

# IEEE Key Management Summit 2008

---

## **OASIS Enterprise Key Management Infrastructure (EKMI)**

**Version 1.3**

**Arshad Noor  
StrongAuth, Inc.**

---

# Background

- 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

# OASIS EKMI TC Members

---

- ARX
- CA
- 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

# The current problem



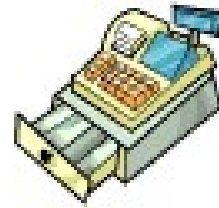
- Define Policy
- Generate
- Encrypt
- Decrypt
- Escrow
- Authorize
- Recover
- Destroy
- Audit



- 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



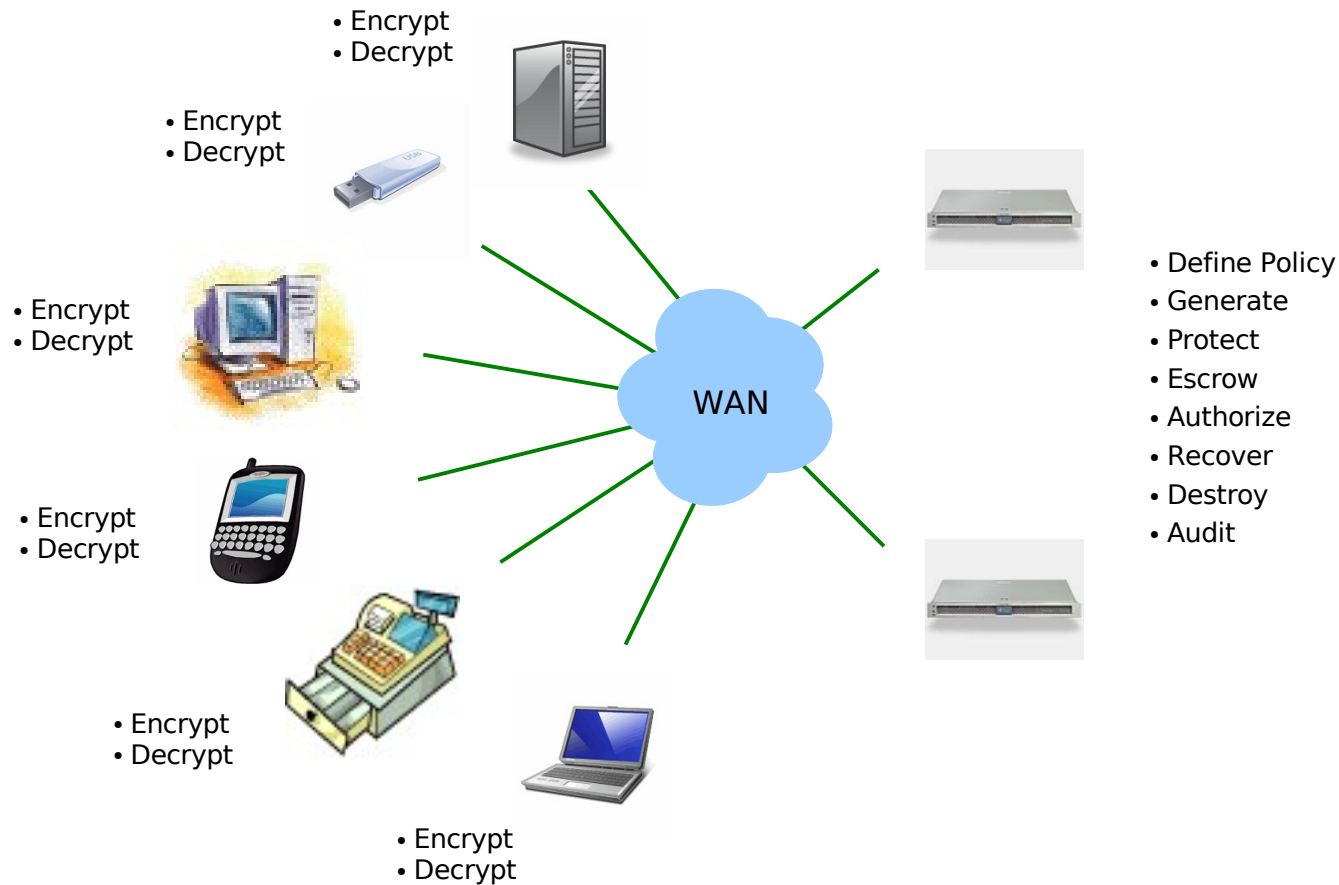
- Define Policy
- Generate
- Encrypt
- Decrypt
- Escrow
- Authorize
- Recover
- Destroy
- Audit



