

Enterprise Key Management Infrastructure (EKMI)

Arshad Noor, Chair, EKMI TC
arshad.noor@strongauth.com

OASIS IDtrust Workshop
Barcelona, Spain
October 22, 2007

Why do you need EKMI?

- Avoid going to jail
 - UK's Regulation of Investigatory Powers (RIPA) Act 2000 Part 3¹
- Avoid breach-related charges
 - TJX charge of \$216M²

1: <http://www.opsi.gov.uk/acts/acts2000/20000023.htm>

2: <http://www.sec.gov/Archives/edgar/data/109198/000095013507005281/b66678tje10vq.htm>

Why do you need EKMI?

- Regulatory Compliance
 - PCI-DSS, PCSA, HIPAA, FISMA, SB-1386, etc.
 - Impending Massachusetts H213 bill
- Avoiding fines - ChoicePoint \$15M, Nationwide Building Society £1M
- Avoiding lawsuits
 - Accenture, BofA, TD Ameritrade, TJX (multiple)
- Avoiding negative publicity
 - VA, IRS, Fidelity, E&Y, Citibank, BofA, WF, Ralph Lauren, UC, 300+ others

The Encryption Problem



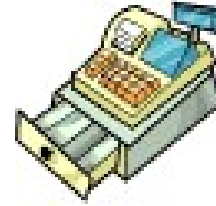
- Define Policy
- Generate
- Encrypt
- Decrypt
- Escrow
- Authorize
- Recover
- Destroy
- Audit



- 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



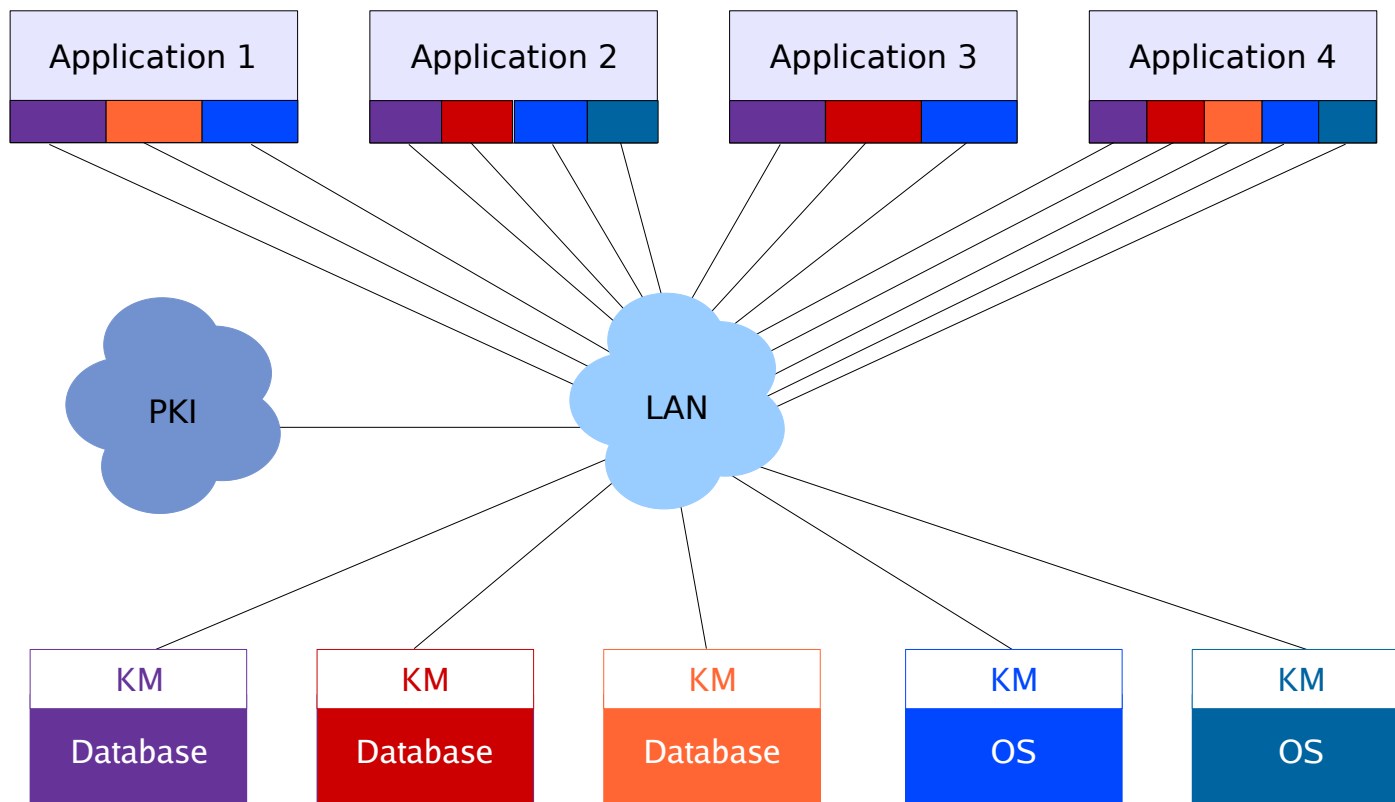
- Define Policy
- Generate
- Encrypt
- Decrypt
- Escrow
- Authorize
- Recover
- Destroy
- Audit



