:58:33.000000000 -0200
@@ -1,824 +1,823 @@
<RequestMessage>
   <RequestHeader>
     <ProtocolVersion>
       <ProtocolVersionMajor type="Integer" value="1"/>
       <ProtocolVersionMinor type="Integer" value="3"/>
     </ProtocolVersion>
     <BatchCount type="Integer" value="1"/>
   </RequestHeader>
   <BatchItem>
     <Operation type="Enumeration" value="CreateKeyPair"/>
     <RequestPayload>
       <CommonTemplateAttribute>
         <Attribute>
           <AttributeName type="TextString" value="Cryptographic Algorithm"/>
           <AttributeValue type="Enumeration" value="RSA"/>
         </Attribute>
         <Attribute>
           <AttributeName type="TextString" value="Cryptographic Length"/>
           <AttributeValue type="Integer" value="2048"/>
         </Attribute>
         <Attribute>
           <AttributeName type="TextString" value="Activation Date"/>
           <AttributeValue type="DateTime" value="NOW-3600"/>
           <AttributeValue type="DateTime" value="2018-01-29T18:58:22.031848"/>
         </Attribute>
       </CommonTemplateAttribute>
       <PrivateKeyTemplateAttribute>
         <Attribute>
           <AttributeName type="TextString" value="Cryptographic Usage Mask"/>
           <AttributeValue type="Integer" value="UnwrapKey"/>
         </Attribute>
       </PrivateKeyTemplateAttribute>
       <PublicKeyTemplateAttribute>
         <Attribute>
           <AttributeName type="TextString" value="Cryptographic Usage Mask"/>
           <AttributeValue type="Integer" value="WrapKey"/>
         </Attribute>
       </PublicKeyTemplateAttribute>
     </RequestPayload>
   </BatchItem>
 </RequestMessage>
 <ResponseMessage>
   <ResponseHeader>
     <ProtocolVersion>
       <ProtocolVersionMajor type="Integer" value="1"/>
       <ProtocolVersionMinor type="Integer" value="3"/>
     </ProtocolVersion>
     <TimeStamp type="DateTime" value="NOW"/>
     <TimeStamp type="DateTime" value="2018-01-29T19:59:19+00:00"/>
     <BatchCount type="Integer" value="1"/>
   </ResponseHeader>
     <Operation type="Enumeration" value="CreateKeyPair"/>
     <ResultStatus type="Enumeration" value="Success"/>
     <ResponsePayload>
      <PrivateKeyUniqueIdentifier type="TextString" value="IMPORTER_PRIV_UID"/>
       <PublicKeyUniqueIdentifier type="TextString" value="IMPORTER_PUB_UID"/>
       <PrivateKeyUniqueIdentifier type="TextString" value="0M3ey+80IWYEqhrKt1sF"/>
       <PublicKeyUniqueIdentifier type="TextString" value="9ihkDcG6/K3J2vkgbqlA"/>
```

</ResponsePayload>
</BatchItem>
</ResponseMessage>

```
<RequestMessage>
  <RequestHeader>
    <ProtocolVersion>
      <ProtocolVersionMajor type="Integer" value="1"/>
      <ProtocolVersionMinor type="Integer" value="3"/>
    </ProtocolVersion>
    <BatchCount type="Integer" value="1"/>
  </RequestHeader>
  <BatchItem>
     <Operation type="Enumeration" value="Get"/>
    <RequestPayload>
      <UniqueIdentifier type="TextString" value="IMPORTER_PUB_UID"/>
      <UniqueIdentifier type="TextString" value="9ihkDcG6/K3J2vkgbqlA"/>
      <KeyFormatType type="Enumeration" value="TransparentRSAPublicKey"/>
    </RequestPayload>
  </BatchItem>
 </RequestMessage>
 <ResponseMessage>
   <ResponseHeader>
    <ProtocolVersion>
      <ProtocolVersionMajor type="Integer" value="1"/>
      <ProtocolVersionMinor type="Integer" value="3"/>
    </ProtocolVersion>
    <TimeStamp type="DateTime" value="NOW"/>
    <TimeStamp type="DateTime" value="2018-01-29T19:59:19+00:00"/>
    <BatchCount type="Integer" value="1"/>
  </ResponseHeader>
  <BatchItem>
    <Operation type="Enumeration" value="Get"/>
    <ResultStatus type="Enumeration" value="Success"/>
    <ResponsePayload>
      <ObjectType type="Enumeration" value="PublicKey"/>
      <UniqueIdentifier type="TextString" value="IMPORTER_PUB_UID"/>
      <UniqueIdentifier type="TextString" value="9ihkDcG6/K3J2vkgbqlA"/>
      <PublicKey>
        <KeyBlock>
          <KeyFormatType type="Enumeration" value="TransparentRSAPublicKey"/>
          <KeyValue>
            <KeyMaterial>
              <Modulus type="BigInteger" value="IMPORTER_PUB_MODULUS"/>
              <PublicExponent type="BigInteger" value="IMPORTER_PUB_EXPONENT"/>
              <Modulus type="BigInteger" value="000000000000000008117a5fe5b7be3fb5</pre>
f6aae1b7c124c8349c6b3f1260989355dfad75ba49192af340d6f02839294b35f8c9f19ce1512958b40b0ef036c865fac6f2
{\tt c140ffdb5b65f89f6d72bf350f6a77e9ffc11c2e04c5ddea67c687893bf0319b25c2e63ba5609c81e54b8703825bcccc6b6d}
6917218154bbfd1559fdf6b6d88f385ea8e50fa6d1d201c67e9e388b575d18612ace3ab4a3fcff2049b056b48b5673"/>
              <PublicExponent type="BigInteger" value="000000000010001"/>
            </KeyMaterial>
          </KeyValue>
          <CryptographicAlgorithm type="Enumeration" value="RSA"/>
          <CryptographicLength type="Integer" value="2048"/>
        </KeyBlock>
      </PublicKey>
     </ResponsePayload>
   </BatchItem>
 </ResponseMessage>
```