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

.....and on and on

# Ideally...



---

# **EKMI and its Components**

# What is an EKMI?

---

- 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.”

# EKMI Components

---

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



# What is an EKMI?

---

- PKI

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

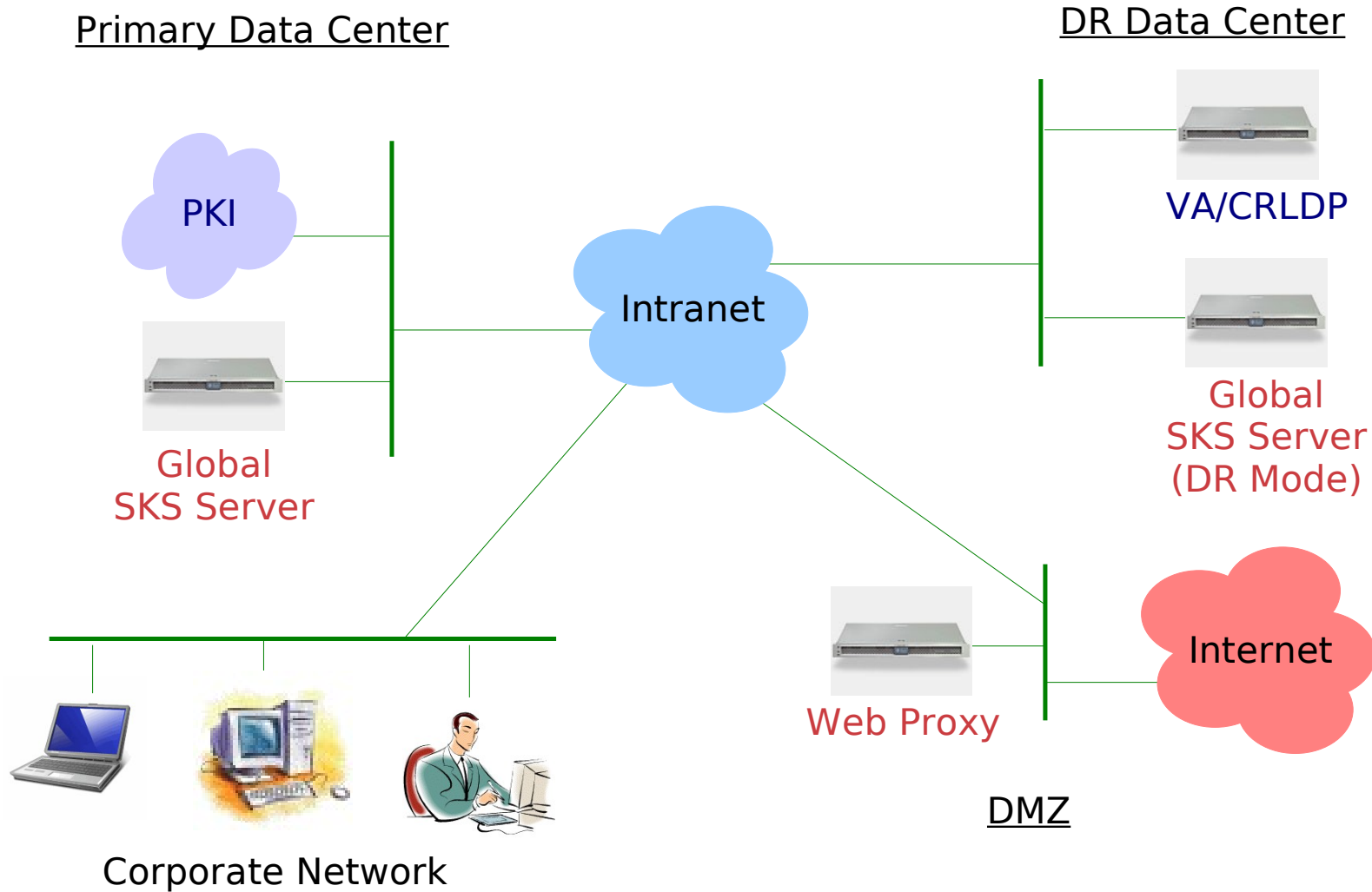
- SKMS

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

---

# **Symmetric Key Management System (SKMS)**

# Typical SKMS



# Global SKS Server

---

- 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\*