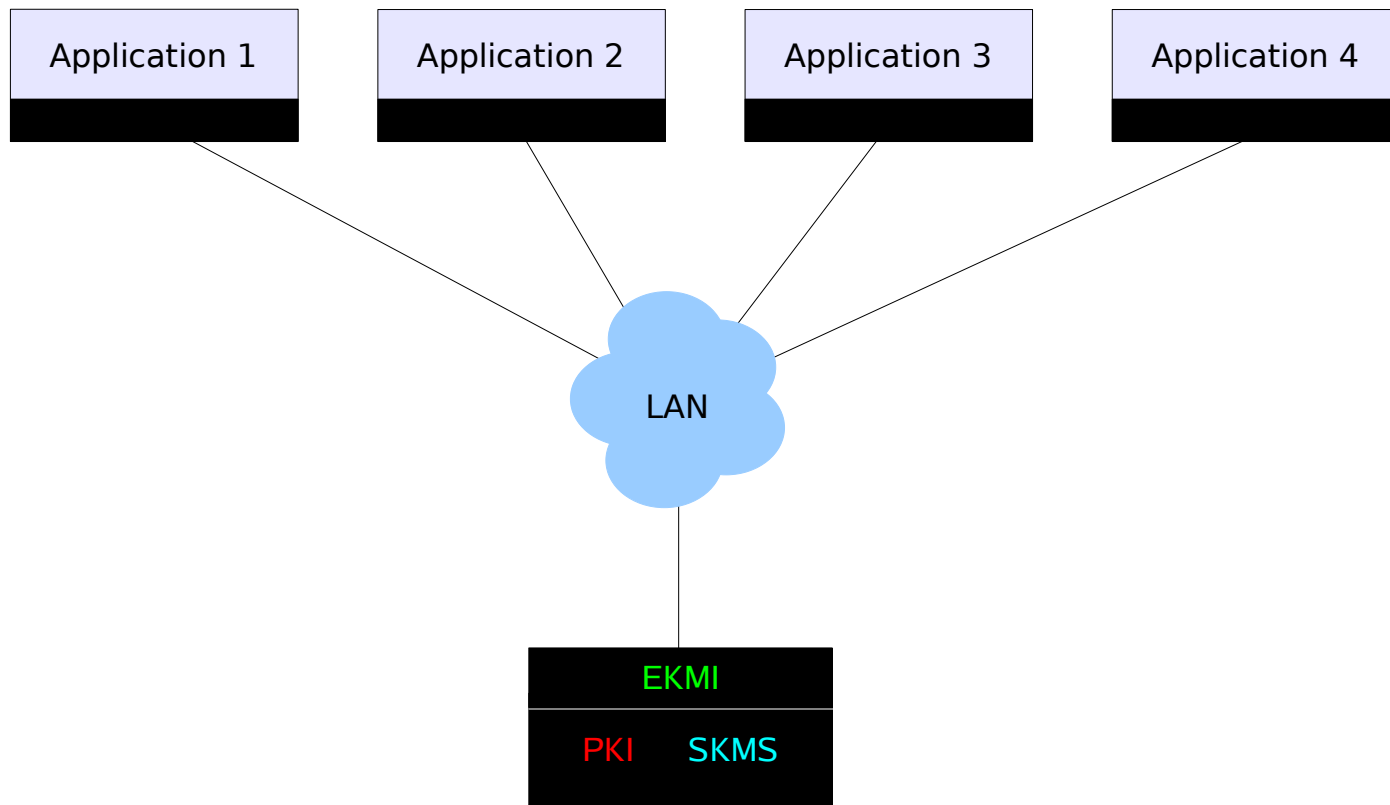
- Define Policy
- Generate
- Encrypt
- Decrypt
- Escrow
- Authorize
- Recover
- Destroy
- Audit

