StrongKey® Securing the Core

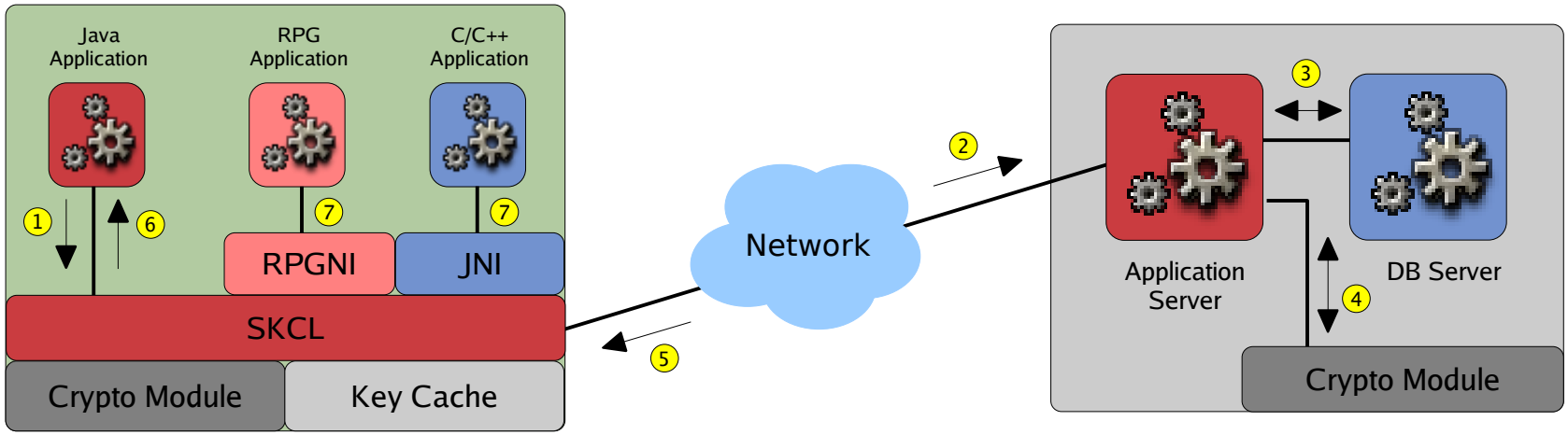
Securing Data Across the Enterprise using SOA

Section III
SKSML Protocol

OASIS Open Standards
April 28, 2008

Arshad Noor, StrongAuth, Inc.
arshad.noor@strongauth.com

The Big Picture



1. Client Application makes a request for a symmetric key
2. SKCL makes a digitally signed request to the SKS
3. SKS verifies SKCL request, generates, encrypts, digitally signs & escrows key in DB
4. Crypto HSM provides security for RSA Signing & Encryption keys of SKS
5. SKS responds to SKCL with signed and encrypted symmetric key
6. SKCL verifies response, decrypts key and hands it to the Client Application
7. Native (non-Java) applications make requests through Java Native Interface

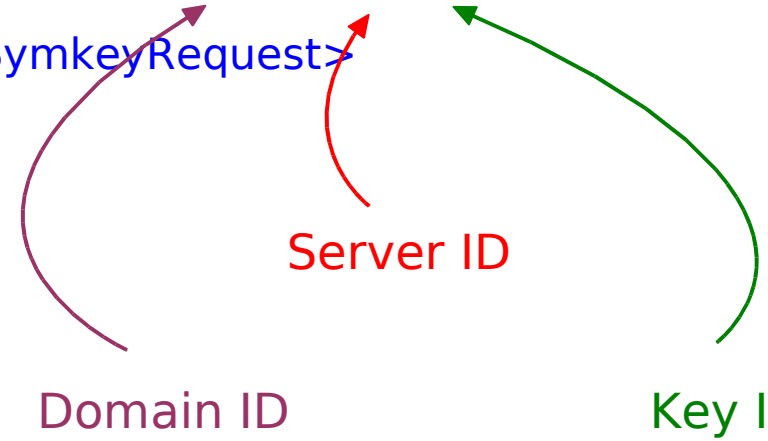
SKSML Protocol

- Symmetric Key Services Markup Language
- Donated to OASIS on royalty-free basis by StrongAuth, Inc.
- Currently at DRAFT version 3; anticipated standard in Summer 2008
- Two (2) Request types
- Three (3) Response types