- CPU-intensive; quad-core recommended
- HSM critical to security of server

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

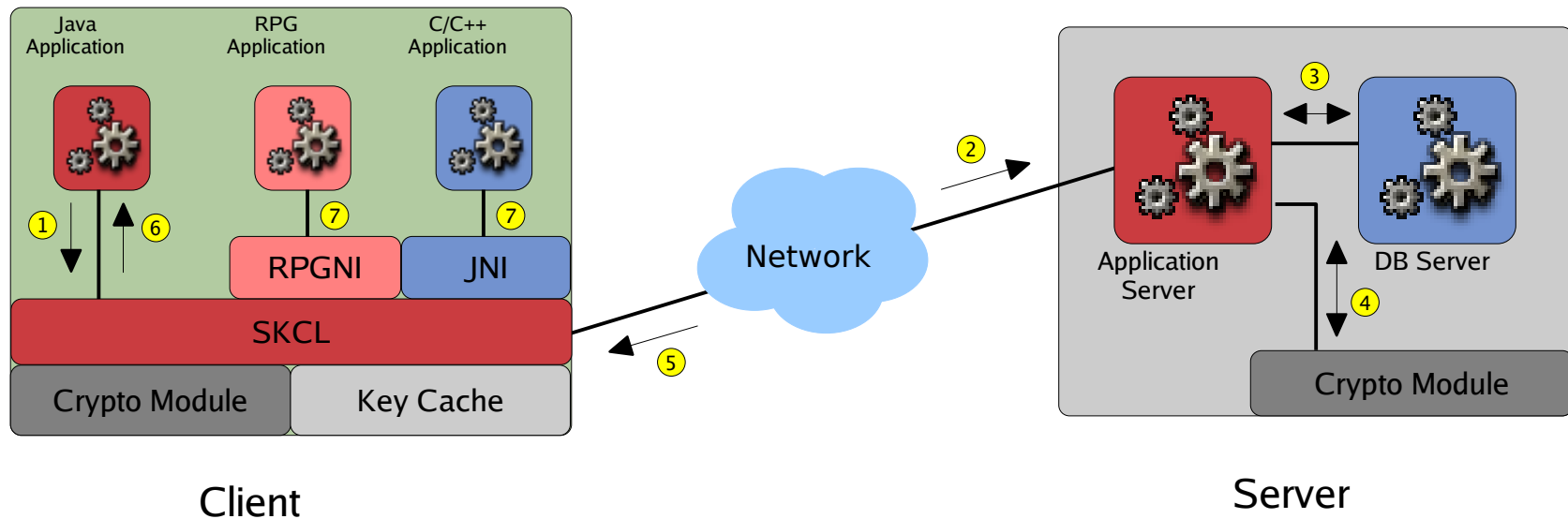
- Any number per enterprise
- Maintains a list of SKS servers to get KM services from:
  - 1) Nearest SKS server on network
  - 2) GSKS Server
  - 3) GSKS DR-Mode Server
- Smartcard token or TPM chip highly recommended for security

# SKMS Client Examples

---

- ERP / CRM Application 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

# 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 6; anticipated standard in December 2008
- Two (2) Request types
- Three (3) Response types