.....and on and on

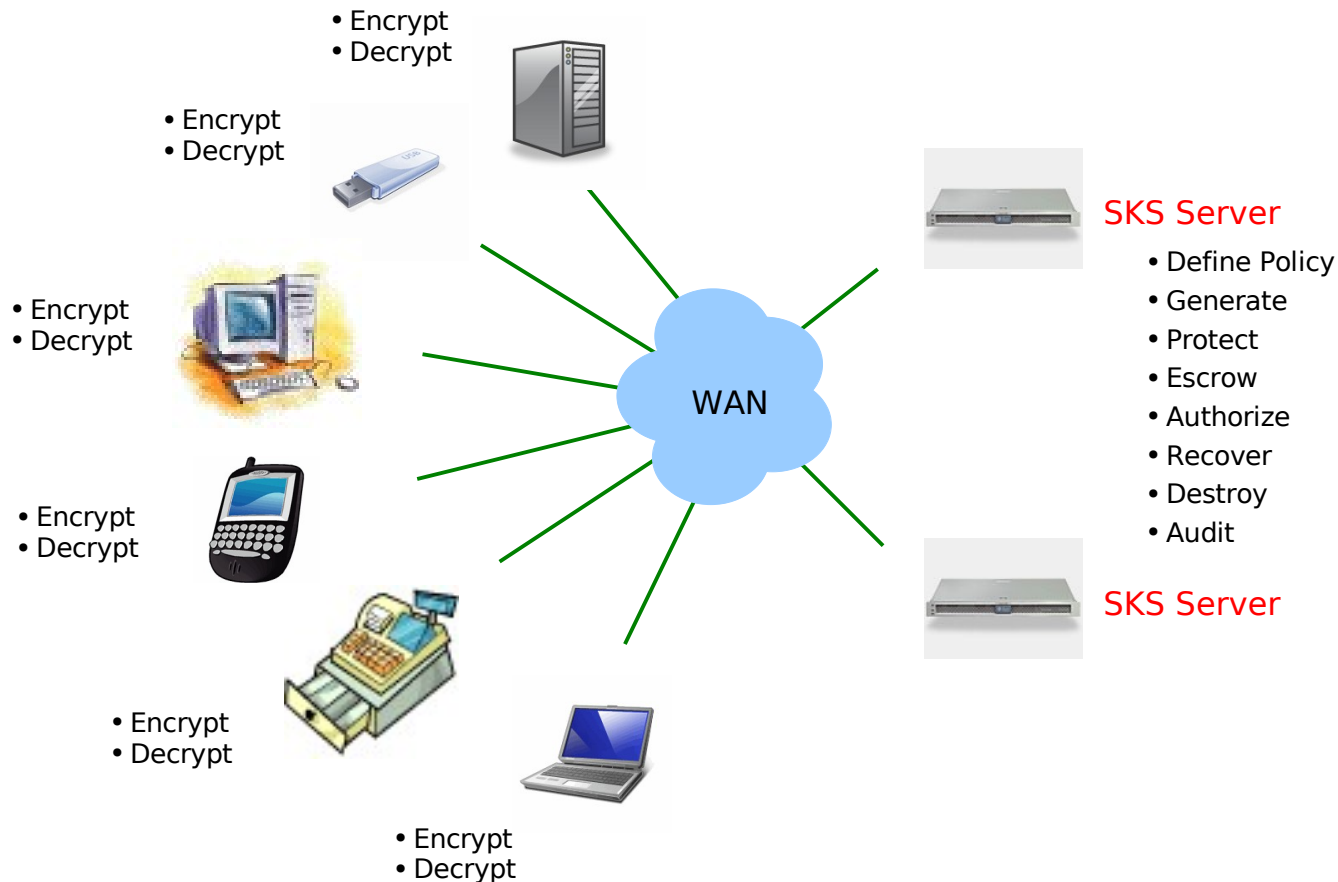
Key Management Silos



EKMI Harmony



The 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.”