```
<RequestMessage>
 <RequestHeader>
   <ProtocolVersion>
      <ProtocolVersionMajor type="Integer" value="1"/>
      <ProtocolVersionMinor type="Integer" value="3"/>
   </ProtocolVersion>
    <BatchCount type="Integer" value="1"/>
 </RequestHeader>
 <BatchItem>
    <Operation type="Enumeration" value="CreateKeyPair"/>
    <RequestPayload>
      <CommonTemplateAttribute>
        <Attribute>
          <AttributeName type="TextString" value="Cryptographic Algorithm"/>
          <AttributeValue type="Enumeration" value="RSA"/>
        </Attribute>
        <Attribute>
          <AttributeName type="TextString" value="Cryptographic Length"/>
          <AttributeValue type="Integer" value="2048"/>
        </Attribute>
      </CommonTemplateAttribute>
      <PrivateKeyTemplateAttribute>
          <AttributeName type="TextString" value="Cryptographic Usage Mask"/>
          <AttributeValue type="Integer" value="Sign"/>
        </Attribute>
      </PrivateKeyTemplateAttribute>
      <PublicKeyTemplateAttribute>
        <Attribute>
          <AttributeName type="TextString" value="Cryptographic Usage Mask"/>
          <AttributeValue type="Integer" value="Verify"/>
        </Attribute>
      </PublicKeyTemplateAttribute>
    </RequestPayload>
 </BatchItem>
</RequestMessage>
<ResponseMessage>
  <ResponseHeader>
    <ProtocolVersion>
      <ProtocolVersionMajor type="Integer" value="1"/>
      <ProtocolVersionMinor type="Integer" value="3"/>
   </ProtocolVersion>
   <TimeStamp type="DateTime" value="NOW"/>
   <TimeStamp type="DateTime" value="2018-01-29T19:59:25+00:00"/>
   <BatchCount type="Integer" value="1"/>
 </ResponseHeader>
 <BatchItem>
    <Operation type="Enumeration" value="CreateKeyPair"/>
    <ResultStatus type="Enumeration" value="Success"/>
    <ResponsePayload>
      <PrivateKeyUniqueIdentifier type="TextString" value="EXPORTER_TBE_PRIV_UID"/>
      <PublicKeyUniqueIdentifier type="TextString" value="EXPORTER_TBE_PUB_UID"/>
      <PrivateKeyUniqueIdentifier type="TextString" value="q8vGENBf8p1kgbEYKHu1"/>
      <PublicKeyUniqueIdentifier type="TextString" value="ZRGyFcCtfpCEwAwrBODz"/>
   </ResponsePayload>
 </BatchItem>
</ResponseMessage>
```

```
<RequestMessage>
  <RequestHeader>
    <ProtocolVersion>
      <ProtocolVersionMajor type="Integer" value="1"/>
      <ProtocolVersionMinor type="Integer" value="3"/>
    </ProtocolVersion>
    <BatchCount type="Integer" value="1"/>
  </RequestHeader>
  <BatchItem>
    <Operation type="Enumeration" value="Register"/>
    <RequestPayload>
      <ObjectType type="Enumeration" value="PublicKey"/>
      <TemplateAttribute>
        <Attribute>
          <AttributeName type="TextString" value="Cryptographic Usage Mask"/>
          <AttributeValue type="Integer" value="WrapKey"/>
        </Attribute>
        <Attribute>
         <AttributeName type="TextString" value="Cryptographic Parameters"/>
         <AttributeValue>
           <PaddingMethod type="Enumeration" value="OAEP"/>
           <HashingAlgorithm type="Enumeration" value="SHA_256"/>
           <CryptographicAlgorithm type="Enumeration" value="RSA"/>
          </AttributeValue>
        </Attribute>
        <Attribute>
          <AttributeName type="TextString" value="Activation Date"/>
          <AttributeValue type="DateTime" value="NOW-3600"/>
          <AttributeValue type="DateTime" value="2018-01-29T18:58:31.596416"/>
        </Attribute>
      </TemplateAttribute>
      <PublicKey>
        <KeyBlock>
          <KeyFormatType type="Enumeration" value="TransparentRSAPublicKey"/>
          <KeyValue>
           <KeyMaterial>
             <Modulus type="BigInteger" value="IMPORTER_PUB_MODULUS"/>
             <PublicExponent type="BigInteger" value="IMPORTER_PUB_EXPONENT"/>
             <Modulus type="BigInteger" value="00000000000000008117a5fe5b7be3fb5</pre>
f6aae1b7c124c8349c6b3f1260989355dfad75ba49192af340d6f02839294b35f8c9f19ce1512958b40b0ef036c865fac6f2
6917218154bbfd1559fdf6b6d88f385ea8e50fa6d1d201c67e9e388b575d18612ace3ab4a3fcff2049b056b48b5673"/>
             <PublicExponent type="BigInteger" value="000000000010001"/>
           </KeyMaterial>
         </KeyValue>
          <CryptographicAlgorithm type="Enumeration" value="RSA"/>
          <CryptographicLength type="Integer" value="2048"/>
        </KeyBlock>
      </PublicKey>
    </RequestPayload>
  </BatchItem>
 </RequestMessage>
 <ResponseMessage>
  <ResponseHeader>
    <ProtocolVersion>
      <ProtocolVersionMajor type="Integer" value="1"/>
      <ProtocolVersionMinor type="Integer" value="3"/>
    </ProtocolVersion>
    <TimeStamp type="DateTime" value="NOW"/>
    <TimeStamp type="DateTime" value="2018-01-29T19:59:26+00:00"/>
    <BatchCount type="Integer" value="1"/>
  </ResponseHeader>
  <BatchItem>
```

```
<RequestMessage>
 <RequestHeader>
   <ProtocolVersion>
      <ProtocolVersionMajor type="Integer" value="1"/>
      <ProtocolVersionMinor type="Integer" value="3"/>
   </ProtocolVersion>
    <BatchCount type="Integer" value="1"/>
 </RequestHeader>
 <BatchItem>
    <Operation type="Enumeration" value="Create"/>
    <RequestPayload>
      <ObjectType type="Enumeration" value="SymmetricKey"/>
      <TemplateAttribute>
        <Attribute>
          <AttributeName type="TextString" value="Cryptographic Algorithm"/>
          <AttributeValue type="Enumeration" value="AES"/>
        </Attribute>
        <Attribute>
          <AttributeName type="TextString" value="Cryptographic Length"/>
          <AttributeValue type="Integer" value="256"/>
        </Attribute>
        <Attribute>
          <AttributeName type="TextString" value="Cryptographic Usage Mask"/>
          <AttributeValue type="Integer" value="WrapKey"/>
        </Attribute>
        <Attribute>
          <AttributeName type="TextString" value="Cryptographic Parameters"/>
          <AttributeValue>
            <BlockCipherMode type="Enumeration" value="CTR"/>
            <RandomIV type="Boolean" value="true"/>
          </AttributeValue>
        </Attribute>
        <Attribute>
          <AttributeName type="TextString" value="Activation Date"/>
          <AttributeValue type="DateTime" value="NOW-3600"/>
          <AttributeValue type="DateTime" value="2018-01-29T18:58:31.800303"/>
        </Attribute>
      </TemplateAttribute>
   </RequestPayload>
 </BatchItem>
</RequestMessage>
<ResponseMessage>
  <ResponseHeader>
    <ProtocolVersion>
      <ProtocolVersionMajor type="Integer" value="1"/>
      <ProtocolVersionMinor type="Integer" value="3"/>
   </ProtocolVersion>
   <TimeStamp type="DateTime" value="NOW"/>
   <TimeStamp type="DateTime" value="2018-01-29T19:59:26+00:00"/>
    <BatchCount type="Integer" value="1"/>
 </ResponseHeader>
 <BatchItem>
    <Operation type="Enumeration" value="Create"/>
    <ResultStatus type="Enumeration" value="Success"/>
    <ResponsePayload>
      <ObjectType type="Enumeration" value="SymmetricKey"/>
      <UniqueIdentifier type="TextString" value="EXPORTER_TEMP_SYMM_KEK_UID"/>
      <UniqueIdentifier type="TextString" value="Q/VMGR8DnP4TfsyU00QJ"/>
   </ResponsePayload>
 </BatchItem>
</ResponseMessage>
```