SKSML Protocol

- Request for a new Symmetric Key

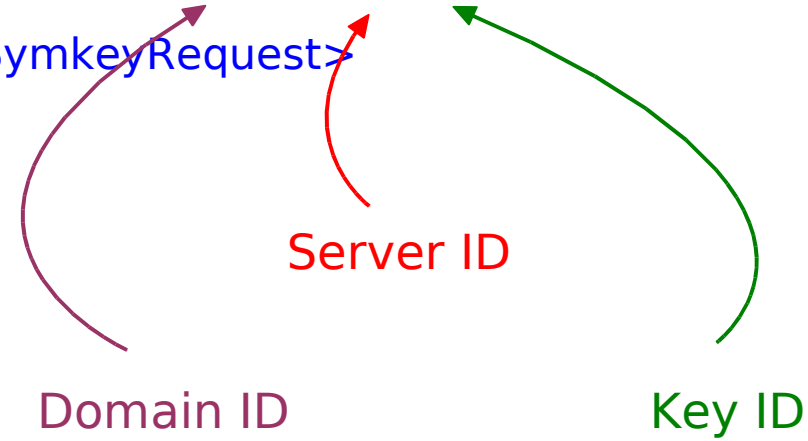
```
ekmi:SymkeyRequest xmlns:ekmi=”http://docs.oasis-open.org/ekmi/2008/01">
      <ekmi:GKID>10514-0-0</ekmi:GKID>
</ekmi:SymkeyRequest>
```



SKSML Protocol

- Request for an existing Symmetric Key

```
ekmi:SymkeyRequest xmlns:ekmi=”http://docs.oasis-open.org/ekmi/2008/01">
      <ekmi:GKID>10514-4-312</ekmi:GKID>
</ekmi:SymkeyRequest>
```



SKSML Protocol

- Request for a new Symmetric Key of a particular KeyClass

```
ekmi:SymkeyRequest xmlns:ekmi=”http://docs.oasis-open.org/ekmi/2008/01">
    <ekmi:GKID>10514-0-0</ekmi:GKID>
    <ekmi:KeyClasses>
        <ekmi:KeyClass>HR-Class</ekmi:KeyClass>
    </ekmi:KeyClasses>
</ekmi:SymkeyRequest>
```

SKSML Protocol

- Request for many new Symmetric Keys of specific KeyClasses

```
ekmi:SymkeyRequest xmlns:ekmi="http://docs.oasis-open.org/ekmi/2008/01">
    <ekmi:GKID>10514-0-0</ekmi:GKID>
    <ekmi:KeyClasses>
        <ekmi:KeyClass>EHR-CDC</ekmi:KeyClass>
        <ekmi:KeyClass>EHR-CRO</ekmi:KeyClass>
        <ekmi:KeyClass>EHR-DEF</ekmi:KeyClass>
        <ekmi:KeyClass>EHR-EMT</ekmi:KeyClass>
        <ekmi:KeyClass>EHR-HOS</ekmi:KeyClass>
        <ekmi:KeyClass>EHR-INS</ekmi:KeyClass>
        <ekmi:KeyClass>EHR-NUR</ekmi:KeyClass>
        <ekmi:KeyClass>EHR-PAT</ekmi:KeyClass>
        <ekmi:KeyClass>EHR-PHY</ekmi:KeyClass>
    </ekmi:KeyClasses>
</ekmi:SymkeyRequest>
```

SKSML Protocol

- Request for many existing Symmetric Keys

```
ekmi:SymkeyRequest xmlns:ekmi=”http://docs.oasis-open.org/ekmi/2008/01">
    <ekmi:GKID>10514-4-312</ekmi:GKID>
    <ekmi:GKID>10514-4-313</ekmi:GKID>
    <ekmi:GKID>10514-4-314</ekmi:GKID>
    <ekmi:GKID>10514-4-315</ekmi:GKID>
    <ekmi:GKID>10514-4-316</ekmi:GKID>
</ekmi:SymkeyRequest>
```

SKSML Protocol

- Successful Symmetric Key Response with one key

```
<ekmi:SymkeyResponse
        xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
        xmlns:ekmi="http://docs.oasis-open.org/ekmi/2008/01">
    <ekmi:Symkey>      .....      </ekmi:Symkey>
</ekmi:SymkeyResponse>
```

SKSML Protocol

- Successful Symmetric Key Response with multiple keys

```
<ekmi:SymkeyResponse
        xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
        xmlns:ekmi="http://docs.oasis-open.org/ekmi/2008/01">
    <ekmi:Symkey>      .....      </ekmi:Symkey>
    <ekmi:Symkey>      .....      </ekmi:Symkey>
    <ekmi:Symkey>      .....      </ekmi:Symkey>
</ekmi:SymkeyResponse>
```