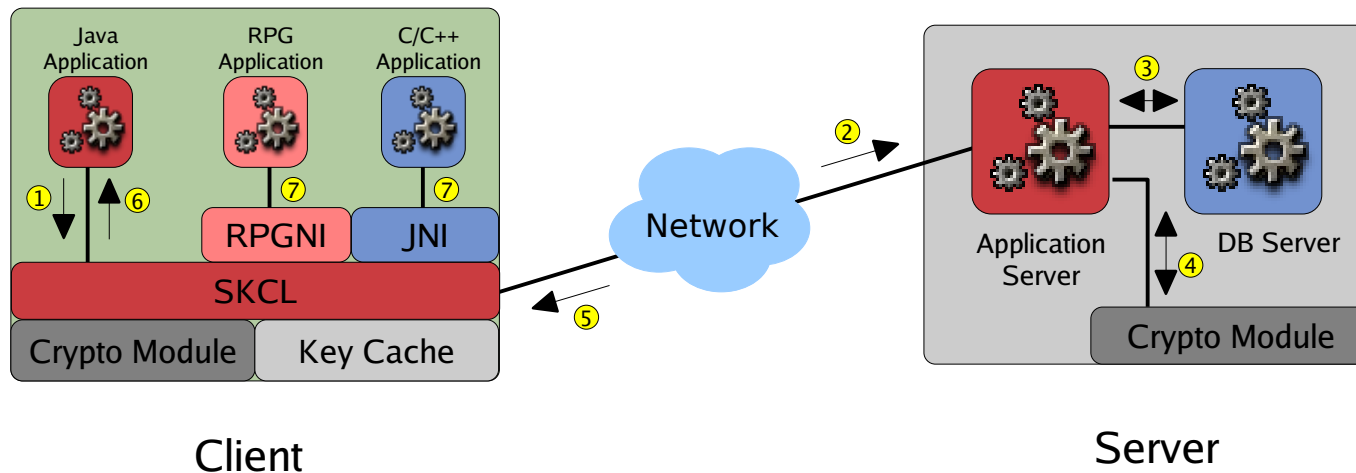
EKMI Characteristics

- 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

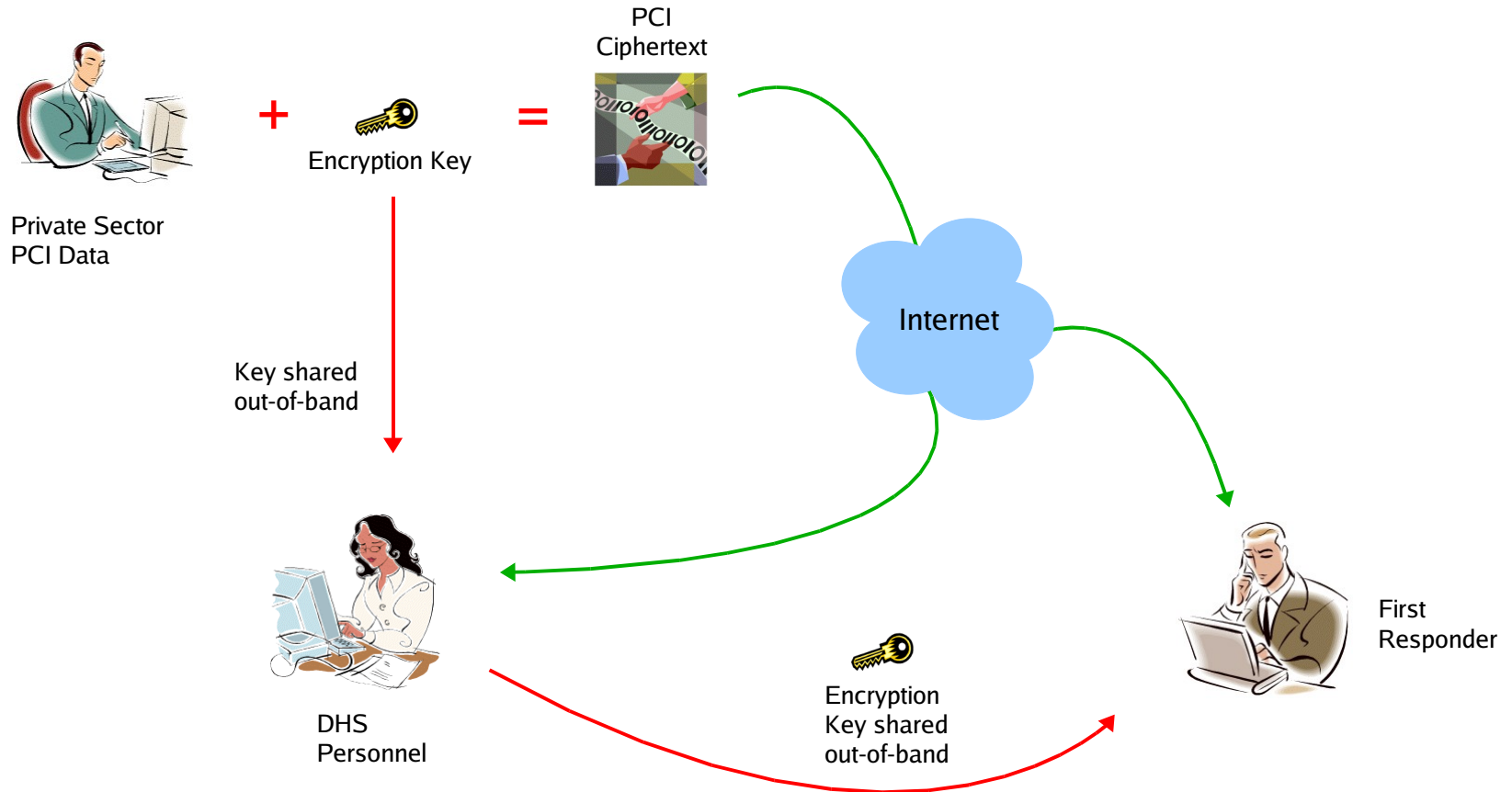
- Public Key Infrastructure
 - For digital certificate management; used for strong-authentication, and secure storage & transport of symmetric encryption keys
- Symmetric Key Management System
 - **SKS Server** for symmetric key management
 - **SKCL** for client interactions with SKS Server
 - **SKSML**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

