

Securing the Core with an Enterprise Key Management Infrastructure (EKMI)

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

- What is an EKMI?
- What are its components?
- How do you build one?
- How do you secure one?
- What is the SKSMS Protocol?

An **Enterprise Key Management Infrastructure** is:

“A collection of technology, policies and procedures for managing the life-cycle of **all** cryptographic keys in the enterprise.”

- PKI

“A collection of technology, policies and procedures for managing the life-cycle of **asymmetric** cryptographic keys in the enterprise.”

- SKMS

“A collection of technology, policies and procedures for managing the life-cycle of **symmetric** cryptographic keys in the enterprise.”



- Public Key Infrastructure (PKI)
- Symmetric Key Management System (SKMS)

The problem



- Define Policy
- Generate
- Encrypt
- Decrypt
- Escrow
- Authorize
- Recover
- Destroy
- Audit



- Define Policy
- Generate
- Encrypt
- Decrypt
- Escrow
- Authorize
- Recover
- Destroy
- Audit



- Define Policy
- Generate
- Encrypt
- Decrypt
- Escrow
- Authorize
- Recover
- Destroy
- Audit



- Define Policy
- Generate
- Encrypt
- Decrypt
- Escrow
- Authorize
- Recover
- Destroy
- Audit

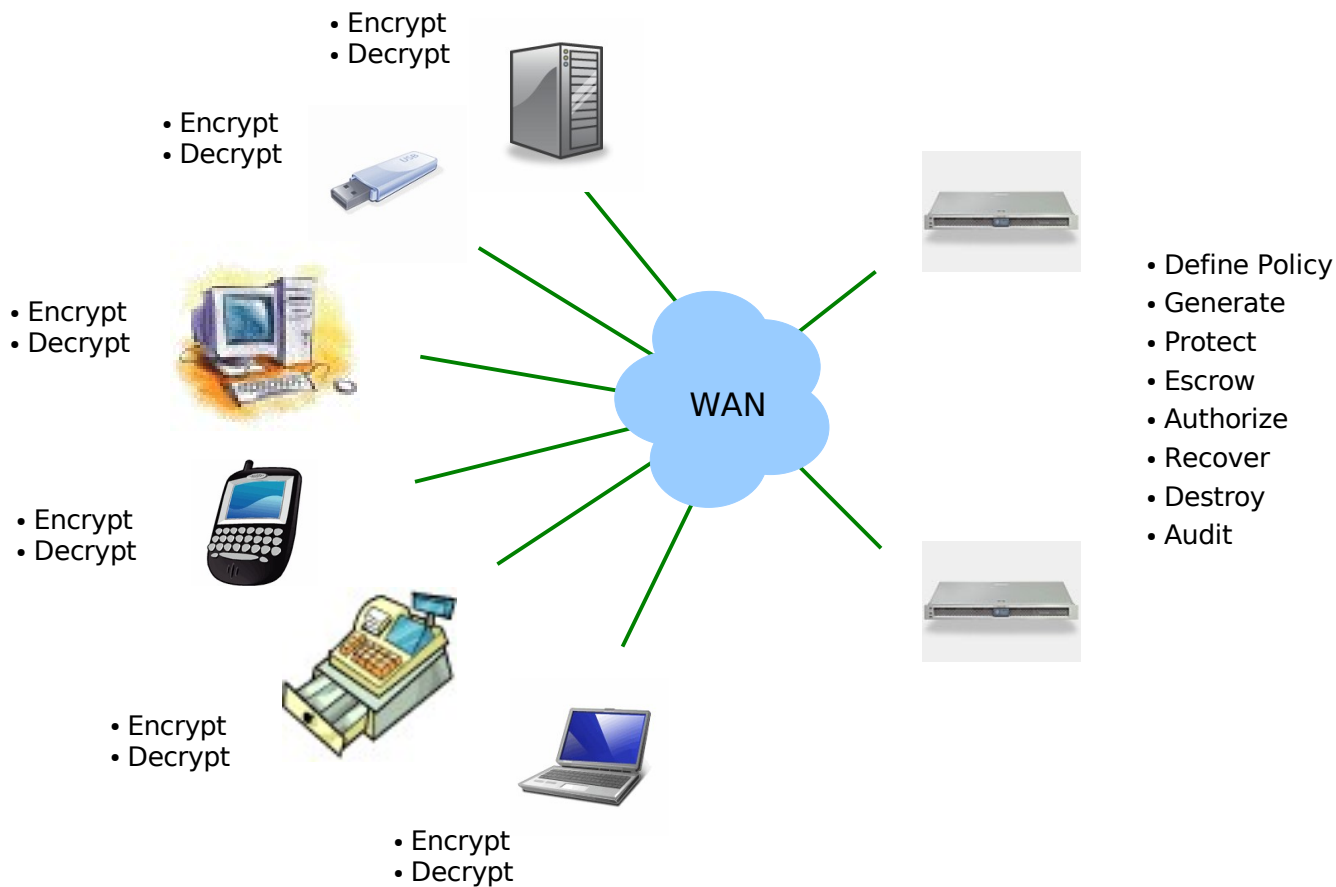


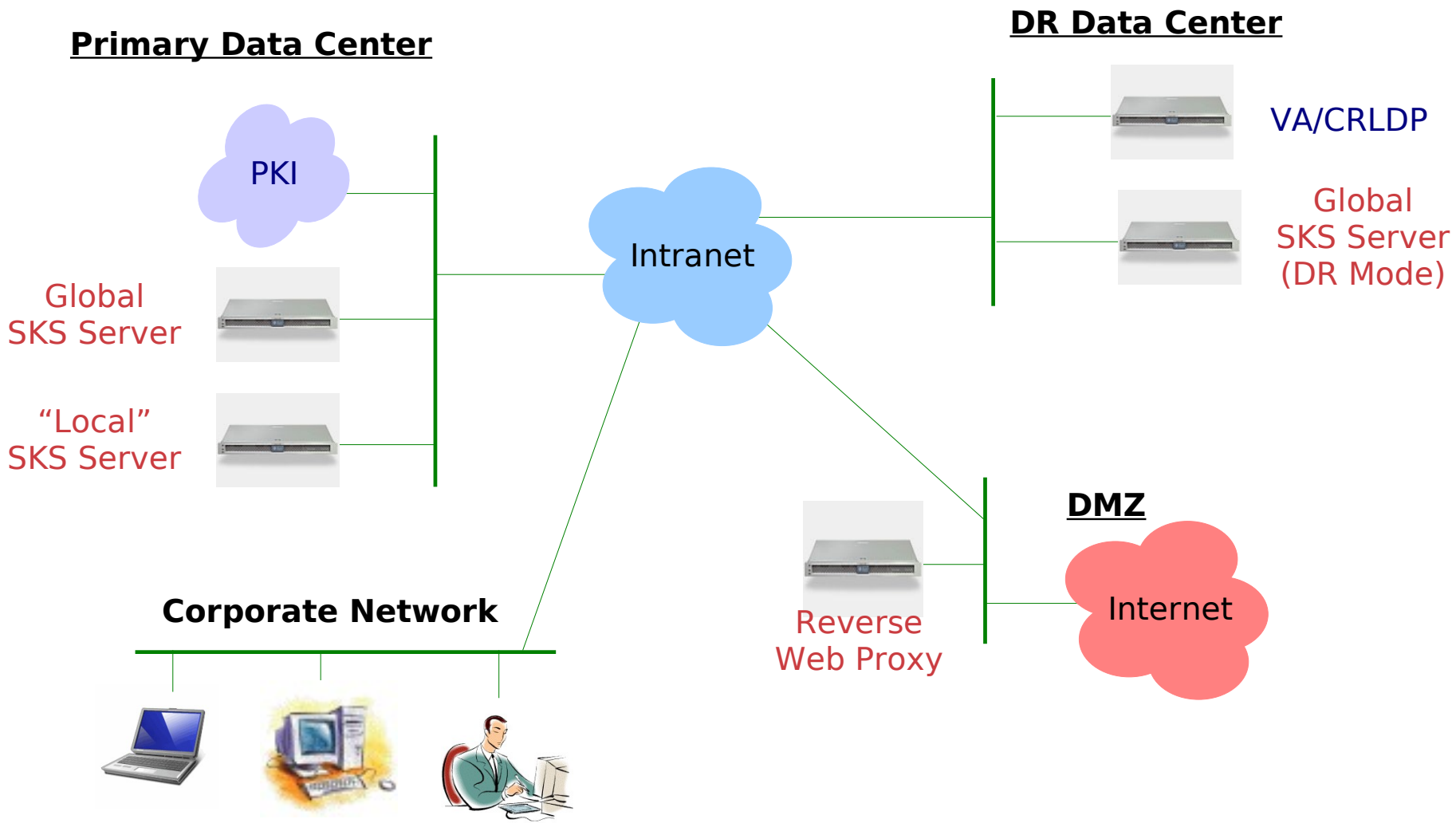
- Define Policy
- Generate
- Encrypt
- Decrypt
- Escrow
- Authorize
- Recover
- Destroy
- Audit