SKSML Protocol

- Failed Symmetric Key Response for one key

```
<ekmi:SymkeyResponse
        xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
        xmlns:ekmi="http://docs.oasis-open.org/ekmi/2008/01">
    <ekmi:SymkeyError>      .......      </ekmi:SymkeyError>
</ekmi:SymkeyResponse>
```

SKSML Protocol

- Failed Symmetric Key Response for one key

```
<ekmi:SymkeyResponse
        xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
        xmlns:ekmi="http://docs.oasis-open.org/ekmi/2008/01">
    <ekmi:SymkeyError>      .....      </ekmi:SymkeyError>
    <ekmi:SymkeyError>      .....      </ekmi:SymkeyError>
</ekmi:SymkeyResponse>
```

SKSML Protocol

- Mixed Symmetric Key Response for multiple keys

```
<ekmi:SymkeyResponse
        xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
        xmlns:ekmi="http://docs.oasis-open.org/ekmi/2008/01">
    <ekmi:Symkey>       .....       </ekmi:Symkey>
    <ekmi:Symkey>       .....       </ekmi:Symkey>
    <ekmi:SymkeyError>      .....       </ekmi:SymkeyError>
    <ekmi:SymkeyError>      .....       </ekmi:SymkeyError>
</ekmi:SymkeyResponse>
```

SKSML Protocol

- Symkey element

```
<ekmi:SymkeyResponse
        xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
        xmlns:ekmi="http://docs.oasis-open.org/ekmi/2008/01">

    <ekmi:Symkey>
        <ekmi:GKID>10514-1-287</ekmi:GKID>
        <ekmi:KeyUsePolicy>      .....      </ekmi:KeyUsePolicy>
        <ekmi:EncryptionMethod Algorithm=
            "http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
        <xenc:CipherData>
            <xenc:CipherValue>
                huUYJMtaGHtXuLlWtx27STRcRpIsY=
            </xenc:CipherValue>
        </xenc:CipherData>
    </ekmi:Symkey>

</ekmi:SymkeyResponse>
```

SKSML Protocol

- KeyUsePolicy element

```
<ekmi:KeyUsePolicy>
    <ekmi:KUPID>10514-4</ekmi:KUPID>
    <ekmi:PolicyName>DES-EDE KeyUsePolicy</ekmi:PolicyName>
    <ekmi:KeyClass>HR-Class</ekmi:KeyClass>
    <ekmi:KeyAlgorithm>http://www.w3.org/2001/04/xmlenc#tripledes-cbc</ekmi:KeyAlgorithm>
    <ekmi:KeySize>192</ekmi:KeySize>
    <ekmi:Status>Active</ekmi:Status>
    <ekmi:Permissions>      .....      </ekmi:Permissions>
</ekmi:KeyUsePolicy>
```

SKSML Protocol

- Permissions element

```
<ekmi:Permissions>
    <ekmi:PermittedApplications> ..... </ekmi:PermittedApplications>
    <ekmi:PermittedDates>    .....      </ekmi:PermittedDates>
    <ekmi:PermittedDuration>     .....  </ekmi:PermittedDuration>
    <ekmi:PermittedLevels>   .....      </ekmi:PermittedLevels>
    <ekmi:PermittedLocations>    .....  </ekmi:PermittedLocations>
    <ekmi:PermittedTimes>    .....      </ekmi:PermittedTimes>
    <ekmi:PermittedTransactions> ..... </ekmi:PermittedTransactions>
    <ekmi:PermittedUses>     .....      </ekmi:PermittedUses>
    <ekmi:Other>     .....              </ekmi:Other>
</ekmi:Permissions>
```