```
<RequestMessage>
             <RequestHeader>
                     <ProtocolVersion>
                              <ProtocolVersionMajor type="Integer" value="1"/>
                              <ProtocolVersionMinor type="Integer" value="3"/>
                     </ProtocolVersion>
                     <BatchCount type="Integer" value="1"/>
             </RequestHeader>
             <BatchItem>
                      <Operation type="Enumeration" value="Get"/>
                      <RequestPayload>
                              <UniqueIdentifier type="TextString" value="EXPORTER_TBE_PRIV_UID"/>
                              <UniqueIdentifier type="TextString" value="q8vGENBf8p1kgbEYKHu1"/>
                              <KeyFormatType type="Enumeration" value="TransparentRSAPrivateKey"/>
                              <KeyWrappingSpecification>
                                      <WrappingMethod type="Enumeration" value="Encrypt"/>
                                      <EncryptionKeyInformation>
                                              <UniqueIdentifier type="TextString" value="EXPORTER_TEMP_SYMM_KEK_UID"/>
                                              <UniqueIdentifier type="TextString" value="Q/VMGR8DnP4TfsyU00QJ"/>
                                      </EncryptionKeyInformation>
                                      <EncodingOption type="Enumeration" value="TTLVEncoding"/>
                              </KeyWrappingSpecification>
                     </RequestPayload>
             </BatchItem>
     </RequestMessage>
     <ResponseMessage>
             <ResponseHeader>
                     <ProtocolVersion>
                             <ProtocolVersionMajor type="Integer" value="1"/>
                              <ProtocolVersionMinor type="Integer" value="3"/>
                     </ProtocolVersion>
                     <TimeStamp type="DateTime" value="NOW"/>
                     <TimeStamp type="DateTime" value="2018-01-29T19:59:26+00:00"/>
                     <BatchCount type="Integer" value="1"/>
             </ResponseHeader>
             <BatchItem>
                      <Operation type="Enumeration" value="Get"/>
                      <ResultStatus type="Enumeration" value="Success"/>
                      <ResponsePayload>
                              <ObjectType type="Enumeration" value="PrivateKey"/>
                              <UniqueIdentifier type="TextString" value="EXPORTER_TBE_PRIV_UID"/>
                              <UniqueIdentifier type="TextString" value="q8vGENBf8p1kgbEYKHu1"/>
                              <PrivateKey>
                                       <KeyBlock>
                                              <KeyFormatType type="Enumeration" value="TransparentRSAPrivateKey"/>
                                              <KeyValue type="ByteString" value="EXPORTER_PRIV_KEY_VALUE"/>
                                              <KeyValue type="ByteString" value="153a70bd7fc40871530d98227d5d2b2cb7cfb</pre>
94a9cd830c464206743be8ad18e75189d9872eeefda83dc96b125ed6aab82e23e97695812fe3487a6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd181fdfaa6fad6d8f9b9cd8fa6fad6d8f9b9cd8fafafad6d8f9b9cd8fafafafad6d8f9b9cd8fafafad6
149c9fb37a21975481c0a3f719363bed5d72c5574e4de34c8ed698a378f6a89cd6e1c8ec69c1866c9cf22552ad3f754547dc
6 dc 237 2 bf 0 325 006462 bb 2843 e6898077621 d04 ba 732778453 d624718433 ae 62 c828 cc7 c74 cb 919448 eadeb fac 0 f5a87425 above 100 fb 10
32 d cafe 63615 b 93031 d f d 2 d c b f 78 f 695 c 03 b 22176 a 9 d 0 c f 603 a f 81303 b 8f 1 a c 10492 f 572479 e 6 d d a a 280 d e c c 715942 84 b 19 f 603 a f 81303 b 8f 1 a c 10492 f 572479 e 6 d d a a 280 d e c c 715942 84 b 19 f 603 a f 81303 b 8f 1 a c 10492 f 572479 e 6 d d a a 280 d e c c 715942 84 b 19 f 603 a f 81303 b 8f 1 a c 10492 f 572479 e 6 d d a a 280 d e c c 715942 84 b 19 f 603 a f 81303 b 8f 1 a c 10492 f 572479 e 6 d d a a 280 d e c c 715942 84 b 19 f 603 a f 603 a
0 + c_{1} + c_{2} + c_{1} + c_{2} + c_{1} + c_{2} + c_{1} + c_{2} + 
12 ef 66 b 7 ec 8 de 22703 f 61 e 553 d 138 b 6 b d 38 d 2275 f 9 f d cc d 68 d 112 d d b b e 5 e b 7 b 08 4 2987 6 4 2 f 1792 d b 5 c 978 a ce 266 f d 9301 b 72 d b 5 c 978 a ce 266 f d 9301 b 72 d b 5 c 978 a ce 266 f d 9301 b 72 d b 5 c 978 a ce 266 f d 9301 b 72 d b 5 c 978 a ce 266 f d 9301 b 72 d b 5 c 978 a ce 266 f d 9301 b 72 d b 5 c 978 a ce 266 f d 9301 b 72 d b 5 c 978 a ce 266 f d 9301 b 72 d b 5 c 978 a ce 266 f d 9301 b 72 d b 5 c 978 a ce 266 f d 9301 b 72 d b 5 c 978 a ce 266 f d 9301 b 72 d b 5 c 978 a ce 266 f d 9301 b 72 d b 5 c 978 a ce 266 f d 9301 b 72 d b 5 c 978 a ce 266 f d 9301 b 72 d b 5 c 978 a ce 266 f d 9301 b 72 d b 5 c 978 a ce 266 f d 9301 b 72 d b 5 c 978 a ce 266 f d 9301 b 72 d b 5 c 978 a ce 266 f d 9301 b 72 d b 5 c 978 a ce 266 f d 9301 b 72 d b 5 c 978 a ce 266 f d 9301 b 72 d b 5 c 978 a ce 266 f d 9301 b 72 d b 5 c 978 a ce 266 f d 9301 b 72 d b 5 c 978 a ce 266 f d 9301 b 72 d b 5 c 978 a ce 266 f d 9301 b 72 d b 72
267073735fa8df2883f81094b6936600d852516bf2bb41462bfe79938205ff1b08b712df2083c32ceecf2a76097bfbc227ff
b84b4fd2b0c709135748823a1ef2f11929e187e2828dde282aa2ad2d14495947b8a27bdf11cbeeac77999ca9a0e1af1d2dcc
4 c ca 9 d 0 8 b c 0 f 1 e 24 f 7 8 6 6 2 e 6 8 e e 8 7 f 4 3 c 9 6 8 0 7 f d 0 e 10 1 c 1 b 1 d a d 4 e a 4 a 19 4 19 7 4 2 e b 1 f 2 3 f a 2 b 1 6 1 5 1 5 c 1 3 6 8 c 0 6 c 5 5 2 3 8 3 6 7 0 8 e a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5 a 6 d 5
```

 $35439c142e5e592392a56fcac843f04e404dcf56aa09147c60fd9af621edc9457bb76805ae4eca1aade7d1efc37794415912\\ 4c997709bb47371217d09f0759c04599f67d67ab86da8ff45dc682bddf4515c529b8c8fa03b1329a788357fe1a889b68f4d1\\ 69136f34ee13d42e807d522ae6794996d088ac4f91dbf26d45dd3dfcd6ed4256f4c1181369d4240a6cacdcf1530c672c50eb\\ e869d7269a6b05252acb9be7091a771e18c8211badfe930fca3da0ff67bef9f213de050ba868be95a565cf553b0fdbbee69e\\ 54e0144a84227bea4954702f03f66bb5d5caa905f8177c5da1ac3c194b36e68e651394dc03c81c92637dc15dc6971b79392c\\ acb44e7a343ff56a77250b6cdc35c7e920fdce17ea399b6955f918c4671abe9b669e624e8c1c2f5085eed43e907312ad8da6\\ c0057931f2bc768b5571dcbe38fb40f7dc4f75d85b0cce5fb0cec3acd3364b70be00c68ba74776deec8a262e6da275ddadb8\\ 9fac3311c4788809f82da9a6931387543eb576f8c1338772b2bc5b35600f50887fdb4af15928630e9d866e46d883965367d0\\ 12251e81e2beb3aeea6eb0097fe3adb2e803f2f"/>$