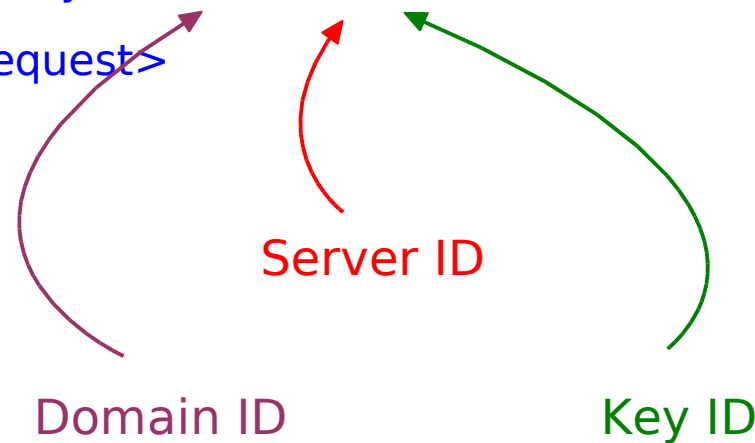
# SKSML Request

- Request for a new Symmetric Key

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

```
  <ekmi:GlobalKeyID>10514-0-0</ekmi:GlobalKeyID>
```

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



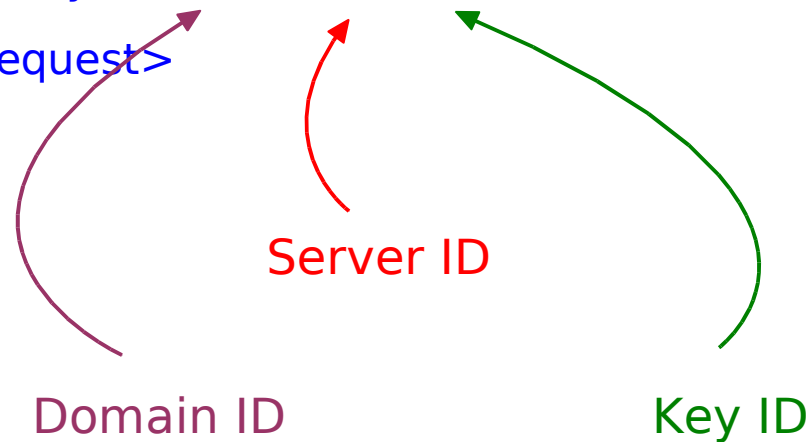
# SKSML Request

- Request for an existing Symmetric Key

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

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

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



# SKSML Request

- Request for a new Symmetric Key of a specific KeyClass

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

# SKSML Request

- Request for many new Symmetric Keys of specific KeyClasses

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

- Request for many existing Symmetric Keys

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

# SKSML Request

- Request for many Symmetric Keys of a specific KeyClass

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

# SKSML Request

- Request for many Symmetric Keys of a default KeyClass

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

# SKSML Response

---

- 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 Response

- 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 Error

- Failed Symmetric Key Response for a single key request

```
<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 Symmetric Key Response for multiple key requests

