Relatório de Teste AKLC-M-1-13-password
Dinamo HSM

LabSEC - Universidade Federal de Santa Catatina

2018-02-15

0.1 Execução

```
--- report/expected.tex 2018-02-15 14:11:20.000000000 -0200
+++ report/results.tex 2018-02-15 14:11:20.000000000 -0200
@@ -1,361 +1,353 @@
 <RequestMessage>
   <RequestHeader>
     <ProtocolVersion>
       <ProtocolVersionMajor type="Integer" value="1"/>
       <ProtocolVersionMinor type="Integer" value="1"/>
     </ProtocolVersion>
     <Authentication>
       <Credential>
         <CredentialType type="Enumeration" value="UsernameAndPassword"/>
         <CredentialValue>
           <Username type="TextString" value="ufsc"/>
           <Password type="TextString" value="12345678"/>
         </CredentialValue>
       </Credential>
     </Authentication>
     <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="1024"/>
         </Attribute>
       </CommonTemplateAttribute>
       <PrivateKeyTemplateAttribute>
         <Attribute>
           <AttributeName type="TextString" value="Name"/>
           <AttributeValue>
             <NameValue type="TextString" value="AKLC-M-1-13-private-pass"/>
             <NameType type="Enumeration" value="UninterpretedTextString"/>
           </AttributeValue>
         </Attribute>
         <Attribute>
           <AttributeName type="TextString" value="Cryptographic Usage Mask"/>
           <AttributeValue type="Integer" value="Sign"/>
         </Attribute>
       </PrivateKeyTemplateAttribute>
       <PublicKeyTemplateAttribute>
         <Attribute>
           <AttributeName type="TextString" value="Name"/>
           <AttributeValue>
             <NameValue type="TextString" value="AKLC-M-1-13-public-pass"/>
             <NameType type="Enumeration" value="UninterpretedTextString"/>
           </AttributeValue>
         </Attribute>
         <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="1"/>
+      <ProtocolVersionMinor type="Integer" value="4"/>
     </ProtocolVersion>
-    <TimeStamp type="DateTime" value="NOW"/>
+    <TimeStamp type="DateTime" value="2018-02-15T12:10:28+00:00"/>
     <BatchCount type="Integer" value="1"/>
   </ResponseHeader>
   <BatchItem>
     <Operation type="Enumeration" value="CreateKeyPair"/>
     <ResultStatus type="Enumeration" value="Success"/>
     <ResponsePayload>
-      <PrivateKeyUniqueIdentifier type="TextString" value="UNIQUE_IDENTIFIER_0"/>
-      <PublicKeyUniqueIdentifier type="TextString" value="UNIQUE_IDENTIFIER_1"/>
+      <PrivateKeyUniqueIdentifier type="TextString" value="071C32A5E30B7966B98A3E4
712E15C37"/>
+      <PublicKeyUniqueIdentifier type="TextString" value="B6FB05B8A40BAF11467B7763
4AB40963"/>
     </ResponsePayload>
   </BatchItem>
 </ResponseMessage>
```

```
 <RequestMessage>
   <RequestHeader>
     <ProtocolVersion>
       <ProtocolVersionMajor type="Integer" value="1"/>
       <ProtocolVersionMinor type="Integer" value="1"/>
     </ProtocolVersion>
     <Authentication>
       <Credential>
         <CredentialType type="Enumeration" value="UsernameAndPassword"/>
         <CredentialValue>
           <Username type="TextString" value="ufsc"/>
           <Password type="TextString" value="12345678"/>
         </CredentialValue>
       </Credential>
     </Authentication>
     <BatchCount type="Integer" value="1"/>
   </RequestHeader>
   <BatchItem>
     <Operation type="Enumeration" value="GetAttributes"/>
     <RequestPayload>
-      <UniqueIdentifier type="TextString" value="UNIQUE_IDENTIFIER_0"/>
+      <UniqueIdentifier type="TextString" value="071C32A5E30B7966B98A3E4712E15C37"
/>
       <AttributeName type="TextString" value="State"/>
       <AttributeName type="TextString" value="Cryptographic Usage Mask"/>
       <AttributeName type="TextString" value="Unique Identifier"/>
       <AttributeName type="TextString" value="Object Type"/>
       <AttributeName type="TextString" value="Cryptographic Algorithm"/>
       <AttributeName type="TextString" value="Cryptographic Length"/>
       <AttributeName type="TextString" value="Digest"/>
       <AttributeName type="TextString" value="Initial Date"/>