SKSML Protocol

- KeyUsePolicy element

```
<ekmi:KeyUsePolicy>
        <ekmi:KUPID>10514-4</ekmi:KUPID>
        <ekmi:PolicyName>DES-EDE KeyUsePolicy</ekmi:PolicyName>
        <ekmi:KeyClass>HR-Class</ekmi:KeyClass>
        <ekmi:KeyAlgorithm>http://www.w3.org/2001/04/xmlenc#tripledes-cbc</ekmi:KeyAlgorithm>
        <ekmi:KeySize>192</ekmi:KeySize>
        <ekmi:Status>Active</ekmi:Status>
        <ekmi:Permissions>
                <ekmi:PermittedApplications>
                        <ekmi:PermittedApplication>
                                <ekmi:ID>10514-23</ekmi:ID>
                                <ekmi:ApplicationName>Payroll Application</ekmi:ApplicationName>
                                <ekmi:Version>1.0</ekmi:Version>
                                <ekmi:DigestAlgorithm>http://www.w3.org/2000/09/xmldsig#sha1</ekmi:DigestAlgorithm>
                                <ekmi:DigestValue>NIG4bKkt4cziEqFFuOoBTM81efU=</ekmi:DigestValue>
                        </ekmi:PermittedApplication>
                </ekmi:PermittedApplications>
                <ekmi:PermittedDates>
                        <ekmi:PermittedDate>
                                <ekmi:StartDate>2008-01-01</ekmi:StartDate>
                                <ekmi:EndDate>2008-12-31</ekmi:EndDate>
                        </ekmi:PermittedDate>
                </ekmi:PermittedDates>
                <ekmi:PermittedTimes>
                        <ekmi:PermittedTime>
                                <ekmi:StartTime>07:00:00</ekmi:StartTime>
                                <ekmi:EndTime>19:00:00</ekmi:EndTime>
                        </ekmi:PermittedTime>
                </ekmi:PermittedTimes>
        </ekmi:Permissions>
</ekmi:KeyUsePolicy>
```

SKSML Protocol

- Symmetric Key Response

```
<ekmi:SymkeyResponse xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" xmlns:ekmi="http://docs.oasis-open.org/ekmi/2008/01">
    <ekmi:Symkey>
        <ekmi:GKID>10514-1-235</ekmi:GKID>
        <ekmi:KeyUsePolicy>
            <ekmi:KUPID>10514-4</ekmi:KUPID>
            <ekmi:PolicyName>DES-EDE KeyUsePolicy</ekmi:PolicyName>
            <ekmi:KeyClass>HR-Class</ekmi:KeyClass>
            <ekmi:KeyAlgorithm>http://www.w3.org/2001/04/xmlenc#tripledes-cbc</ekmi:KeyAlgorithm>
            <ekmi:KeySize>192</ekmi:KeySize>
            <ekmi:Status>Active</ekmi:Status>
            <ekmi:Permissions>
                <ekmi:PermittedApplications>
                    <ekmi:PermittedApplication>
                        <ekmi:ID>10514-23</ekmi:ID>
                        <ekmi:ApplicationName>Payroll Application</ekmi:ApplicationName>
                        <ekmi:Version>1.0</ekmi:Version>
                        <ekmi:DigestAlgorithm>http://www.w3.org/2000/09/xmldsig#sha1</ekmi:DigestAlgorithm>
                        <ekmi:DigestValue>NIG4bKkt4cziEqFFuOoBTM81efU=</ekmi:DigestValue>
                    </ekmi:PermittedApplication>
                </ekmi:PermittedApplications>
                <ekmi:PermittedDates>
                    <ekmi:PermittedDate>
                        <ekmi:StartDate>2008-01-01</ekmi:StartDate>
                        <ekmi:EndDate>2008-12-31</ekmi:EndDate>
                    </ekmi:PermittedDate>
                </ekmi:PermittedDates>
                <ekmi:PermittedTimes>
                    <ekmi:PermittedTime>
                        <ekmi:StartTime>07:00:00</ekmi:StartTime>
                        <ekmi:EndTime>19:00:00</ekmi:EndTime>
                    </ekmi:PermittedTime>
                </ekmi:PermittedTimes>
            </ekmi:Permissions>
        </ekmi:KeyUsePolicy>
        <ekmi:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
        <xenc:CipherData>
            <xenc:CipherValue>Yjv9h5FDqUiQXG0ca8EU871zBoXBjDXmlNxTux+mt1tXuLlWtx27STRcRpIsY=</xenc:CipherValue>
        </xenc:CipherData>
    </ekmi:Symkey>
</ekmi:SymkeyResponse>
```

SKSML Protocol

- SymkeyError element

```
<ekmi:SymkeyResponse
        xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
        xmlns:ekmi="http://docs.oasis-open.org/ekmi/2008/01">

    <ekmi:SymkeyError>
        <ekmi:RequestedGKID>10514-0-0</ekmi:RequestedGKID>
        <ekmi:RequestedKeyClass>Payroll</ekmi:RequestedKeyClass>
        <ekmi:ErrorCode>SKS-100010</ekmi:ErrorCode>
        <ekmi:ErrorMessage>
            Unauthorized to request this key-class
        </ekmi:ErrorMessage>
    </ekmi:SymkeyError>

</ekmi:SymkeyResponse>
```