```
<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 Response/Error

- 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>
```

# 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:GlobalKeyID>10514-1-287</ekmi:GlobalKeyID>
```

```
    <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:KeyUsePolicyID>10514-4</ekmi:KeyUsePolicyID>

<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:PermittedDays> ..... </ekmi:PermittedDays>

<ekmi:PermittedDuration> ..... </ekmi:PermittedDuration>

<ekmi:PermittedLevels> ..... </ekmi:PermittedLevels>

<ekmi:PermittedLocations> ..... </ekmi:PermittedLocations>

<ekmi:PermittedNumberOfTransactions>

.....

</ekmi:PermittedNumberOfTransactions>

<ekmi:PermittedTimes> ..... </ekmi:PermittedTimes>

<ekmi:PermittedUses> ..... </ekmi:PermittedUses>

</ekmi:Permissions>

# PermittedApplications

<ekmi:Permissions>

<ekmi:PermittedApplications ekmi:any="false">

<ekmi:PermittedApplication>

<ekmi:ApplicationID>10514-23</ekmi:ID>

<ekmi:ApplicationName>Payroll Application</ekmi:ApplicationName>

<ekmi:Version>1.0</ekmi:Version>

<ekmi:DigestAlgorithm>

<http://www.w3.org/2000/09/xmlsig#sha1>

</ekmi:DigestAlgorithm>

<ekmi:DigestValue>NIG4bKkt4cziEqFFuOoBTM81efU=</ekmi:DigestValue>

</ekmi:PermittedApplication>

</ekmi:PermittedApplications>

<ekmi:PermittedDates ekmi:any="true" xsi:nil="true"/>

<ekmi:PermittedDays ekmi:any="true" xsi:nil="true"/>

<ekmi:PermittedDuration ekmi:any="true" xsi:nil="true"/>

<ekmi:PermittedLevels ekmi:any="true" xsi:nil="true"/>

<ekmi:PermittedLocations ekmi:any="true" xsi:nil="true"/>

<ekmi:PermittedNumberOfTransactions ekmi:any="true" xsi:nil="true"/>

<ekmi:PermittedTimes ekmi:any="true" xsi:nil="true"/>

<ekmi:PermittedUses ekmi:any="true" xsi:nil="true"/>

</ekmi:Permissions>

# PermittedDates