```
<CryptographicAlgorithm type="Enumeration" value="RSA"/>
           <CryptographicLength type="Integer" value="2048"/>
           <KeyWrappingData>
             <WrappingMethod type="Enumeration" value="Encrypt"/>
             <EncryptionKeyInformation>
               <UniqueIdentifier type="TextString" value="EXPORTER_TEMP_SYMM_KEK_UID</pre>
               <UniqueIdentifier type="TextString" value="Q/VMGR8DnP4TfsyU00QJ"/>
               <CryptographicParameters>
                 <BlockCipherMode type="Enumeration" value="CTR"/>
                 <PaddingMethod type="Enumeration" value="None"/>
                 <RandomIV type="Boolean" value="true"/>
               </CryptographicParameters>
             </EncryptionKeyInformation>
             <IVCounterNonce type="ByteString" value="EXPORTER_WRAP_01_IV"/>
             <IVCounterNonce type="ByteString" value="092497b4e2f113b0790e76cc0ef8c</pre>
57f"/>
             <EncodingOption type="Enumeration" value="TTLVEncoding"/>
           </KeyWrappingData>
         </KeyBlock>
       </PrivateKey>
     </ResponsePayload>
   </BatchItem>
 </ResponseMessage>
```

```
<RequestMessage>
     <RequestHeader>
        <ProtocolVersion>
            <ProtocolVersionMajor type="Integer" value="1"/>
            <ProtocolVersionMinor type="Integer" value="3"/>
        </ProtocolVersion>
        <BatchCount type="Integer" value="1"/>
     </RequestHeader>
     <BatchItem>
        <Operation type="Enumeration" value="Get"/>
        <RequestPayload>
            <UniqueIdentifier type="TextString" value="EXPORTER_TEMP_SYMM_KEK_UID"/>
            <UniqueIdentifier type="TextString" value="Q/VMGR8DnP4TfsyU00QJ"/>
            <KeyFormatType type="Enumeration" value="Raw"/>
            <KeyWrappingSpecification>
               <WrappingMethod type="Enumeration" value="Encrypt"/>
               <EncryptionKeyInformation>
                  <UniqueIdentifier type="TextString" value="EXPORTER_CLIENT_KEK_UID"/>
                  <UniqueIdentifier type="TextString" value="YYzt6q4Y0Wdo2EGT6k/Z"/>
               </EncryptionKeyInformation>
               <EncodingOption type="Enumeration" value="NoEncoding"/>
            </KeyWrappingSpecification>
        </RequestPayload>
     </BatchItem>
  </RequestMessage>
  <ResponseMessage>
     <ResponseHeader>
        <ProtocolVersion>
           <ProtocolVersionMajor type="Integer" value="1"/>
           <ProtocolVersionMinor type="Integer" value="3"/>
        </ProtocolVersion>
        <TimeStamp type="DateTime" value="NOW"/>
        <TimeStamp type="DateTime" value="2018-01-29T19:59:26+00:00"/>
        <BatchCount type="Integer" value="1"/>
     </ResponseHeader>
     <BatchItem>
        <Operation type="Enumeration" value="Get"/>
        <ResultStatus type="Enumeration" value="Success"/>
        <ResponsePayload>
           <ObjectType type="Enumeration" value="SymmetricKey"/>
            <UniqueIdentifier type="TextString" value="TEMP_SYMM_KEK_UID"/>
            <UniqueIdentifier type="TextString" value="Q/VMGR8DnP4TfsyU00QJ"/>
            <SymmetricKey>
               <KeyBlock>
                  <KeyFormatType type="Enumeration" value="Raw"/>
                  <KeyValue type="ByteString" value="EXPORTER_TEMP_SYMM_KEK_KEY_VALUE"/>
                  <KeyValue type="ByteString" value="8f5184faaf805fc324e29be721467d903cc8d"</pre>
\verb|b5c93aee653c520afe790e74f8cff8192ee73753b31678913d1a41f491aea281fb1d3f1c960cbc023f4ab5ee30d94ccf4973||
1a8b53acc080812ff4ff8f290e43ed4e3ceef033a79f216d87bfed79198c9f59c61e574ff09c22f0bb49b3cba5978adff4f2126d87bfed79198c9f59c61e574ff09c22f0bb49b3cba5978adff4f2126d87bfed79198c9f59c61e574ff09c22f0bb49b3cba5978adff4f2126d87bfed79198c9f59c61e574ff09c22f0bb49b3cba5978adff4f2126d87bfed79198c9f59c61e574ff09c22f0bb49b3cba5978adff4f2126d87bfed79198c9f59c61e574ff09c22f0bb49b3cba5978adff4f2126d87bfed79198c9f59c61e574ff09c22f0bb49b3cba5978adff4f2126d87bfed79198c9f59c61e574ff09c22f0bb49b3cba5978adff4f2126d87bfed79198c9f59c61e574ff09c22f0bb49b3cba5978adff4f2126d87bfed79198c9f59c61e574ff09c22f0bb49b3cba5978adff4f2126d87bfed79198c9f59c61e574ff09c22f0bb49b3cba5978adff4f2126d87bfed79198c9f59c61e574ff09c22f0bb49b3cba5978adff4f2126d87bfed79198c9f59c61e574ff09c22f0bb49b3cba5978adff4f2126d87bfed79198c9f59c61e574ff09c22f0bb49b3cba5978adff4f2126d87bfed79198c9f59c61e574ff09c22ff0bb49b3cba5978adff4f2126d87bfed79198c9f59c61e574ff09c22ff0bb49b3cba5978adff4f216d87bfed79198c9f59c61e574ff09c22ff0bb49b3cba5978adff4f216d87bfed79198c9f69c61e574ff09c22ff0bb49b3cba5978adff4f216d87bfed79198c9f69c61e574ff09c22ff0bb49b3cba5978adff4f216d87bfed79198c9f69c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e5746ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e5746ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09c61e574ff09
aab5051971c3b7fc78dedf17e51aeee14f18d239a3f746c4e922c2c1ac4eeed44f7e9702033"/>
                  <CryptographicAlgorithm type="Enumeration" value="AES"/>
                  <CryptographicLength type="Integer" value="256"/>
                  <KeyWrappingData>
                     <WrappingMethod type="Enumeration" value="Encrypt"/>
                     <EncryptionKeyInformation>
                         <UniqueIdentifier type="TextString" value="EXPORTER_CLIENT_KEK_UID"/>
                         <UniqueIdentifier type="TextString" value="YYzt6q4Y0Wdo2EGT6k/Z"/>
                         <CryptographicParameters>
                            <PaddingMethod type="Enumeration" value="OAEP"/>
                            <HashingAlgorithm type="Enumeration" value="SHA_256"/>
                            <CryptographicAlgorithm type="Enumeration" value="RSA"/>
                         </CryptographicParameters>
```

