

**OASIS**  **IDtrust**

**The OASIS IDtrust**  
**(Identity and Trusted Infrastructure)**  
**Member Section**

**John Sabo, CA, Inc.**

**For more information please see:**

**<http://www.oasis-idtrust.org/>**

**For more information related to 'Joining OASIS,' please see:**

**<http://www.oasis-open.org/join>**

# **OASIS** **IDtrust**

**OASIS provides a neutral setting where government agencies, companies, research institutes, and individuals work together to advance the use of trusted infrastructures.**

**The OASIS PKI Member Section has restructured as the OASIS Identity and Trusted Infrastructure (IDtrust) Member Section**

**The IDtrust MS has expanded its scope to encompass additional standards-based identity and trusted infrastructure technologies, policies, and practices.**

# Transformation

- Old PKI Forum
- Migration to OASIS PKI MS in November 2002
- One TC
- Focus on use of PKI and addressing barriers to deployment, not development of technical standards
- London OASIS Adoption Forum in November 2006
- Led to transformation into IDtrust MS in 2007

## Four Strategic Focus Areas:

- **Identity and Trusted Infrastructure components** such as cataloguing and carrying out studies and projects addressing technology-based Identity and Trust models and standards, including those that are PKI-based as well as those utilizing other security mechanisms; relevant protocols and standards; trust infrastructures in use; and costs, benefits and risk management issues
- **Identity and Trust Policies and Enforcement,** including policies and policy issues; policy mapping and standardization; assurance; technical validation mechanisms; and trust path building and validation

## Four Strategic Focus Areas:

- **Education and Outreach**: documenting trust use cases and business case scenarios, best practices and adoption reports and papers; organizing conferences and workshops; and establishing Web-based resources
- **Barriers and Emerging Issues associated with Identity and Trusted Infrastructures**, including data privacy issues; interoperability; cross border/organizational trust; outsourcing; cryptographic issues; application integration; and international issues

# PKI IDtrust Steering Committee

- Dr. Abbie Barbir, Nortel
- June Leung, FundSERV
- Arshad Noor, StrongAuth
- John Sabo, CA, Inc.
- Ann Terwilliger, Visa International

# Two Technical Committees

- Enterprise Key Management Infrastructure TC
  - Chairs:
    - Hans van Tilburg, Visa
    - Arshad Noor, StrongAuth
- PKI Adoption TC
  - Chair: Stephen Wilson, Lockstep LLC

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

# Business Motivation

- Regulatory Compliance
  - PCI-DSS, HIPAA, FISMA, SB-1386, etc.
- Avoiding fines
  - ChoicePoint \$15M, Nationwide \$2M
- Avoiding lawsuits – BofA, TJX
- Avoiding negative publicity
  - VA, IRS, TJX, E&Y, Citibank, BofA, WF, Ralph Lauren, UC, etc.

# e-Business/e-Government Challenges

- Sharing data while keeping it secure
  - Protected Critical Information Infrastructure (PCII) at the DHS
  - Medical, Taxpayer and Employee data
  - Other sensitive data
- Protecting data across the enterprise
  - Laptops, Desktops, Databases, PDAs, Servers, Storage devices, Partners, etc.

# Encryption Problem



- . Generate
- . Encrypt
- . Decrypt
- . Escrow
- . Authorize
- . Recover
- . Destroy

- . Generate
- . Encrypt
- . Decrypt
- . Escrow
- . Authorize
- . Recover
- . Destroy

- . Generate
- . Encrypt
- . Decrypt
- . Escrow
- . Authorize
- . Recover
- . Destroy