- Define Policy
- Generate
- Encrypt
- Decrypt
- Escrow
- Authorize
- Recover
- Destroy
- Audit

.....and on and on



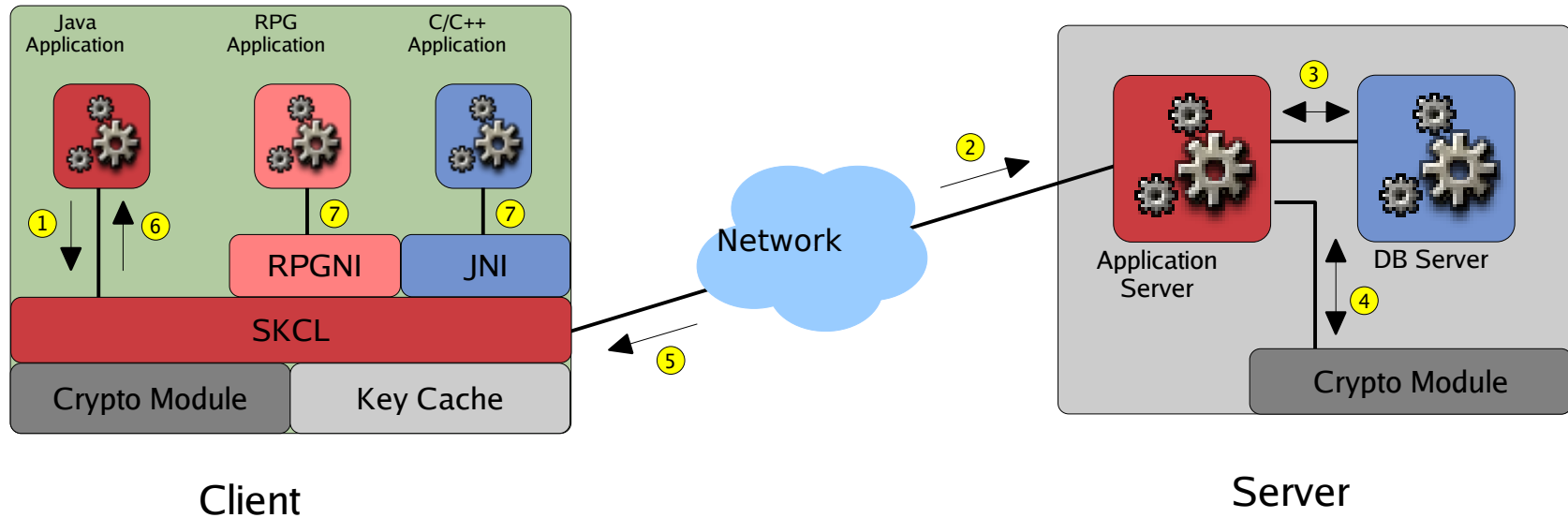


- One per enterprise
- Define all SKMS objects here:
 - Clients, Servers, Client Groups, Key Groups, Key Use Policies, Key Cache Policies, Grants
- DR Mode GSKS server is identical but Read-Only*
- HSM critical to security of server

- Any number per enterprise, as needed
 - One per continent recommended for global enterprises
- Configured to replicate to GSKS*
- HSM critical to security of server

- Any number per enterprise
- Maintains a list of SKS servers to get KM services from:
 - 1) Nearest SKS server on network
 - 2) GSKS Server
 - 3) GSKS DR-Mode Server
- HSM, smartcard token or TPM chip **strongly recommended** for security

- Database servers
- Web Application servers
- Network File servers
- Desktops/Laptops
- Automated Teller Machines (ATM)
- Point-of-Sale (POS) Registers
- Personal Digital Assistant (PDA)
- Smart mobile devices: Banking, Healthcare



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

- 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.