```
<RequestMessage>
 <RequestHeader>
   <ProtocolVersion>
      <ProtocolVersionMajor type="Integer" value="1"/>
      <ProtocolVersionMinor type="Integer" value="3"/>
   </ProtocolVersion>
    <BatchCount type="Integer" value="2"/>
 </RequestHeader>
 <BatchItem>
    <Operation type="Enumeration" value="Revoke"/>
    <RequestPayload>
      <UniqueIdentifier type="TextString" value="EXPORTER_TEMP_SYMM_KEK_UID"/>
      <UniqueIdentifier type="TextString" value="Q/VMGR8DnP4TfsyU00QJ"/>
      <RevocationReason>
        <RevocationReasonCode type="Enumeration" value="CessationOfOperation"/>
      </RevocationReason>
   </RequestPayload>
 </BatchItem>
 <BatchItem>
    <Operation type="Enumeration" value="Destroy"/>
   <RequestPayload>
      <UniqueIdentifier type="TextString" value="EXPORTER_TEMP_SYMM_KEK_UID"/>
      <UniqueIdentifier type="TextString" value="Q/VMGR8DnP4TfsyU00QJ"/>
 </BatchItem>
</RequestMessage>
<ResponseMessage>
 <ResponseHeader>
   <ProtocolVersion>
      <ProtocolVersionMajor type="Integer" value="1"/>
      <ProtocolVersionMinor type="Integer" value="3"/>
   </ProtocolVersion>
   <TimeStamp type="DateTime" value="NOW"/>
   <TimeStamp type="DateTime" value="2018-01-29T19:59:26+00:00"/>
   <BatchCount type="Integer" value="2"/>
 </ResponseHeader>
 <BatchItem>
    <Operation type="Enumeration" value="Revoke"/>
   <ResultStatus type="Enumeration" value="Success"/>
   <ResponsePayload>
      <UniqueIdentifier type="TextString" value="EXPORTER_TEMP_SYMM_KEK_UID"/>
      <UniqueIdentifier type="TextString" value="Q/VMGR8DnP4TfsyU00QJ"/>
   </ResponsePayload>
 </BatchItem>
 <BatchItem>
   <Operation type="Enumeration" value="Destroy"/>
   <ResultStatus type="Enumeration" value="Success"/>
   <ResponsePayload>
      <UniqueIdentifier type="TextString" value="EXPORTER_TEMP_SYMM_KEK_UID"/>
      <UniqueIdentifier type="TextString" value="Q/VMGR8DnP4TfsyU00QJ"/>
    </ResponsePayload>
 </BatchItem>
</ResponseMessage>
```

```
<RequestMessage>
   <RequestHeader>
    <ProtocolVersion>
       <ProtocolVersionMajor type="Integer" value="1"/>
       <ProtocolVersionMinor type="Integer" value="3"/>
    </ProtocolVersion>
     <BatchCount type="Integer" value="1"/>
   </RequestHeader>
   <BatchItem>
     <Operation type="Enumeration" value="Register"/>
     <RequestPayload>
       <ObjectType type="Enumeration" value="SymmetricKey"/>
       <TemplateAttribute>
        <Attribute>
           <AttributeName type="TextString" value="Cryptographic Usage Mask"/>
           <AttributeValue type="Integer" value="UnwrapKey"/>
        </Attribute>
        <Attribute>
          <AttributeName type="TextString" value="Cryptographic Parameters"/>
          <AttributeValue>
            <BlockCipherMode type="Enumeration" value="CTR"/>
             <RandomIV type="Boolean" value="true"/>
           </AttributeValue>
        </Attribute>
        <Attribute>
          <AttributeName type="TextString" value="Activation Date"/>
           <AttributeValue type="DateTime" value="NOW-3600"/>
           <AttributeValue type="DateTime" value="2018-01-29T18:58:32.528722"/>
        </Attribute>
       </TemplateAttribute>
       <SymmetricKey>
        <KeyBlock>
           <KeyFormatType type="Enumeration" value="Raw"/>
          <KeyValue type="ByteString" value="EXPORTER_TEMP_SYMM_KEK_KEY_VALUE"/>
<KeyValue type="ByteString" value="8f5184faaf805fc324e29be721467d903cc8d")</pre>
\verb|b5c93aee653c520afe790e74f8cff8192ee73753b31678913d1a41f491aea281fb1d3f1c960cbc023f4ab5ee30d94ccf4973||
33d03ce932f660ba7dadcafb56667dfe99e5f3e7932f8d5fc881d8b370d1b2d3f3525c870c934dfe3f2359515585f421d066
aab5051971c3b7fc78dedf17e51aeee14f18d239a3f746c4e922c2c1ac4eeed44f7e9702033"/>
           <CryptographicAlgorithm type="Enumeration" value="AES"/>
           <CryptographicLength type="Integer" value="128"/>
           <KeyWrappingData>
             <WrappingMethod type="Enumeration" value="Encrypt"/>
            <EncryptionKeyInformation>
              <UniqueIdentifier type="TextString" value="IMPORTER_PRIV_UID"/>
              <UniqueIdentifier type="TextString" value="0M3ey+80IWYEqhrKt1sF"/>
              <CryptographicParameters>
                <CryptographicAlgorithm type="Enumeration" value="RSA"/>
                <PaddingMethod type="Enumeration" value="OAEP"/>
                <HashingAlgorithm type="Enumeration" value="SHA_256"/>
              </CryptographicParameters>
            </EncryptionKeyInformation>
            <EncodingOption type="Enumeration" value="NoEncoding"/>
           </KeyWrappingData>
        </KeyBlock>
       </SymmetricKey>
    </RequestPayload>
   </BatchItem>
 </RequestMessage>
 <ResponseMessage>
   <ResponseHeader>
     <ProtocolVersion>
       <ProtocolVersionMajor type="Integer" value="1"/>
       <ProtocolVersionMinor type="Integer" value="3"/>
```