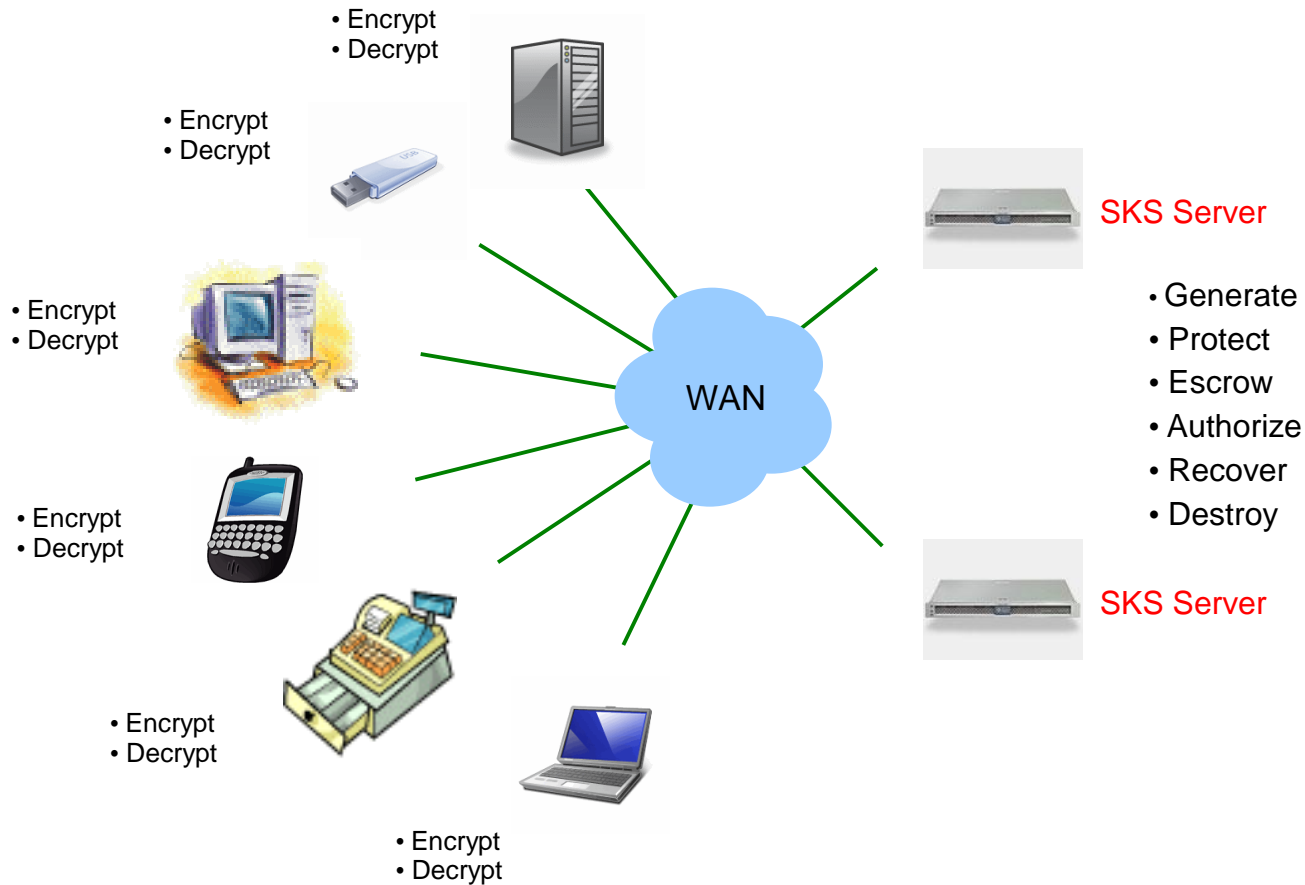
- . Generate
- . Encrypt
- . Decrypt
- . Escrow
- . Authorize
- . Recover
- . Destroy

- . Generate
- . Encrypt
- . Decrypt
- . Escrow
- . Authorize
- . Recover
- . Destroy

- . Generate
- . Encrypt
- . Decrypt
- . Escrow
- . Authorize
- . Recover
- . Destroy

.....and on and on

# Encryption Solution



# What is an EKMI?

- An **Enterprise Key Management Infrastructure** is:

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

## **EKMI Characteristics**

- A single place to define EKM policy
- A single place to manage all keys
- Standard protocols for EKM services
- Platform and Application-independent
- Scalable to service millions of clients
- Available even when network fails
- Extremely secure

# EKMI Components

- PKI
  - For digital certificate management; used for strong-authentication, and secure storage & transport of symmetric encryption keys
- Symmetric Key Management System
  - **SKS Server** for symmetric key management
  - **SKCL** for client interactions with SKS Server
- **EKMI = PKI + SKMS**

## **EKMI-TC Goals**

- Standardize on a **Symmetric Key Services Markup Language (SKSML)**
- Create **Implementation & Operations Guidelines**
- Create **Audit Guidelines**
- Create **Interoperability Test-Suite**

# **EKMI-TC**

## **Members/Observers**

- FundServ, PA Consulting, PrimeKey, Sterling Commerce, StrongAuth, US DoD, Visa International, Wave Systems
- Booz Allen Hamilton, EMC (RSA), Entrust, Mitre Corporation, Oracle, Sigaba, Symantec
- Individuals representing Audit and Security backgrounds