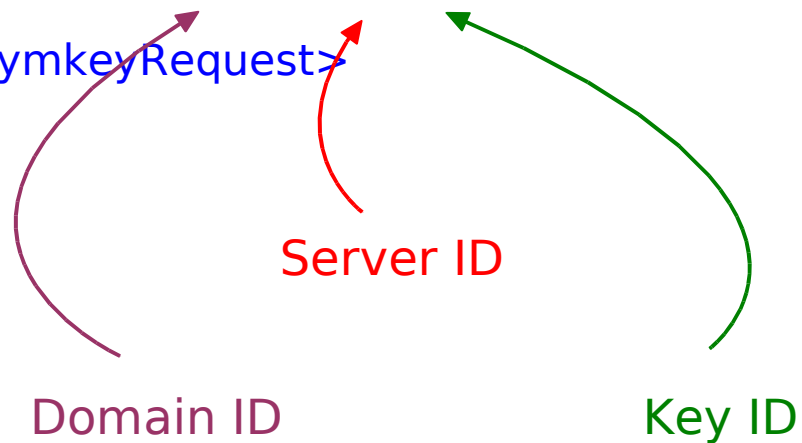
- Symmetric Key Services Markup Language
- Donated to OASIS on royalty-free basis by StrongAuth, Inc.
- Currently a TC DRAFT; anticipated standard in Summer 2008
- Two (2) Request types: Key and CachePolicy
- Three (3) Response types: Key, CachePolicy and Fault

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>
```

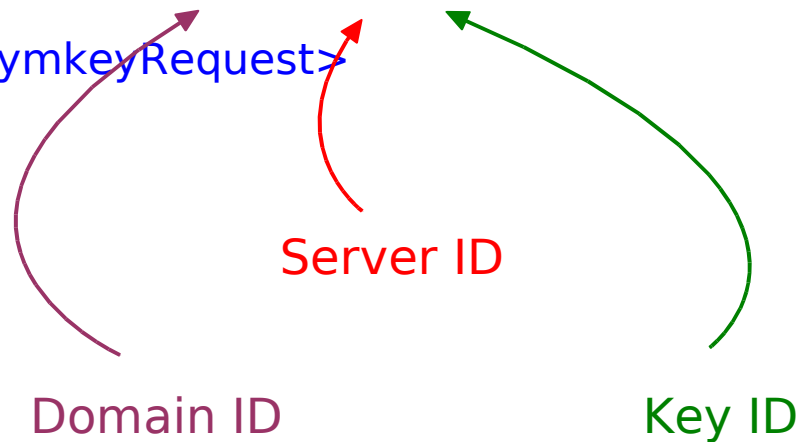


Request for an existing Symmetric Key

```
ekmi:SymkeyRequest xmlns:ekmi="http://docs.oasis-open.org/ekmi/2008/01">
```

```
<ekmi:GKID>10514-4-312</ekmi:GKID>
```

```
</ekmi:SymkeyRequest>
```



Request for a new Symmetric Key of 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>
```

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>
```

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>
```

Successful 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>
```

Successful 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>
```

Failed 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>
```

Failed 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:SymkeyError> ..... </ekmi:SymkeyError>
  <ekmi:SymkeyError> ..... </ekmi:SymkeyError>
</ekmi:SymkeyResponse>
```

Mixed 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>
```

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>
```

```
        huUYJMtaGHtXuLIWtx27STRcRplsY=
```

```
      </xenc:CipherValue>
```

```
    </xenc:CipherData>
```

```
  </ekmi:Symkey>
```

```
</ekmi:SymkeyResponse>
```

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>
```

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>

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>
```

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>Yjv9h5FDqUiQXG0ca8EU871zBoXBjDXmINxTux+mt1tXuLIWtx27STRcRplsY=</xenc:CipherValue>
    </xenc:CipherData>
  </ekmi:Symkey>
</ekmi:SymkeyResponse>
```

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>
```

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>
```

Request for a Key Caching Policy

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


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>
```

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-11546444952951942616024">
    <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>
```

- Technical Committee with 4 goals:
 1. Standardize Symmetric Key Services Markup Language (SKSML)
 2. Create Implementation & Operations Guidelines
 3. Create Audit Guidelines
 4. Create interoperability test-suite for SKSML

- FundServ* (Canada)
- MISMO
- NuParadigm Government Systems
- PA Consulting (UK)
- PrimeKey (Sweden)
- Red Hat
- StrongAuth*
- US Dept. of Defense
- Visa*
- Wave Systems
- Wells Fargo
- OS Software company
- Database SW company
- Storage/Security SW company
- Storage/Security SW company
- Govt. Agency (New Zealand)
- Individuals representing Audit and Security backgrounds*

* Founder Members

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