```
<RequestMessage>
          <RequestHeader>
                <ProtocolVersion>
                       <ProtocolVersionMajor type="Integer" value="1"/>
                       <ProtocolVersionMinor type="Integer" value="3"/>
                </ProtocolVersion>
                <BatchCount type="Integer" value="1"/>
          </RequestHeader>
          <BatchItem>
                 <Operation type="Enumeration" value="Register"/>
                 <RequestPayload>
                       <ObjectType type="Enumeration" value="PrivateKey"/>
                       <TemplateAttribute>
                             <Attribute>
                                    <AttributeName type="TextString" value="Cryptographic Usage Mask"/>
                                    <AttributeValue type="Integer" value="Sign"/>
                             </Attribute>
                             <Attribute>
                                   <AttributeName type="TextString" value="Cryptographic Algorithm"/>
                                    <AttributeValue type="Enumeration" value="RSA"/>
                             </Attribute>
                             <Attribute>
                                    <AttributeName type="TextString" value="Cryptographic Length"/>
                                    <AttributeValue type="Integer" value="2048"/>
                             </Attribute>
                      </TemplateAttribute>
                      <PrivateKey>
                             <KeyBlock>
                                    <KeyFormatType type="Enumeration" value="TransparentRSAPrivateKey"/>
                                    <KeyValue type="ByteString" value="EXPORTER_PRIV_KEY_VALUE"/>
                                    <KeyValue type="ByteString" value="153a70bd7fc40871530d98227d5d2b2cb7cfb</pre>
94a9cd830c464206743be8ad18e75189d9872eeefda83dc96b125ed6aab82e23e97695812fe3487a6fad6d8f9b9cd181fdfa
149c9fb37a21975481c0a3f719363bed5d72c5574e4de34c8ed698a378f6a89cd6e1c8ec69c1866c9cf22552ad3f754547dc
6dc2372bf0325006462bb2843e6898077621d04ba732778453d624718433ae62c828cc7c74cb919448eadebfac0f5a87425a
32dcafe63615b93031dfd2dcbf78f695c03b22176a9d0cf603af81303b8f1ac10492f572479e6ddaa280decc71594284b19f
0 + c_{3} + c_{1} + c_{2} + c_{1} + c_{2} + c_{1} + c_{2} + c_{1} + c_{2} + 
5577c2b271e233a118d7a19d0b7016be30f8598c1599c299399e6be1ced5082f855c3fc5198af13a2dec98b5e8d43236582f
267073735fa8df2883f81094b6936600d852516bf2bb41462bfe79938205ff1b08b712df2083c32ceecf2a76097bfbc227ff
35439c142e5e592392a56fcac843f04e404dcf56aa09147c60fd9af621edc9457bb76805ae4eca1aade7d1efc37794415912afcaffcac843f04e404dcf56aa09147c60fd9af621edc9457bb76805ae4eca1aade7d1efc37794415912afcaffcac843f04e404dcf56aa09147c60fd9af621edc9457bb76805ae4eca1aade7d1efc37794415912afcaffcac843f04e404dcf56aa09147c60fd9af621edc9457bb76805ae4eca1aade7d1efc37794415912afcaffcac843f04e404dcf56aa09147c60fd9af621edc9457bb76805ae4eca1aade7d1efc37794415912afcaffcac843f04e404dcf56aa09147c60fd9af621edc9457bb76805ae4eca1aade7d1efc37794415912afcaffcac843f04e404dcf56aa09147c60fd9af621edc9457bb76805ae4eca1aade7d1efc37794415912afcaffcac843f04e404dcf56aa09147c60fd9af621edc9457bb76805ae4eca1aade7d1efc37794415912afcaffcac843f04e404dcf56aa09147c60fd9af621edc9457bb76805ae4eca1aade7d1efc37794415912afcaffcac843f04e404dcf56aa09147c60fd9af621edc9457bb76805ae4eca1aade7d1efc37794415912afcaffcac843f04e404dcf56aa09147c60fd9af621edc9457bb76805ae4eca1aade7d1efc37794415912afcaffcac8456ae4eca1aade7dfac8456ae4eca1aade7dfac8456ae4eca1aade7dfac8456ae4eca1aade7dfac8456ae4eca1aade7dfac8456ae4eca1aade7dfac8456ae4eca1aade7dfac8456ae4eca1aade7dfac8456ae4eca1aade7dfac8456ae4eca1aade7dfac8456ae4eca1aade7dfac8456ae4eca1aade7dfac8456ae4eca1aade7dfac8456ae4eca1aade7dfac8456ae4eca1aade7dfac8456ae4eca1aade7dfac8456ae4eca1aade7dfac8456ae4eca1aade7dfac8456ae4eca1aade7dfac8456ae4eca1aade7dfac8456ae4eca1aade7dfac8456ae4eca1aade7dfac8456ae4eca1aade7dfac8456ae4eca1aade7dfac8456ae4eca1aade7dfac8456ae4eca1aade7dfac8456ae4eca1aade7dfac8456ae4eca1aade7dfac8456ae4eca1aade7dfac8456ae4eca1aade7dfac8456ae4eca1aade7dfac8456ae4eca1aade7dfac8456ae4eca1aade7dfac8456ae4eca1aade7dfac8456ae4eca1aade7dfac8456ae4eca1aade7dfac8456ae4eca1aade7dfac8456ae4eca1aade7dfac8456ae4eca1aade7dfac8456ae4eca1aade7dfac8456ae4eca1aade7dfac8456ae4eca1aade7dfac846ae4eca1aade7dfac846ae4eca1aade7dfac846ae4eca1aade7dfac846ae4eca1aade7dfac846ae4eca1aade7dfac846ae4eca1aade7dfac846ae4eca1aade7dfac846ae4eca1aade7dfac846ae4eca1aade7dfac866ae4eca1aade7dfac866ae4eca1aade7dfac86ae4eca1aade7dfac86ae4eca1aade7dfac86ae4eca1a
4c997709bb47371217d09f0759c04599f67d67ab86da8ff45dc682bddf4515c529b8c8fa03b1329a788357fe1a889b68f4d1
69136f34ee13d42e807d522ae6794996d088ac4f91dbf26d45dd3dfcd6ed4256f4c1181369d4240a6cacdcf1530c672c50eb
e869d7269a6b05252acb9be7091a771e18c8211badfe930fca3da0ff67bef9f213de050ba868be95a565cf553b0fdbbee69e1264bbe669e1264bbe669e1264bbe669e1264bbe669e1264bbe669e1264bbe669e1264bbe669e1264bbe669e1264bbe669e1264bbe669e1264bbe669e1264bbe669e1264bbe669e1264bbe669e1264bbe669e1264bbe669e1264bbe669e1264bbe669e1264bbe669e1264bb669bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb6709bb67000bb67000bb67000bb67000bb67000bb67000bb67000bb67000bb67000bb67000bb67000bb67000bb67000bb67000bb67000bb67000bb67000bb67000bb67000bb67000bb67000bb67000bb67000bb67000bb67000bb67000bb67000bb67000bb67000bb67000bb67000bb67000bb67000bb67000bb670000bb67000bb67000bb67000bb67000bb67000bb67000bb67000bb67000bb67000bb67000bb67000bb67000bb67000bb6
54e0144a84227 bea4954702 f03f66 bb5d5 caa 905f8177 c5 da1 ac3 c194 b36e68e651394 dc03 c81 c92637 dc15 dc6971 b79392 cases and according to the contraction of the c
9 fac 3311c 4788809f82 da9a 6931387543 eb576f8c 1338772 b2 bc5b35600f 50887f db4 af 15928630 e9d866 e46d883965367 d020 bc5b35600f 50887f db4 af 15928630 e9d866 e46d883965367 d020 bc5b35600 bc5b3
12251e81e2beb3aeea6eb0097fe3adb2e803f2f"/>
                                    <CryptographicAlgorithm type="Enumeration" value="RSA"/>
                                    <CryptographicLength type="Integer" value="2048"/>
                                    <KeyWrappingData>
                                          <WrappingMethod type="Enumeration" value="Encrypt"/>
                                          <EncryptionKeyInformation>
                                                <UniqueIdentifier type="TextString" value="IMPORTER_TEMP_SYMM_KEK_UID</pre>
                                                <UniqueIdentifier type="TextString" value="w6TOdif4zpp1CvK7DtvC"/>
```