# **PKI Adoption TC**

## The PKI environment c. 2006

- PKI is resurgent, driven by applications needing signatures, esp. for paperless transacting
- Embedded keys & certs now commonplace
- Certificates now more about *relationships* between issuer & subject than “identity” of strangers
- In the midst of paradigm shift to identity plurality
- PKI becoming *application specific*, not general purpose

# Resurgent, Embedded Business-Driven PKI

- Closed/Vertical/Community based schemes
  - US PIV, Identrus, ICAO e-passports, CableLabs, Skype, BankID (Sweden)
- National ID smartcards with PKI
  - Hong Kong, Malaysia, Estonia, Belgium, Thailand ...
- Health smartcards with PKI
  - France, Germany, Taiwan, Italy, Austria, Australia ...
- Digital Credentials based on certificates
  - US Patent Office, Australia, France, Taiwan, ...

# PKI Adoption: Draft objectives

***Note: These are proposed objectives of the new PKI Adoption TC, yet to be ratified by the Committee.***

- Continue to overcome obstacles with *targeted practical initiatives that improve understanding of PKI*
- Re-vitalise and complete the Third International Survey
  - See [www.oasis-open.org](http://www.oasis-open.org) to download survey
- Canvass and disseminate PKI case studies
- Modernise the PKI message so it reflects real needs
- De-mystify legal, governance and interoperability issues
- Liaise more closely with other OASIS efforts

# **Study on the Use of PKI in OASIS Standards**

- Chet Ensign

# Overall project goals

- Document use & applicability of PKI for OASIS standards
- Identify expectations re authentication, integrity, confidentiality, etc.
- Identify assumptions re specific PKI methods/systems available
- List explicit standards referenced
- Identify possible issues & barriers
- Provide recommendations

# Status

- 2nd stage of study on use of PKI & related technologies in OASIS standards
- Study has 3 stages:
  - Update earlier 2003 report
  - Write new report on applicability, expectations and assumptions in OASIS TCs
  - Provide briefings to Member Section

## Approach to TC reviews

- Group TCs by importance of e-business services to TC success
- Interview 3 - 5 TC chairs or technical leads
- Review email archives & documents for discussion of:
  - Services, e.g. authentication, trust, encryption, digital signature
  - Specific standards, e.g. PKI, X.509, Kerberos, SAML
- Summarize trends, observations, themes & provide any recommendations

# Preliminary observations (1)

- Acronym “PKI” not broadly used. Instead, TCs discuss services (e.g. authentication, digital signature) or standards (e.g. X.509, Kerberos, SAML)
- Concepts and issues generally lumped under “Security”
- ‘End-user’ standards (e.g. Election & Voter Services, Court Filing) leave solution to implementation or reference other standards

## Preliminary observations (2)

- PKI perceived as big, expensive and complex relative to the issues users believe they need to solve. Also has reputation for interoperability problems.
- Many standards leave flexibility to implementation to ensure use.
- General sense that buyers do not understand issues, so do not call for PKI solutions.

# **TC PKI References**

## Closed TCs

- Since 09/03, 27 TCs closed
- 22 in original 2003 study; 5 were not
- Of 22, only 7 (about 1/3/) discussed PKI concepts or standards in archives or specifications
- Only 1 explicitly addressed authentication & security in its spec

## Closed TCs

- Published documents & discussion of PKI (4 TCs):
  - Business Transactions; Application Vulnerability Description Language; Directory Services ML; XML Common Biometric Format
- XML Common Biometric Format was only spec to address PKI in depth

## New TCs

- Since 09/03 draft, 37 TCs started
- 6 completed & covered above
- Of 31, 15 (about 1/2/) discuss PKI concepts or standards in archives or documents
- 7 explicitly address PKI concepts or issues in their work

# New TCs

- New TCs most actively addressing PKI issues, concepts and standards:
  - Enterprise Key Management Infrastructure
  - Framework for Web Services Implementation
  - International Health Continuum
  - WS Quality Model
  - WS Reliable Exchange
  - WS Secure Exchange
  - WS Transaction

## **Study Next Steps**

- Chet Ensign now completing interviews
- Analysis of findings
- Development of inferences and conclusions
- Final report and presentation to the MS within next two months

## **IDTrust Summary**

- Steering Committee developing new work plan for 2007 and 2008
- Many opportunities to get involved
- Invitation to join OASIS and participate in the MS and/or TCs
- Contact Dee Schur
  - [Dee.schur@oasis-open.org](mailto:Dee.schur@oasis-open.org)