```
<ekmi:Permissions>
```

```
  <ekmi:PermittedApplications ekmi:any="true" xsi:nil="true"/>
```

```
  <ekmi:PermittedDates ekmi:any="false">
```

```
    <ekmi:PermittedDate>
```

```
      <ekmi:StartDate>2008-01-01</ekmi:StartDate>
```

```
      <ekmi:EndDate>2008-07-03</ekmi:EndDate>
```

```
    </ekmi:PermittedDate>
```

```
    <ekmi:PermittedDate>
```

```
      <ekmi:StartDate>2008-07-07</ekmi:StartDate>
```

```
      <ekmi:EndDate>2008-12-31</ekmi:EndDate>
```

```
    </ekmi:PermittedDate>
```

```
  </ekmi:PermittedDates>
```

```
  <ekmi:PermittedDays ekmi:any="true" xsi:nil="true"/>
```

```
  <ekmi:PermittedDuration ekmi:any="true" xsi:nil="true"/>
```

```
  <ekmi:PermittedLevels ekmi:any="true" xsi:nil="true"/>
```

```
  <ekmi:PermittedLocations ekmi:any="true" xsi:nil="true"/>
```

```
  <ekmi:PermittedNumberOfTransactions ekmi:any="true" xsi:nil="true"/>
```

```
  <ekmi:PermittedTimes ekmi:any="true" xsi:nil="true"/>
```

```
  <ekmi:PermittedUses ekmi:any="true" xsi:nil="true"/>
```

```
</ekmi:Permissions>
```

# PermittedDays

```
<ekmi:Permissions>
```

```
  <ekmi:PermittedApplications ekmi:any="true" xsi:nil="true"/>
```

```
  <ekmi:PermittedDates ekmi:any="true" xsi:nil="true"/>
```

```
  <ekmi:PermittedDays ekmi:any="false">
```

```
    <ekmi:PermittedDay>Weekday</ekmi:PermittedDay>
```

```
  </ekmi:PermittedDays>
```

```
  <ekmi:PermittedDuration ekmi:any="true" xsi:nil="true"/>
```

```
  <ekmi:PermittedLevels ekmi:any="true" xsi:nil="true"/>
```

```
  <ekmi:PermittedLocations ekmi:any="true" xsi:nil="true"/>
```

```
  <ekmi:PermittedNumberOfTransactions ekmi:any="true" xsi:nil="true"/>
```

```
  <ekmi:PermittedTimes ekmi:any="true" xsi:nil="true"/>
```

```
  <ekmi:PermittedUses ekmi:any="true" xsi:nil="true"/>
```

```
</ekmi:Permissions>
```

# PermittedDuration

---

<ekmi:Permissions>

<ekmi:PermittedApplications ekmi:any="true" xsi:nil="true"/>

<ekmi:PermittedDates ekmi:any="true" xsi:nil="true"/>

<ekmi:PermittedDays ekmi:any="true" xsi:nil="true"/>

<ekmi:PermittedDuration ekmi:any="false">

300

</ekmi:PermittedDuration>

<ekmi:PermittedLevels ekmi:any="true" xsi:nil="true"/>

<ekmi:PermittedLocations ekmi:any="true" xsi:nil="true"/>

<ekmi:PermittedNumberOfTransactions ekmi:any="true" xsi:nil="true"/>

<ekmi:PermittedTimes ekmi:any="true" xsi:nil="true"/>

<ekmi:PermittedUses ekmi:any="true" xsi:nil="true"/>

</ekmi:Permissions>

# PermittedLevels

<ekmi:Permissions>

```
<ekmi:PermittedApplications ekmi:any="true" xsi:nil="true"/>
<ekmi:PermittedDates ekmi:any="true" xsi:nil="true"/>
<ekmi:PermittedDays ekmi:any="true" xsi:nil="true"/>
<ekmi:PermittedDuration ekmi:any="true" xsi:nil="true"/>
<ekmi:PermittedLevels ekmi:any="false">
  <ekmi:PermittedLevel>Secret</ekmi:PermittedLevel>
  <ekmi:PermittedLevel>Top-Secret<ekmi:PermittedLevel>
</ekmi:PermittedLevels>
<ekmi:PermittedLocations ekmi:any="true" xsi:nil="true"/>
<ekmi:PermittedNumberOfTransactions ekmi:any="true" xsi:nil="true"/>
<ekmi:PermittedTimes ekmi:any="true" xsi:nil="true"/>
<ekmi:PermittedUses ekmi:any="true" xsi:nil="true"/>
```

</ekmi:Permissions>

# PermittedLocations

<ekmi:Permissions>

```
<ekmi:PermittedApplications ekmi:any="true" xsi:nil="true"/>
<ekmi:PermittedDates ekmi:any="true" xsi:nil="true"/>
<ekmi:PermittedDays ekmi:any="true" xsi:nil="true"/>
<ekmi:PermittedDuration ekmi:any="true" xsi:nil="true"/>
<ekmi:PermittedLevels ekmi:any="true" xsi:nil="true"/>
<ekmi:PermittedLocations ekmi:any="false">
  <ekmi:PermittedLocation>
    <ekmi:LocationName>Primary Data Center</ekmi:LocationName>
    <ekmi:Latitude>37.385653</ekmi:Latitude>
    <ekmi:Longitude>-121.993192</ekmi:Longitude>
  </ekmi:PermittedLocation>
  <ekmi:PermittedLocation>
    <ekmi:LocationName>DR Data Center</ekmi:LocationName>
    <ekmi:Latitude>68.845901</ekmi:Latitude>
    <ekmi:Longitude>11.393385</ekmi:Longitude>
  </ekmi:PermittedLocation>
</ekmi:PermittedLocations>
<ekmi:PermittedNumberOfTransactions ekmi:any="true" xsi:nil="true"/>
<ekmi:PermittedTimes ekmi:any="true" xsi:nil="true"/>
<ekmi:PermittedUses ekmi:any="true" xsi:nil="true"/>
```

</ekmi:Permissions>

# PermittedNumberOfTransactions

---

<ekmi:Permissions>

```
<ekmi:PermittedApplications ekmi:any="true" xsi:nil="true"/>
<ekmi:PermittedDates ekmi:any="true" xsi:nil="true"/>
<ekmi:PermittedDays ekmi:any="true" xsi:nil="true"/>
<ekmi:PermittedDuration ekmi:any="true" xsi:nil="true"/>
<ekmi:PermittedLevels ekmi:any="true" xsi:nil="true"/>
<ekmi:PermittedLocations ekmi:any="true" xsi:nil="true"/>
<ekmi:PermittedNumberOfTransactions ekmi:any="false">
    100
</ekmi:PermittedNumberOfTransactions>
<ekmi:PermittedTimes ekmi:any="true" xsi:nil="true"/>
<ekmi:PermittedUses ekmi:any="true" xsi:nil="true"/>
```

</ekmi:Permissions>

# PermittedTimes

<ekmi:Permissions>