```
<CryptographicParameters>
                 <BlockCipherMode type="Enumeration" value="CTR"/>
                 <RandomIV type="Boolean" value="true"/>
               </CryptographicParameters>
             </EncryptionKeyInformation>
             <IVCounterNonce type="ByteString" value="EXPORTER_WRAP_01_IV"/>
             <IVCounterNonce type="ByteString" value="092497b4e2f113b0790e76cc0ef8c</pre>
57f"/>
             <EncodingOption type="Enumeration" value="TTLVEncoding"/>
           </KeyWrappingData>
         </KeyBlock>
       </PrivateKey>
     </RequestPayload>
   </BatchItem>
 </RequestMessage>
 <ResponseMessage>
   <ResponseHeader>
     <ProtocolVersion>
       <ProtocolVersionMajor type="Integer" value="1"/>
       <ProtocolVersionMinor type="Integer" value="3"/>
     </ProtocolVersion>
     <TimeStamp type="DateTime" value="NOW"/>
     <TimeStamp type="DateTime" value="2018-01-29T19:59:27+00:00"/>
     <BatchCount type="Integer" value="1"/>
   </ResponseHeader>
   <BatchItem>
     <Operation type="Enumeration" value="Register"/>
     <ResultStatus type="Enumeration" value="Success"/>
     <ResponsePayload>
       <UniqueIdentifier type="TextString" value="IMPORTER_IMPORTED_UID"/>
       <UniqueIdentifier type="TextString" value="DdTJo6zRp5qQ+Q8KJYzW"/>
     </ResponsePayload>
   </BatchItem>
 </ResponseMessage>
```

```
<RequestMessage>
  <RequestHeader>
    <ProtocolVersion>
      <ProtocolVersionMajor type="Integer" value="1"/>
      <ProtocolVersionMinor type="Integer" value="3"/>
    </ProtocolVersion>
    <BatchCount type="Integer" value="2"/>
  </RequestHeader>
  <BatchItem>
    <Operation type="Enumeration" value="Revoke"/>
    <RequestPayload>
      <UniqueIdentifier type="TextString" value="IMPORTER_TEMP_SYMM_KEK_UID"/>
      <UniqueIdentifier type="TextString" value="w6TOdif4zpp1CvK7DtvC"/>
      <RevocationReason>
        <RevocationReasonCode type="Enumeration" value="CessationOfOperation"/>
      </RevocationReason>
    </RequestPayload>
  </BatchItem>
  <BatchItem>
    <Operation type="Enumeration" value="Destroy"/>
    <RequestPayload>
      <UniqueIdentifier type="TextString" value="IMPORTER_TEMP_SYMM_KEK_UID"/>
      <UniqueIdentifier type="TextString" value="w6TOdif4zpp1CvK7DtvC"/>
  </BatchItem>
</RequestMessage>
<ResponseMessage>
  <ResponseHeader>
    <ProtocolVersion>
      <ProtocolVersionMajor type="Integer" value="1"/>
      <ProtocolVersionMinor type="Integer" value="3"/>
    </ProtocolVersion>
    <TimeStamp type="DateTime" value="NOW"/>
    <TimeStamp type="DateTime" value="2018-01-29T19:59:27+00:00"/>
    <BatchCount type="Integer" value="2"/>
  </ResponseHeader>
  <BatchItem>
    <Operation type="Enumeration" value="Revoke"/>
    <ResultStatus type="Enumeration" value="Success"/>
    <ResponsePayload>
      <UniqueIdentifier type="TextString" value="IMPORTER_TEMP_SYMM_KEK_UID"/>
      <UniqueIdentifier type="TextString" value="w6TOdif4zpp1CvK7DtvC"/>
    </ResponsePayload>
  </BatchItem>
  <BatchItem>
    <Operation type="Enumeration" value="Destroy"/>
    <ResultStatus type="Enumeration" value="Success"/>
    <ResponsePayload>
      <UniqueIdentifier type="TextString" value="IMPORTER_TEMP_SYMM_KEK_UID"/>
      <UniqueIdentifier type="TextString" value="w6TOdif4zpp1CvK7DtvC"/>
    </ResponsePayload>
  </BatchItem>
</ResponseMessage>
```

```
<RequestMessage>
 <RequestHeader>
   <ProtocolVersion>
      <ProtocolVersionMajor type="Integer" value="1"/>
      <ProtocolVersionMinor type="Integer" value="3"/>
   </ProtocolVersion>
    <BatchCount type="Integer" value="5"/>
 </RequestHeader>
 <BatchItem>
    <Operation type="Enumeration" value="Revoke"/>
    <RequestPayload>
      <UniqueIdentifier type="TextString" value="IMPORTER_PRIV_UID"/>
      <UniqueIdentifier type="TextString" value="0M3ey+80IWYEqhrKt1sF"/>
      <RevocationReason>
        <RevocationReasonCode type="Enumeration" value="CessationOfOperation"/>
      </RevocationReason>
    </RequestPayload>
 </BatchItem>
 <BatchItem>
    <Operation type="Enumeration" value="Destroy"/>
   <RequestPayload>
      <UniqueIdentifier type="TextString" value="IMPORTER_PRIV_UID"/>
      <UniqueIdentifier type="TextString" value="0M3ey+80IWYEqhrKt1sF"/>
 </BatchItem>
 <BatchItem>
   <Operation type="Enumeration" value="Revoke"/>
    <RequestPayload>
      <UniqueIdentifier type="TextString" value="IMPORTER_PUB_UID"/>
      <UniqueIdentifier type="TextString" value="9ihkDcG6/K3J2vkgbqlA"/>
      <RevocationReason>
        <RevocationReasonCode type="Enumeration" value="CessationOfOperation"/>
      </RevocationReason>
    </RequestPayload>
 </BatchItem>
 <BatchItem>
    <Operation type="Enumeration" value="Destroy"/>
    <RequestPayload>
      <UniqueIdentifier type="TextString" value="IMPORTER_PUB_UID"/>
      <UniqueIdentifier type="TextString" value="9ihkDcG6/K3J2vkgbqlA"/>
   </RequestPayload>
 </BatchItem>
  <BatchItem>
    <Operation type="Enumeration" value="Destroy"/>
   <RequestPayload>
      <UniqueIdentifier type="TextString" value="IMPORTER_IMPORTED_UID"/>
      <UniqueIdentifier type="TextString" value="DdTJo6zRp5qQ+Q8KJYzW"/>
    </RequestPayload>
 </BatchItem>
</RequestMessage>
<ResponseMessage>
  <ResponseHeader>
   <ProtocolVersion>
      <ProtocolVersionMajor type="Integer" value="1"/>
      <ProtocolVersionMinor type="Integer" value="3"/>
   </ProtocolVersion>
   <TimeStamp type="DateTime" value="NOW"/>
   <TimeStamp type="DateTime" value="2018-01-29T19:59:27+00:00"/>
   <BatchCount type="Integer" value="5"/>
 </ResponseHeader>
 <BatchItem>
    <Operation type="Enumeration" value="Revoke"/>
    <ResultStatus type="Enumeration" value="Success"/>
    <ResponsePayload>
      <UniqueIdentifier type="TextString" value="IMPORTER_PRIV_UID"/>
```