SKMS 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

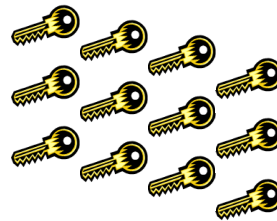
The Sharing Problem - (DHS-PCII)



The Sharing Problem - Multiplied



Private Sector PCI Data
(Tens of thousands?)



Encryption Keys

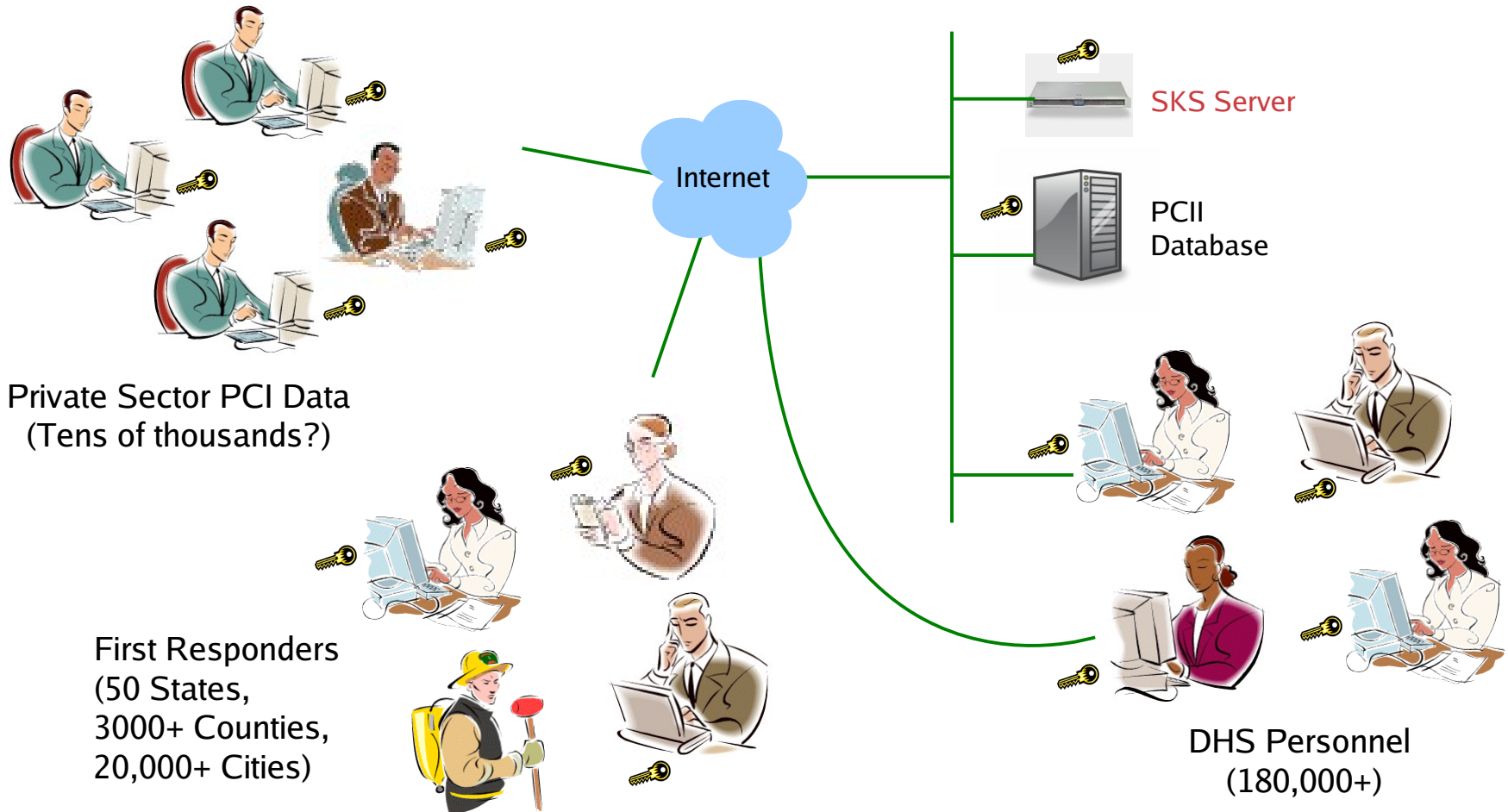


First Responders
(50 States,
3000+ Counties,
20,000+ Cities)

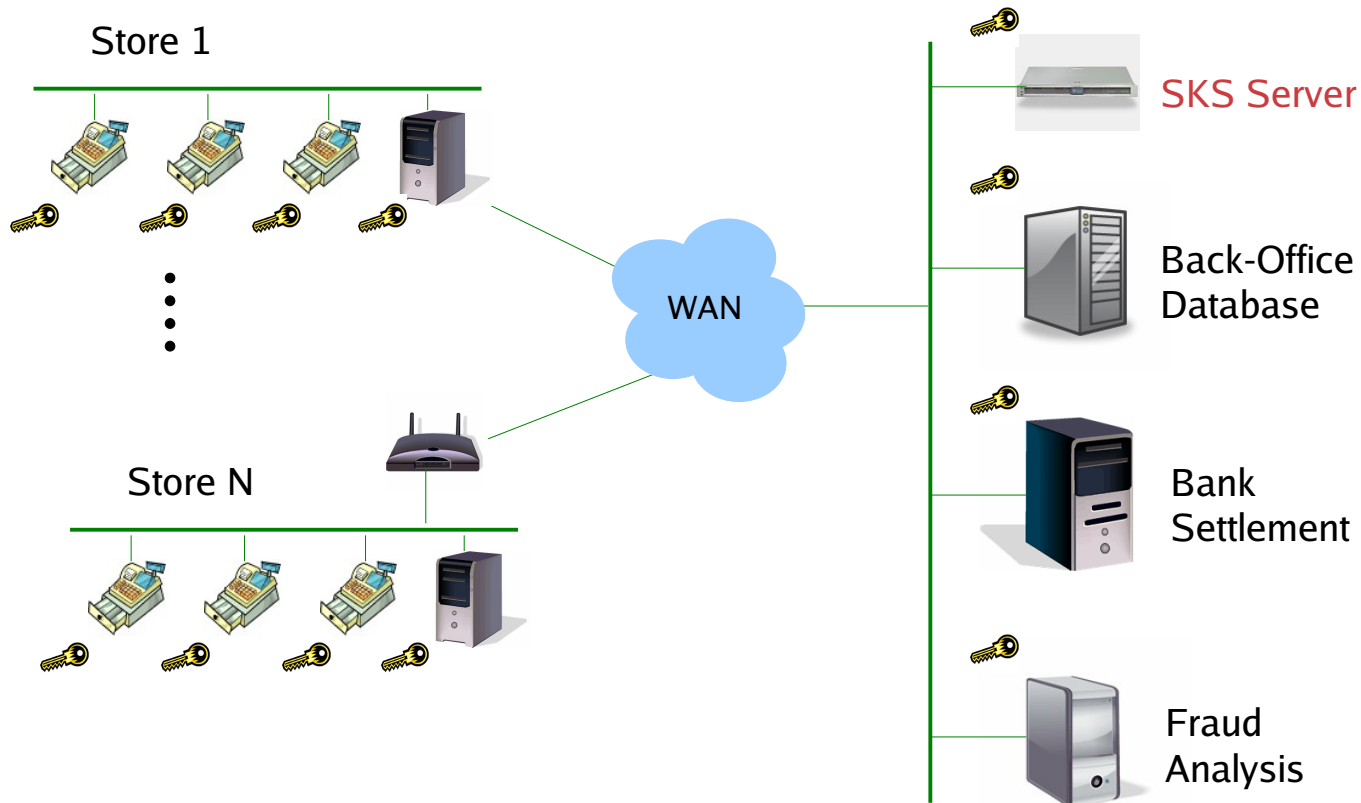


DHS Personnel
(180,000+)