       <AttributeName type="TextString" value="Last Change Date"/>
       <AttributeName type="TextString" value="Activation Date"/>
       <AttributeName type="TextString" value="Original Creation Date"/>
     </RequestPayload>
   </BatchItem>
 </RequestMessage>
 <ResponseMessage>
   <ResponseHeader>
     <ProtocolVersion>
       <ProtocolVersionMajor type="Integer" value="1"/>
-      <ProtocolVersionMinor type="Integer" value="3"/>
+      <ProtocolVersionMinor type="Integer" value="4"/>
     </ProtocolVersion>
-    <TimeStamp type="DateTime" value="NOW"/>
+    <TimeStamp type="DateTime" value="2018-02-15T12:10:29+00:00"/>
     <BatchCount type="Integer" value="1"/>
   </ResponseHeader>
   <BatchItem>
     <Operation type="Enumeration" value="GetAttributes"/>
     <ResultStatus type="Enumeration" value="Success"/>
     <ResponsePayload>
-      <UniqueIdentifier type="TextString" value="UNIQUE_IDENTIFIER_0"/>
+      <UniqueIdentifier type="TextString" value="071C32A5E30B7966B98A3E4712E15C37"
/>
       <Attribute>
         <AttributeName type="TextString" value="State"/>
-        <AttributeValue type="Enumeration" value="PreActive"/>
-      </Attribute>
-      <Attribute>
-        <AttributeName type="TextString" value="Cryptographic Usage Mask"/>
-        <AttributeValue type="Integer" value="Sign"/>
-      </Attribute>
-      <Attribute>
-        <AttributeName type="TextString" value="Unique Identifier"/>
```

```
-         <AttributeValue type="TextString" value="UNIQUE_IDENTIFIER_0"/>
+         <AttributeValue type="Enumeration" value="0x00000001"/>
        </Attribute>
        <Attribute>
          <AttributeName type="TextString" value="Object Type"/>
-         <AttributeValue type="Enumeration" value="PrivateKey"/>
+         <AttributeValue type="Enumeration" value="0x00000004"/>
        </Attribute>
        <Attribute>
          <AttributeName type="TextString" value="Cryptographic Algorithm"/>
-         <AttributeValue type="Enumeration" value="RSA"/>
+         <AttributeValue type="Enumeration" value="0x00000004"/>
        </Attribute>
        <Attribute>
          <AttributeName type="TextString" value="Cryptographic Length"/>
          <AttributeValue type="Integer" value="1024"/>
        </Attribute>
        <Attribute>
          <AttributeName type="TextString" value="Digest"/>
          <AttributeValue>
            <HashingAlgorithm type="Enumeration" value="SHA_256"/>
-           <DigestValue type="ByteString" value="8eb422ae2b006a05d3c8a542a2853673524
1b6dc1c37926bc8007bd6220d9230"/>
+           <DigestValue type="ByteString" value="5ac3ef59fb826afdcadb5756a5b25cfc3d
f9c274c4138b021c55a69fe42b2a40"/>
            <KeyFormatType type="Enumeration" value="PKCS_1"/>
          </AttributeValue>
        </Attribute>
        <Attribute>
+         <AttributeName type="TextString" value="Cryptographic Usage Mask"/>
+         <AttributeValue type="Integer" value="1"/>
+       </Attribute>
+       <Attribute>
          <AttributeName type="TextString" value="Initial Date"/>
-         <AttributeValue type="DateTime" value="NOW"/>
+         <AttributeValue type="DateTime" value="2018-02-15T12:10:28+00:00"/>
        </Attribute>
        <Attribute>
          <AttributeName type="TextString" value="Last Change Date"/>
-         <AttributeValue type="DateTime" value="NOW"/>
+         <AttributeValue type="DateTime" value="2018-02-15T12:10:28+00:00"/>
        </Attribute>
        <Attribute>
          <AttributeName type="TextString" value="Original Creation Date"/>
-         <AttributeValue type="DateTime" value="NOW"/>
+         <AttributeValue type="DateTime" value="2018-02-15T12:10:28+00:00"/>
        </Attribute>
      </ResponsePayload>
    </BatchItem>
  </ResponseMessage>
```

```
 <RequestMessage>
   <RequestHeader>
     <ProtocolVersion>
       <ProtocolVersionMajor type="Integer" value="1"/>
       <ProtocolVersionMinor type="Integer" value="3"/>
     </ProtocolVersion>
     <Authentication>
       <Credential>
         <CredentialType type="Enumeration" value="UsernameAndPassword"/>
         <CredentialValue>