```
<ekmi:PermittedApplications ekmi:any="true" xsi:nil="true"/>
<ekmi:PermittedDates ekmi:any="true" xsi:nil="true"/>
<ekmi:PermittedDays ekmi:any="true" xsi:nil="true"/>
<ekmi:PermittedDuration ekmi:any="true" xsi:nil="true"/>
<ekmi:PermittedLevels ekmi:any="true" xsi:nil="true"/>
<ekmi:PermittedLocations ekmi:any="true" xsi:nil="true"/>
<ekmi:PermittedNumberOfTransactions ekmi:any="true" xsi:nil="true"/>
<ekmi:PermittedTimes ekmi:any="false">
  <ekmi:PermittedTime>
    <ekmi:StartTime>08:00:00</ekmi:StartTime>
    <ekmi:EndTime>17:00:00</ekmi:EndTime>
  </ekmi:PermittedTime>
</ekmi:PermittedTimes>
<ekmi:PermittedUses ekmi:any="true" xsi:nil="true"/>
```

</ekmi:Permissions>

# PermittedUses

<ekmi:Permissions>

```
<ekmi:PermittedApplications ekmi:any="true" xsi:nil="true"/>
<ekmi:PermittedDates ekmi:any="true" xsi:nil="true"/>
<ekmi:PermittedDays ekmi:any="true" xsi:nil="true"/>
<ekmi:PermittedDuration ekmi:any="true" xsi:nil="true"/>
<ekmi:PermittedLevels ekmi:any="true" xsi:nil="true"/>
<ekmi:PermittedLocations ekmi:any="true" xsi:nil="true"/>
<ekmi:PermittedNumberOfTransactions ekmi:any="true" xsi:nil="true"/>
<ekmi:PermittedTimes ekmi:any="true" xsi:nil="true"/>
<ekmi:PermittedUses ekmi:any="false">
  <ekmi:PermittedUse>Laptop</ekmi:PermittedUse>
  <ekmi:PermittedUse>PDA</ekmi:PermittedUse>
  <ekmi:PermittedUse>Mobile Phone</ekmi:PermittedUse>
  <ekmi:PermittedUse>Tablet</ekmi:PermittedUse>
</ekmi:PermittedUses>
```

</ekmi:Permissions>

# KeyUsePolicy element

```
<ekmi:KeyUsePolicy>
  <ekmi:KeyUsePolicyID>10514-4</ekmi:KeyUsePolicyID>
  <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:any="false">
      <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:any="false">
      <ekmi:PermittedDate>
        <ekmi:StartDate>2008-01-01</ekmi:StartDate>
        <ekmi:EndDate>2008-12-31</ekmi:EndDate>
      </ekmi:PermittedDate>
    </ekmi:PermittedDates>
    <ekmi:PermittedDays ekmi:any="true" xsi:nil="true"/>
    <ekmi:PermittedDuration ekmi:any="true" xsi:nil="true"/>
    <ekmi:PermittedLevels ekmi:any="true" xsi:nil="true"/>
    <ekmi:PermittedLocations ekmi:any="true" xsi:nil="true"/>
    <ekmi:PermittedNumberOfTransactions ekmi:any="true" xsi:nil="true"/>
    <ekmi:PermittedTimes ekmi:any="true" xsi:nil="true"/>
    <ekmi:PermittedUses ekmi:any="true" xsi:nil="true"/>
  </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:GlobalKeyID>10514-1-235</ekmi:GlobalKeyID>
    <ekmi:KeyUsePolicy>
      <ekmi:KeyUsePolicyID>10514-4</ekmi:KeyUsePolicyID>
      <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:any="false">
          <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:any="false">
          <ekmi:PermittedDate>
            <ekmi:StartDate>2008-01-01</ekmi:StartDate>
            <ekmi:EndDate>2008-12-31</ekmi:EndDate>
          </ekmi:PermittedDate>
        </ekmi:PermittedDates>
        <ekmi:PermittedDays ekmi:any="true" xsi:nil="true"/>
        <ekmi:PermittedDuration ekmi:any="true" xsi:nil="true"/>
        <ekmi:PermittedLevels ekmi:any="true" xsi:nil="true"/>
        <ekmi:PermittedLocations ekmi:any="true" xsi:nil="true"/>
        <ekmi:PermittedNumberOfTransactions ekmi:any="true" xsi:nil="true"/>
        <ekmi:PermittedTimes ekmi:any="true" xsi:nil="true"/>
        <ekmi:PermittedUses ekmi:any="true" xsi:nil="true"/>
      </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:RequestedGlobalKeyID>
```

