

StrongKey

The industry's first open-source SKMS

Arshad Noor
CTO, StrongAuth, Inc.

NIST Key Management Workshop 2009

For those viewing via webcast, please submit questions for this presentation to:

kmwquestions@nist.gov

Thank you.

- 8 year-old, private California company
- Enterprise Key Management
- PKI-based Identity Management
- Open-source key-management related products:
 - CSRTool
 - RSA/ECDSA key-pairs -> P10 -> P12
 - StrongKey
 - Symmetric Key Management System

The problem we solve



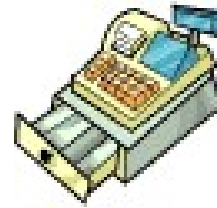
- Define Policy
- Generate
- Encrypt
- Decrypt
- Escrow
- Authorize
- Recover
- Destroy
- Audit



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



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



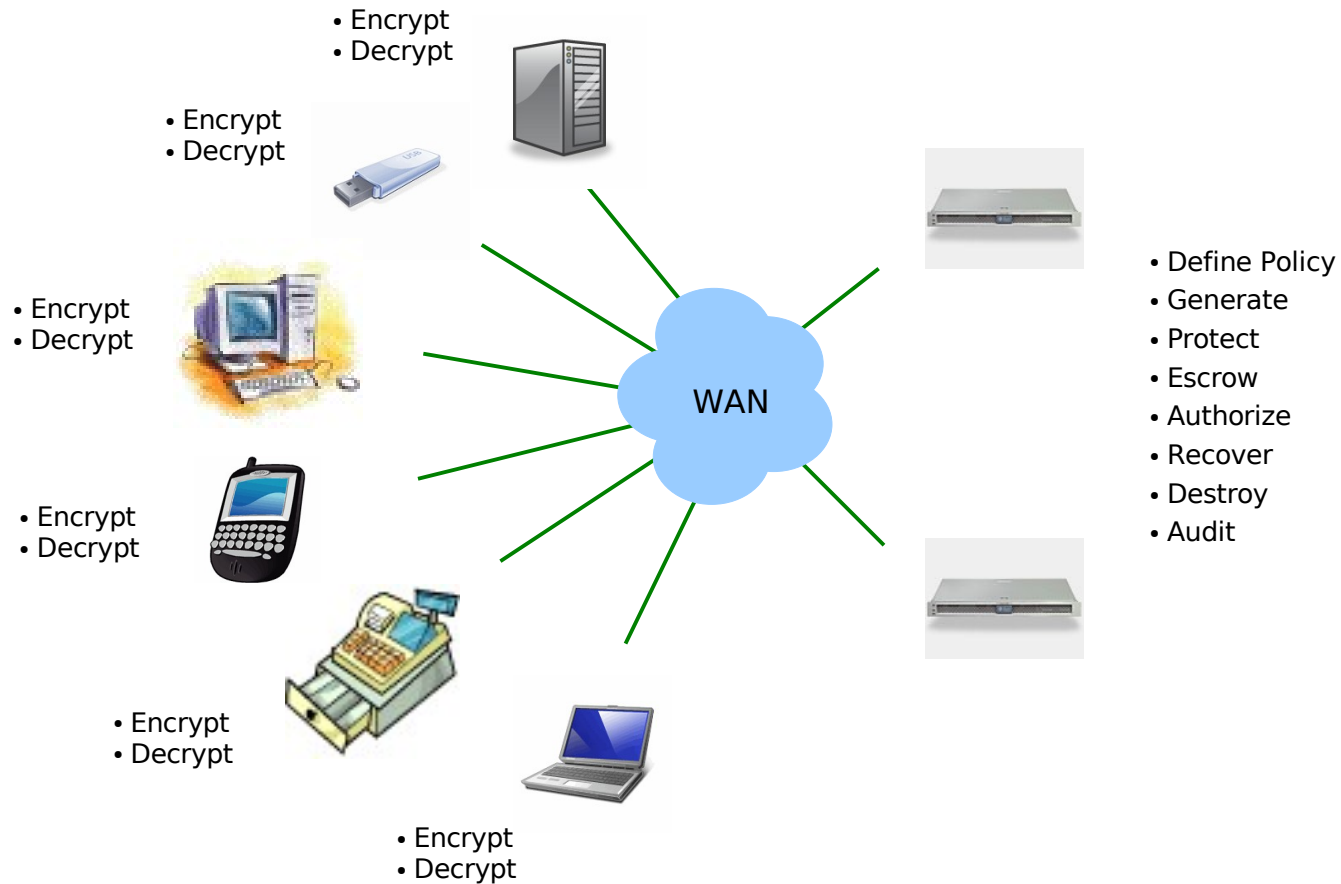
- Define Policy
- Generate
- Encrypt
- Decrypt
- Escrow
- Authorize
- Recover
- Destroy
- Audit