           <Username type="TextString" value="ufsc"/>
           <Password type="TextString" value="12345678"/>
         </CredentialValue>
       </Credential>
     </Authentication>
     <BatchCount type="Integer" value="1"/>
   </RequestHeader>
   <BatchItem>
     <Operation type="Enumeration" value="GetAttributes"/>
     <RequestPayload>
-      <UniqueIdentifier type="TextString" value="UNIQUE_IDENTIFIER_1"/>
+      <UniqueIdentifier type="TextString" value="B6FB05B8A40BAF11467B77634AB40963"
/>
       <AttributeName type="TextString" value="State"/>
       <AttributeName type="TextString" value="Cryptographic Usage Mask"/>
       <AttributeName type="TextString" value="Unique Identifier"/>
       <AttributeName type="TextString" value="Object Type"/>
       <AttributeName type="TextString" value="Cryptographic Algorithm"/>
       <AttributeName type="TextString" value="Cryptographic Length"/>
       <AttributeName type="TextString" value="Digest"/>
       <AttributeName type="TextString" value="Initial Date"/>
       <AttributeName type="TextString" value="Last Change Date"/>
       <AttributeName type="TextString" value="Activation Date"/>
       <AttributeName type="TextString" value="Original Creation Date"/>
     </RequestPayload>
   </BatchItem>
 </RequestMessage>
 <ResponseMessage>
   <ResponseHeader>
     <ProtocolVersion>
       <ProtocolVersionMajor type="Integer" value="1"/>
-      <ProtocolVersionMinor type="Integer" value="3"/>
+      <ProtocolVersionMinor type="Integer" value="4"/>
     </ProtocolVersion>
-    <TimeStamp type="DateTime" value="NOW"/>
+    <TimeStamp type="DateTime" value="2018-02-15T12:10:29+00:00"/>
     <BatchCount type="Integer" value="1"/>
   </ResponseHeader>
   <BatchItem>
     <Operation type="Enumeration" value="GetAttributes"/>
     <ResultStatus type="Enumeration" value="Success"/>
     <ResponsePayload>
-      <UniqueIdentifier type="TextString" value="UNIQUE_IDENTIFIER_1"/>
+      <UniqueIdentifier type="TextString" value="B6FB05B8A40BAF11467B77634AB40963"
/>
       <Attribute>
         <AttributeName type="TextString" value="State"/>
-        <AttributeValue type="Enumeration" value="PreActive"/>
-      </Attribute>
-      <Attribute>
-        <AttributeName type="TextString" value="Cryptographic Usage Mask"/>
-        <AttributeValue type="Integer" value="Verify"/>
-      </Attribute>
-      <Attribute>
-        <AttributeName type="TextString" value="Unique Identifier"/>
```

```
-         <AttributeValue type="TextString" value="UNIQUE_IDENTIFIER_1"/>
+         <AttributeValue type="Enumeration" value="0x00000001"/>
        </Attribute>
        <Attribute>
          <AttributeName type="TextString" value="Object Type"/>
-         <AttributeValue type="Enumeration" value="PublicKey"/>
+         <AttributeValue type="Enumeration" value="0x00000003"/>
        </Attribute>
        <Attribute>
          <AttributeName type="TextString" value="Cryptographic Algorithm"/>
-         <AttributeValue type="Enumeration" value="RSA"/>
+         <AttributeValue type="Enumeration" value="0x00000004"/>
        </Attribute>
        <Attribute>
          <AttributeName type="TextString" value="Cryptographic Length"/>
          <AttributeValue type="Integer" value="1024"/>
        </Attribute>
        <Attribute>
          <AttributeName type="TextString" value="Digest"/>
          <AttributeValue>
            <HashingAlgorithm type="Enumeration" value="SHA_256"/>
-           <DigestValue type="ByteString" value="82bcff8afab753809db804e654013ded708
c3996a50c6ce9313f9b3915442ce9"/>
+           <DigestValue type="ByteString" value="ee93f77f349ca6661001d3952a4e2dbc1a
791ae893cca0abe10588046077ea5e"/>
            <KeyFormatType type="Enumeration" value="PKCS_1"/>
          </AttributeValue>
        </Attribute>
        <Attribute>
+         <AttributeName type="TextString" value="Cryptographic Usage Mask"/>
+         <AttributeValue type="Integer" value="2"/>
+       </Attribute>
+       <Attribute>
          <AttributeName type="TextString" value="Initial Date"/>