```
<UniqueIdentifier type="TextString" value="OM3ey+80IWYEqhrKt1sF"/>
    </ResponsePayload>
  </BatchItem>
  <BatchItem>
    <Operation type="Enumeration" value="Destroy"/>
    <ResultStatus type="Enumeration" value="Success"/>
    <ResponsePayload>
      <UniqueIdentifier type="TextString" value="IMPORTER_PRIV_UID"/>
      <UniqueIdentifier type="TextString" value="0M3ey+80IWYEqhrKt1sF"/>
    </ResponsePayload>
  </BatchItem>
  <BatchItem>
    <Operation type="Enumeration" value="Revoke"/>
    <ResultStatus type="Enumeration" value="Success"/>
    <ResponsePayload>
      <UniqueIdentifier type="TextString" value="IMPORTER_PUB_UID"/>
      <UniqueIdentifier type="TextString" value="9ihkDcG6/K3J2vkgbqlA"/>
    </ResponsePayload>
 </BatchItem>
  <BatchItem>
    <Operation type="Enumeration" value="Destroy"/>
    <ResultStatus type="Enumeration" value="Success"/>
    <ResponsePayload>
      <UniqueIdentifier type="TextString" value="IMPORTER_PUB_UID"/>
      <UniqueIdentifier type="TextString" value="9ihkDcG6/K3J2vkgbqlA"/>
    </ResponsePayload>
 </BatchItem>
  <BatchItem>
    <Operation type="Enumeration" value="Destroy"/>
    <ResultStatus type="Enumeration" value="Success"/>
    <ResponsePayload>
      <UniqueIdentifier type="TextString" value="IMPORTER_IMPORTED_UID"/>
      <UniqueIdentifier type="TextString" value="DdTJo6zRp5qQ+Q8KJYzW"/>
    </ResponsePayload>
  </BatchItem>
</ResponseMessage>
```

```
<RequestMessage>
 <RequestHeader>
   <ProtocolVersion>
      <ProtocolVersionMajor type="Integer" value="1"/>
      <ProtocolVersionMinor type="Integer" value="3"/>
   </ProtocolVersion>
    <BatchCount type="Integer" value="4"/>
 </RequestHeader>
 <BatchItem>
    <Operation type="Enumeration" value="Revoke"/>
    <RequestPayload>
      <UniqueIdentifier type="TextString" value="EXPORTER_CLIENT_KEK_UID"/>
      <UniqueIdentifier type="TextString" value="YYzt6q4Y0Wdo2EGT6k/Z"/>
      <RevocationReason>
        <RevocationReasonCode type="Enumeration" value="CessationOfOperation"/>
      </RevocationReason>
   </RequestPayload>
 </BatchItem>
  <BatchItem>
    <Operation type="Enumeration" value="Destroy"/>
   <RequestPayload>
      <UniqueIdentifier type="TextString" value="EXPORTER_CLIENT_KEK_UID"/>
      <UniqueIdentifier type="TextString" value="YYzt6q4Y0Wdo2EGT6k/Z"/>
 </BatchItem>
 <BatchItem>
   <Operation type="Enumeration" value="Destroy"/>
   <RequestPayload>
      <UniqueIdentifier type="TextString" value="EXPORTER_TBE_PRIV_UID"/>
      <UniqueIdentifier type="TextString" value="q8vGENBf8p1kgbEYKHu1"/>
   </RequestPayload>
 </BatchItem>
  <BatchItem>
    <Operation type="Enumeration" value="Destroy"/>
    <RequestPayload>
      <UniqueIdentifier type="TextString" value="EXPORTER_TBE_PUB_UID"/>
      <UniqueIdentifier type="TextString" value="ZRGyFcCtfpCEwAwrB0Dz"/>
   </RequestPayload>
 </BatchItem>
</RequestMessage>
<ResponseMessage>
  <ResponseHeader>
    <ProtocolVersion>
      <ProtocolVersionMajor type="Integer" value="1"/>
      <ProtocolVersionMinor type="Integer" value="3"/>
   </ProtocolVersion>
   <TimeStamp type="DateTime" value="NOW"/>
   <TimeStamp type="DateTime" value="2018-01-29T19:59:28+00:00"/>
   <BatchCount type="Integer" value="4"/>
 </ResponseHeader>
 <BatchItem>
    <Operation type="Enumeration" value="Revoke"/>
   <ResultStatus type="Enumeration" value="Success"/>
   <ResponsePayload>
      <UniqueIdentifier type="TextString" value="EXPORTER_CLIENT_KEK_UID"/>
      <UniqueIdentifier type="TextString" value="YYzt6q4Y0Wdo2EGT6k/Z"/>
   </ResponsePayload>
 </BatchItem>
    <Operation type="Enumeration" value="Destroy"/>
   <ResultStatus type="Enumeration" value="Success"/>
    <ResponsePayload>
      <UniqueIdentifier type="TextString" value="EXPORTER_CLIENT_KEK_UID"/>
      <UniqueIdentifier type="TextString" value="YYzt6q4Y0Wdo2EGT6k/Z"/>
   </ResponsePayload>
```

```
</BatchItem>
  <BatchItem>
    <Operation type="Enumeration" value="Destroy"/>
    <ResultStatus type="Enumeration" value="Success"/>
    <ResponsePayload>
      <UniqueIdentifier type="TextString" value="EXPORTER_TBE_PRIV_UID"/>
      <UniqueIdentifier type="TextString" value="q8vGENBf8p1kgbEYKHu1"/>
    </ResponsePayload>
  </BatchItem>
  <BatchItem>
    <Operation type="Enumeration" value="Destroy"/>
    <ResultStatus type="Enumeration" value="Success"/>
    <ResponsePayload>
      <UniqueIdentifier type="TextString" value="EXPORTER_TBE_PUB_UID"/>
<UniqueIdentifier type="TextString" value="ZRGyFcCtfpCEwAwrBODz"/>
    </ResponsePayload>
  </BatchItem>
</ResponseMessage>
```