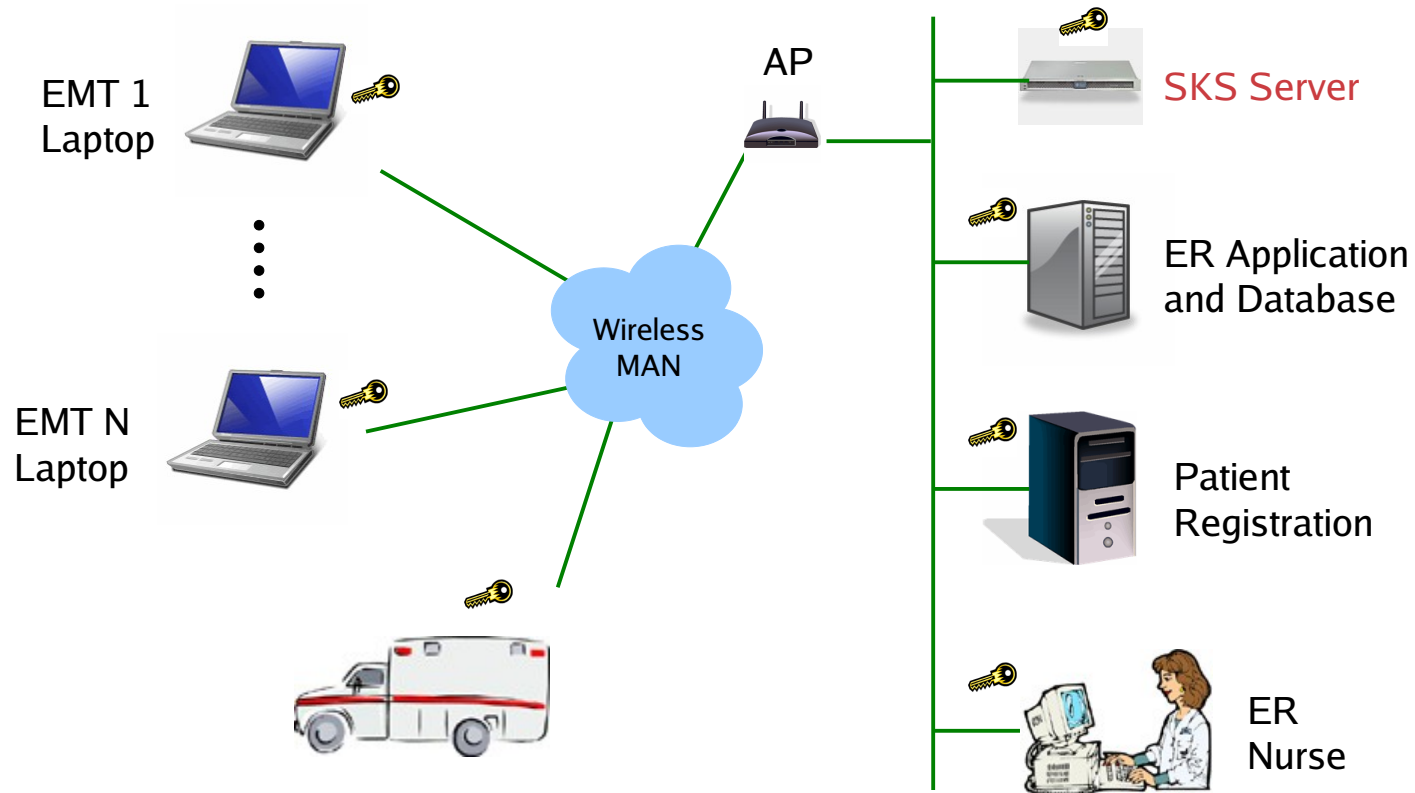
The Sharing Problem - Solved*



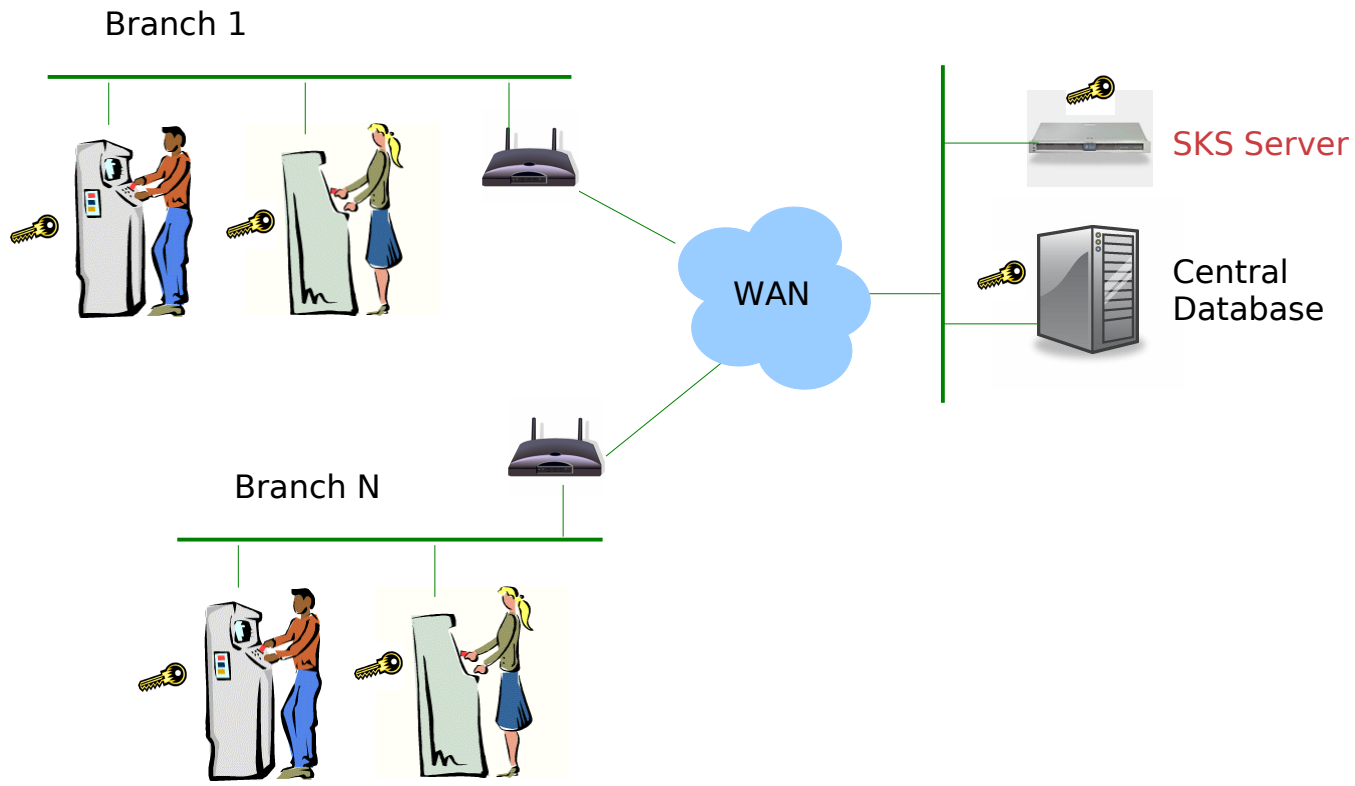
The Retail Solution



The Healthcare Solution



The Financial Solution



EKMI TC Goals

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

33 EKMI TC Members/Observers

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

* Founder Members

Burton Group on EKMI

"The life cycle of encryption keys is incredibly important. As enterprises deploy ever-increasing numbers of encryption solutions, they often find themselves managing silos with inconsistent policies, availability, and strength of protection. Enterprises need to maintain keys in a consistent way across various applications and business units," *said Trent Henry, senior analyst, Burton Group.* **"EKMI will be an important step in addressing this problem in an open, cross-vendor manner."**

<http://www.oasis-open.org/news/oasis-news-2007-06-25.php>

Conclusion

- “Securing the Core” should have been Plan A from the beginning – but its not too late for remediation
- OASIS EKMI TC is driving new key-management standards that cuts across platforms, applications and industries.
- Get involved!

Resources

- OASIS EKMI TC Resources
 - Use Cases, SKSML Schema, Presentations, White Papers, Guidelines, etc.
- www.strongkey.org - Open Source SKMS implementation
- www.issa.org - Article on SKMS in February 2007 issue of ISSA Journal