SKSML Protocol

- SymkeyError element

```
<ekmi:SymkeyResponse
        xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
        xmlns:ekmi="http://docs.oasis-open.org/ekmi/2008/01">

    <ekmi:SymkeyError>
        <ekmi:RequestedGKID>10514-2-2254</ekmi:RequestedGKID>
        <ekmi:ErrorCode>SKS-100004</ekmi:ErrorCode>
        <ekmi:ErrorMessage>Unauthorized request</ekmi:ErrorMessage>
    </ekmi:SymkeyError>
    <ekmi:SymkeyError>
        <ekmi:RequestedGKID>10514-0-2254</ekmi:RequestedGKID>
        <ekmi:ErrorCode>SKS-100001</ekmi:ErrorCode>
        <ekmi:ErrorMessage>Invalid GKID</ekmi:ErrorMessage>
    </ekmi:SymkeyError>

</ekmi:SymkeyResponse>
```

SKSML Protocol

- Request for a Key Caching Policy

```
<ekmi:KCPRequest   xmlns:ekmi="http://doc.oasis-open.org/ekmi/2008/01"/>
```

SKSML Protocol

- Full SOAP request for a Key Caching Policy

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header>
    <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" SOAP-ENV:mustUnderstand="1">
      <wsse:BinarySecurityToken xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" EncodingType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3"
wsu:Id="XWSSGID-1172790286164-631000224">MIIDfDCCAmSgAwIBAgIIAe/AvliGc3AwDQYJKoZIhvcNAQELBQAwZzEmMCQGA1UEAxMdU3Ryb25n
          S2V5IERFTU8gU3Vib3JkaW5hdGUgQ0ExJDAiBgNVBAsTG0ZvciBTdHJvbmdLZXkgREVNTyBVc2Ug
          T25seTEXMBUGA1UEChMOU3Ryb25nQXV0aCBJbmMwHhcNMDYwNzI1MTcxMDMwWhcNMDcwNzI1MTcy
          MDMwWjBtMREwDwYKCZImiZPyLGQBARMBMjEZMBcGA1UEAxMQUE9TIFJlZ2lzdGVyIDIyMjEkMCIG
          A1UECxMbRm9yIFN0cm9uZ0tleSBERU1PIFVzZSBPbmx5MRcwFQYDVQQKEw5TdHJvbmdBdXRoIElua
          YzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAyAmxMZhYA8wHJ4UE4b61s51JVWe4Fygj4MCf
          U7LA3JhpUS4TlX0XFWqrcmltLOiVG7YBFarJFluBFJW2X6q8FuvUprv4V9nJrgiwAPtkiRyIx96n
          qKXIxkUlQ4idIEg1AZI9dEdf4Y5cqBBCygPYnBoTudgIM7R47AjR4nr4ks8CAwEAAaOBqTCBpjAO\
          MTAvoC2gK4YpaHR0cDovL2RlbW8uc3Ryb25na2V5Lm9yZy9kZW1vLXN1Yi1jYS5jcmwwDQYJKoZI
          hvcNAQELBQADggEBACK05PtvZD4WPglOe+EHUiApzFyCdRzf0pFZtxRwG9lR1PZUWUjmwTNfGFsL
          S6kyoHgUfVa5fpT1EU1mXUB/Lmo3hFGyprZjfmD7DwuBcYgmZHv7yHrmGOMIOXjFTACvHpM0vOce
          hVx2e4VE0yhBLu/ldH9awGGDp6Bk2XzxqQcs8y6ZzOXZAnPgKQZdjbFKERSsy/d1D8pk5baBk4bd
          Zh568OcaUrbm9ZReRVTVaY5qiQpkOU+tDrBSj/HIL6GAqegYllkz6KYCy6RVOy6iVVSjHocDqdJr
          EVOR+ds6xn8mmojdlERrILmuxiLpibPp609SfnDIxNlzLwe5g7ep3lc=</wsse:BinarySecurityToken>
          <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
          <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
              <InclusiveNamespaces xmlns="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="wsse SOAP-ENV"/>
            </ds:CanonicalizationMethod>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
            <ds:Reference URI="#XWSSGID-1172790287316421676595">|
              <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
              <ds:DigestValue>xgITEmXg4yMMg+RkKDTyVUw87VM=</ds:DigestValue>
            </ds:Reference>
            <ds:Reference URI="#XWSSGID-11727902873271435349604">
              <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
              <ds:DigestValue>tlWtno1OMA7Os8GCZrUhmHXmmhM=</ds:DigestValue>
            </ds:Reference>
          </ds:SignedInfo>
          <ds:SignatureValue>Uv1zAePPoQmFey6UyslAYc2IzArOPwfXB48eTehoYaESrgzYVXSJetis2+2Jd8AgAsh1LF6Ayh67LhIAdigZPHR/9SxUYh4=</ds:SignatureValue>
          <ds:KeyInfo>
            <wsse:SecurityTokenReference xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity- tility-1.0.xsd" wsu:Id="XWSSGID-1172790287191-1130524177">
              <wsse:Reference URI="#XWSSGID-1172790286164-631000224" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3"/>
            </wsse:SecurityTokenReference>
          </ds:KeyInfo>
        </ds:Signature>
        <wsu:Timestamp xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"wsu:Id="XWSSGID-11727902873271435349604">
          <wsu:Created>2007-03-01T23:04:47Z</wsu:Created>
          <wsu:Expires>2007-03-01T23:04:52Z</wsu:Expires>
        </wsu:Timestamp>
    </wsse:Security>
  </SOAP-ENV:Header>
  <SOAP-ENV:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="XWSSGID-1172790287316421676595">
    <ekmi:KCPRequest xmlns:ekmi="http://docs.oasis-open.org/ekmi/2008/01"/>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