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



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



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

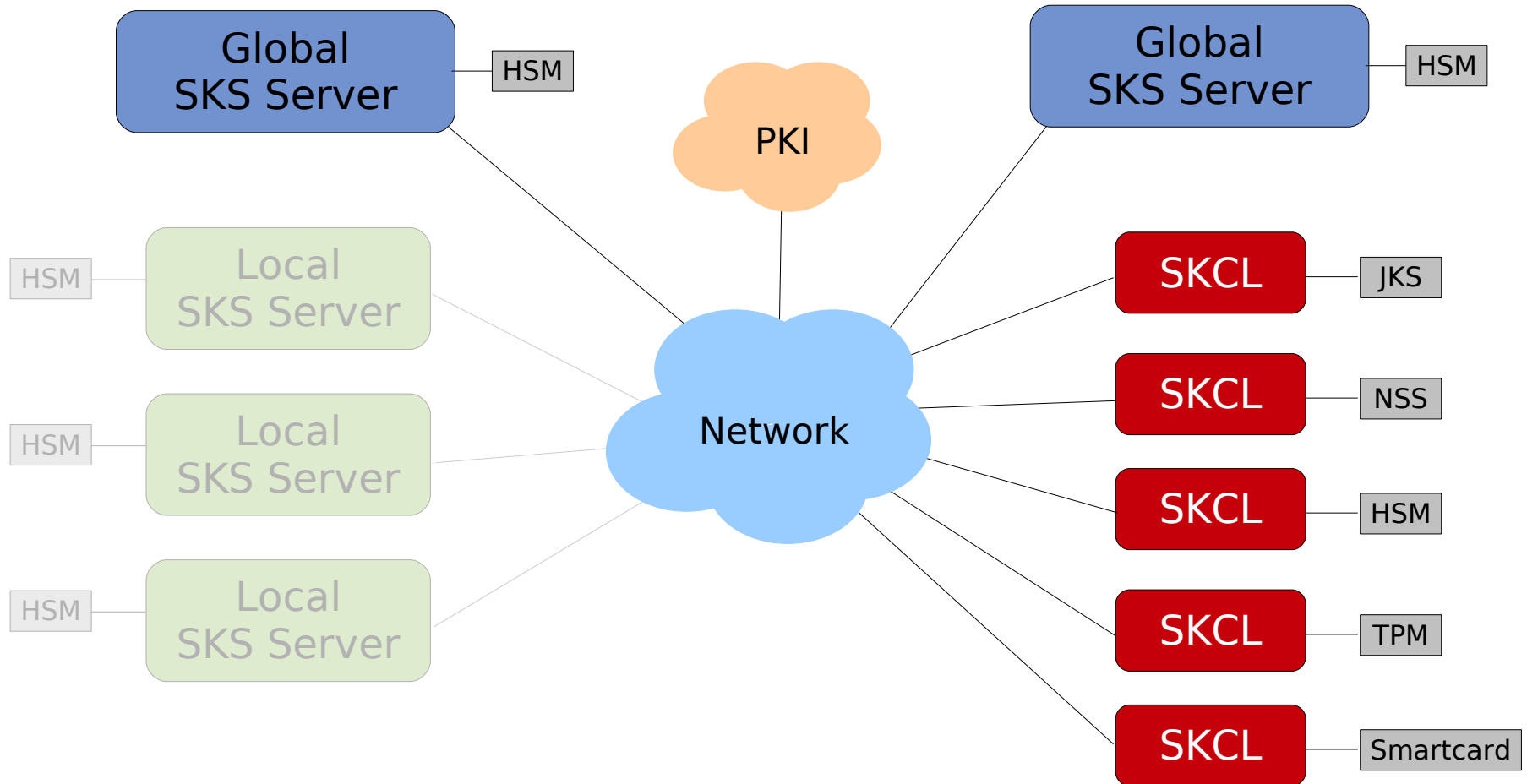
EKMI

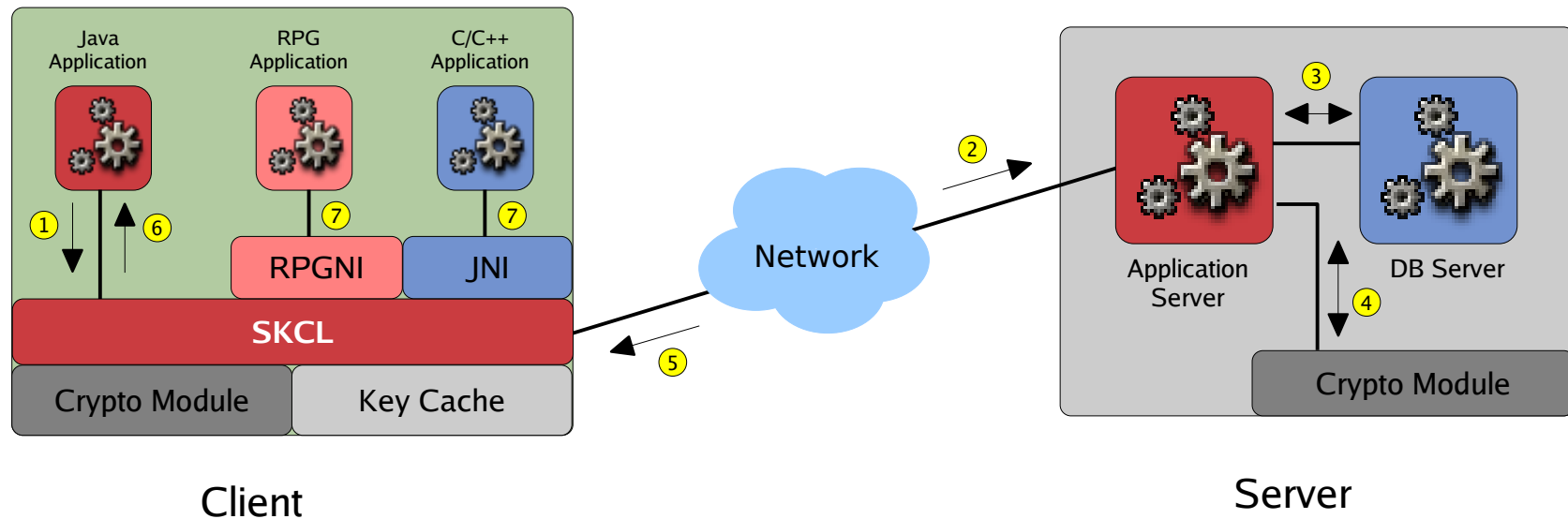
PKI

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.