-         <AttributeValue type="DateTime" value="NOW"/>
+         <AttributeValue type="DateTime" value="2018-02-15T12:10:28+00:00"/>
        </Attribute>
        <Attribute>
          <AttributeName type="TextString" value="Last Change Date"/>
-         <AttributeValue type="DateTime" value="NOW"/>
+         <AttributeValue type="DateTime" value="2018-02-15T12:10:28+00:00"/>
        </Attribute>
        <Attribute>
          <AttributeName type="TextString" value="Original Creation Date"/>
-         <AttributeValue type="DateTime" value="NOW"/>
+         <AttributeValue type="DateTime" value="2018-02-15T12:10:28+00:00"/>
        </Attribute>
      </ResponsePayload>
    </BatchItem>
  </ResponseMessage>
```

```
 <RequestMessage>
   <RequestHeader>
     <ProtocolVersion>
       <ProtocolVersionMajor type="Integer" value="1"/>
       <ProtocolVersionMinor type="Integer" value="3"/>
     </ProtocolVersion>
     <Authentication>
       <Credential>
         <CredentialType type="Enumeration" value="UsernameAndPassword"/>
         <CredentialValue>
           <Username type="TextString" value="ufsc"/>
           <Password type="TextString" value="12345678"/>
         </CredentialValue>
       </Credential>
     </Authentication>
     <BatchCount type="Integer" value="1"/>
   </RequestHeader>
   <BatchItem>
     <Operation type="Enumeration" value="Destroy"/>
     <RequestPayload>
-      <UniqueIdentifier type="TextString" value="UNIQUE_IDENTIFIER_0"/>
+      <UniqueIdentifier type="TextString" value="071C32A5E30B7966B98A3E4712E15C37"
/>
     </RequestPayload>
   </BatchItem>
 </RequestMessage>
 <ResponseMessage>
   <ResponseHeader>
     <ProtocolVersion>
       <ProtocolVersionMajor type="Integer" value="1"/>
-      <ProtocolVersionMinor type="Integer" value="3"/>
+      <ProtocolVersionMinor type="Integer" value="4"/>
     </ProtocolVersion>
-    <TimeStamp type="DateTime" value="NOW"/>
+    <TimeStamp type="DateTime" value="2018-02-15T12:10:29+00:00"/>
     <BatchCount type="Integer" value="1"/>
   </ResponseHeader>
   <BatchItem>
     <Operation type="Enumeration" value="Destroy"/>
     <ResultStatus type="Enumeration" value="Success"/>
     <ResponsePayload>
-      <UniqueIdentifier type="TextString" value="UNIQUE_IDENTIFIER_0"/>
+      <UniqueIdentifier type="TextString" value="071C32A5E30B7966B98A3E4712E15C37"
/>
     </ResponsePayload>
   </BatchItem>
 </ResponseMessage>
```

```
 <RequestMessage>
   <RequestHeader>
     <ProtocolVersion>
       <ProtocolVersionMajor type="Integer" value="1"/>
       <ProtocolVersionMinor type="Integer" value="1"/>
     </ProtocolVersion>
     <Authentication>
       <Credential>
         <CredentialType type="Enumeration" value="UsernameAndPassword"/>
         <CredentialValue>
           <Username type="TextString" value="ufsc"/>
           <Password type="TextString" value="12345678"/>
         </CredentialValue>
       </Credential>
     </Authentication>
     <BatchCount type="Integer" value="1"/>
   </RequestHeader>
   <BatchItem>
     <Operation type="Enumeration" value="Destroy"/>
     <RequestPayload>
-      <UniqueIdentifier type="TextString" value="UNIQUE_IDENTIFIER_1"/>
+      <UniqueIdentifier type="TextString" value="B6FB05B8A40BAF11467B77634AB40963"
/>
     </RequestPayload>
   </BatchItem>
 </RequestMessage>
 <ResponseMessage>
   <ResponseHeader>
     <ProtocolVersion>
       <ProtocolVersionMajor type="Integer" value="1"/>
-      <ProtocolVersionMinor type="Integer" value="3"/>
+      <ProtocolVersionMinor type="Integer" value="4"/>
     </ProtocolVersion>
-    <TimeStamp type="DateTime" value="NOW"/>
+    <TimeStamp type="DateTime" value="2018-02-15T12:10:29+00:00"/>
     <BatchCount type="Integer" value="1"/>
   </ResponseHeader>
   <BatchItem>
     <Operation type="Enumeration" value="Destroy"/>
     <ResultStatus type="Enumeration" value="Success"/>
     <ResponsePayload>
-      <UniqueIdentifier type="TextString" value="UNIQUE_IDENTIFIER_1"/>
+      <UniqueIdentifier type="TextString" value="B6FB05B8A40BAF11467B77634AB40963"
/>
     </ResponsePayload>
   </BatchItem>
 </ResponseMessage>
```