SKSML Protocol

- Key Cache Policy Response

```
<ekmi:KeyCachePolicy xmlns:ekmi='http://docs.oasis-open.org/ekmi/2008/01'>
    <ekmi:KCPID>10514-17</ekmi:KCPID>
    <ekmi:PolicyName>Corporate Laptop Symmetric Key Caching Policy</ekmi:PolicyName>
    <ekmi:Description>
        This policy defines how company-issued laptops will manage symmetric keys
        used for file/disk encryption in their local cache.
    </ekmi:Description>
    <ekmi:StartDate>2008-01-01T00:00:01.0</ekmi:StartDate>
    <ekmi:EndDate>2008-12-31T24:00:00.0</ekmi:EndDate>
    <ekmi:PolicyCheckInterval>86400</ekmi:PolicyCheckInterval>
    <ekmi:Status>Active</ekmi:Status>
    <ekmi:NewKeysCacheDetail>
        <ekmi:MaximumKeys>3</ekmi:MaximumKeys>
        <ekmi:MaximumDuration>7776000</ekmi:MaximumDuration>
    </ekmi:NewKeysCacheDetail>
    <ekmi:UsedKeysCacheDetail>
        <ekmi:MaximumKeys>3</ekmi:MaximumKeys>
        <ekmi:MaximumDuration>7776000</ekmi:MaximumDuration>
    </ekmi:UsedKeysCacheDetail>
</ekmi:KeyCachePolicy>
```

SKSML Protocol

- SOAP Fault

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
   <SOAP-ENV:Header>
        ERROR: Other error reported; please review logs for details.  Server error message is: No authorization
        to request this key:10514-2-2; if you believe this response is an error, please contact your Security Officer
   </SOAP-ENV:Header>
   <SOAP-ENV:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
            wsu:Id="XWSSGID-1154644495295194261602 4">
        <SOAP-ENV:Fault>
             <faultcode xmlns:skf="http://www.strongauth.com/2006/01/symkey#SymkeyFault">
                  skf:SymkeyFault
             </faultcode>
             <faultstring>symkey.sks.msg.severe.0085</faultstring>
             <detail>
                  <EndEntity>
                       <EEID>10514-2</EEID>
                       <DN>O=StrongAuth Inc,CN=POS Register 222,UID=2</DN>
                       <Status>Active</Status>
                  </EndEntity>
                  <Request>
                       <RID>10514-3</RID>
                       <GKID>10514-2-2</GKID>
                       <Timestamp>2006-08-03 15:34:55.0</Timestamp>
                       <Disposition>Failed</Disposition>
                  </Request>
             </detail>
        </SOAP-ENV:Fault>
    </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

StrongKey® Securing the Core

SKMS Security

- Every request/response is digitally signed
- Every response is encrypted
- Every object in database is digitally signed
- All symmetric keys in cache are digitally signed and encrypted
- All crypto code is abstracted
  - FIPS 140-2 devices are easily integrated
- Administration console does not use UserID and Passwords; only SSL Client Auth.

Conclusion

- Questions?
- Contact Information
  - www.strongauth.com
  - www.strongkey.org
  - info@strongauth.com
  - (408) 331-2000