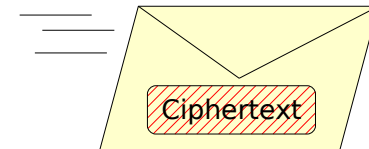
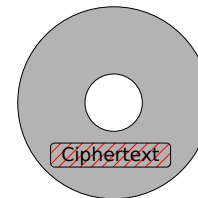
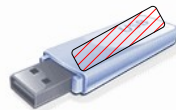
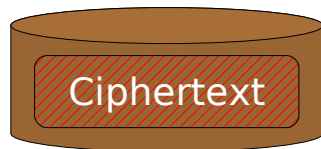
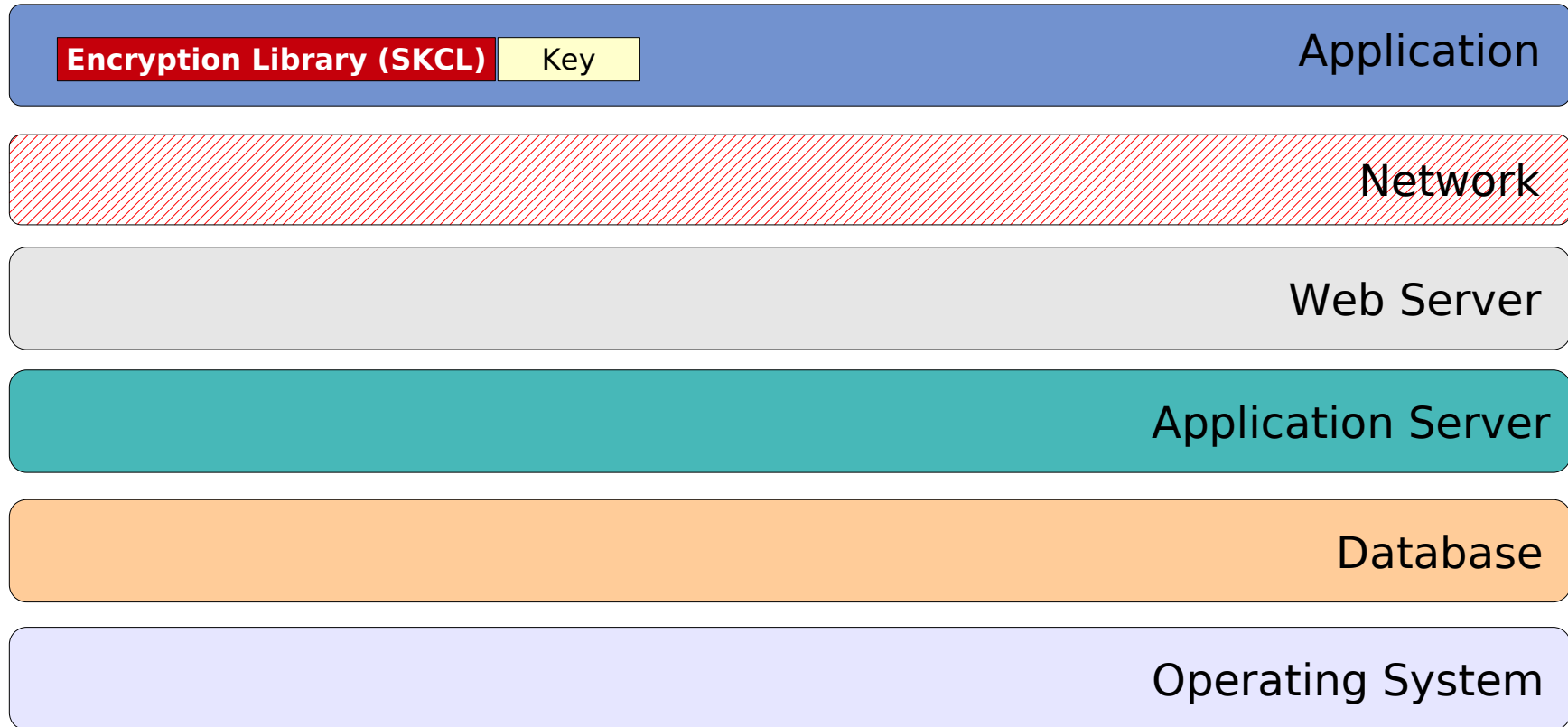


1. Client Application makes a request for a symmetric key
2. SKCL makes a digitally signed request to the SKS
3. SKS verifies SKCL request, generates, encrypts, digitally signs & escrows key in DB
4. Crypto HSM provides security for RSA Signing & Encryption keys of SKS
5. SKS responds to SKCL with signed 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

- public Symkey getSymkey (.....)
- public byte[] encryptToBytes (.....)
- public String encryptToXML (.....)
- public byte[] decryptBytes (.....)
- public byte[] decryptXML (.....)
- public String getSHA1 (.....)
- public String getSHA256 (.....)
- public String getSHA384 (.....)
- public String getSHA512 (.....)

- Every request/response is digitally signed
- Symmetric-key in response is always encrypted
- Every object in database is digitally-signed including audit trail
- Symmetric keys in cache are encrypted and digitally-signed
- Cryptographic code is abstracted
 - FIPS 140-2 devices are easily integrated
- SKMS certificates only from “closed” PKI
- Administration console does not use UserID and Passwords; only SSL Client Authentication

Where should one encrypt?



- Who is already encrypting at Layer 7?
 - PABP Application vendors
 - POS Application vendors
 - E-commerce platform vendors
 - E-commerce startups
 - Healthcare companies
 - VoIP service companies
 - Application Development teams who do not control the underlying IT infrastructure

- SKMS will do for symmetric key-management what DNS did for name-service management and DBMS did for data-management

DNS	DBMS	SKMS
Abstracts name-resolution outside application <i>(libresolv.so)</i>	Abstracts I/O outside application <i>(JDBC/ODBC libraries)</i>	Abstracts cryptography outside application <i>(skcl.jar)</i>
Abstracts name-space management outside application	Abstracts data-management outside application	Abstracts key-management outside application
Is an “invisible” infrastructure component	Is an “invisible” infrastructure component	Will become an “invisible” infrastructure component

- Open-source implementation available since 2006
 - www.strongkey.org
- 100% Java and supported on Linux, Windows, Solaris, OS/400 (client-only)
- C/C++ libraries available for Linux and Windows (Commercial license)
- Customers have built PHP and Ruby implementations of SKCL
- Support forum
 - www.strongauth.com/forum

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