```
      10514-0-0
```

```
    </ekmi:RequestedGlobalKeyID>
```

```
    <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:RequestedGlobalKeyID>
```

```
      10514-2-2254
```

```
    </ekmi:RequestedGlobalKeyID>
```

```
    <ekmi:RequestedKeyClass>EHR-HOS</ekmi:RequestedKeyClass>
```

```
    <ekmi:ErrorCode>SKS-100004</ekmi:ErrorCode>
```

```
    <ekmi:ErrorMessage>Unauthorized request</ekmi:ErrorMessage>
```

```
  </ekmi:SymkeyError>
```

```
  <ekmi:SymkeyError>
```

```
    <ekmi:RequestedGlobalKeyID>
```

```
      10514-0-2254
```

```
    </ekmi:RequestedGlobalKeyID>
```

```
    <ekmi:RequestedKeyClass>EHR-PHY</ekmi:RequestedKeyClass>
```

```
    <ekmi:ErrorCode>SKS-100001</ekmi:ErrorCode>
```

```
    <ekmi:ErrorMessage>Invalid GKID</ekmi:ErrorMessage>
```

```
  </ekmi:SymkeyError>
```

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

# KeyCachePolicy Request

---

<ekmi:KeyCachePolicyRequest

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



# KeyCachePolicy element

```
<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>
```

# 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
  - All FIPS 140-2 devices are easily integrated
- SKMS certificates from “closed” PKI only

# Application encryption

---

- Why encrypt data at “Layer 7”?
  - Minimizes attack surface
  - Addresses the problem once and for all
  - Eliminates need for duplicated encryption
- Who is already encrypting at this layer?
  - PABP Application vendors
  - POS Application vendors

# Current Status

---

- SKSML v1.0 protocol is in “Public Review”
  - Closed on September 23, 2008
- TC addresses PR comments
  - Potential changes/clarifications to protocol
- Potential OASIS vote in Q4 2008
- Potential OASIS standard in Q1 2009

# Next Steps for TC

---

- Multiple efforts
  - Continue work on Implementation Guidelines
    - Document(s) to assist enterprises on how to build a secure EKMI
  - Start work on Audit Guidelines
    - Document(s) to assist IT Auditors on how to audit an EKMI, and what questions to ask about key-management systems
  - Start work on SKSML Conformance Tool

- SKSML Specification

- <http://www.oasis-open.org/committees/download.php/28725/SKSML-1.0-Specification-Normative-DRAFT6.0.pdf>

- SKSML XSD file and example messages

- <http://www.oasis-open.org/committees/download.php/28653/SKSML-DRAFT-6.0.zip>

- Tons of EKMI documents

- <http://www.oasis-open.org/committees/documents.php>

- ISSA Article

- [http://www.oasis-open.org/committees/download.php/22096/Noor\\_Symmetric%20Key%20Management%20Systems-1.pdf](http://www.oasis-open.org/committees/download.php/22096/Noor_Symmetric%20Key%20Management%20Systems-1.pdf)

- ACM Papers (older version of protocol)

- <http://middleware.internet2.edu/idtrust/2008/papers/07-noor-ekmi.pdf>

- Questions?
- Contact Information
  - [http://www.oasis-open.org/committees/tc\\_home.php?wg\\_abbrev=ekmi](http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ekmi)
  - [arshad.noor@strongauth.com](mailto:arshad.noor@strongauth.com)
  - (408) 331-2000