Securing Data Across the Enterprise using SOA

Section I
EKMI Rationale and Components

OASIS Open Standards
April 28, 2008

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

StrongKey® Securing the Core

Today's Goals

- Why do you need an EKMI?
- What is an EKMI?
- What are its components?
  - Architecture
  - Protocol
  - Working mechanics
- Use-case
- Demonstration

Why EKMI?

- Avoid going to jail
  - UK's Regulation of Investigatory Powers (RIPA) Act 2000 Part 3[1]
- Avoid breach-related charges
  - TJX charge of $216M[2]
- Protect your career

1: http://www.opsi.gov.uk/acts/acts2000/20000023.htm
2: http://www.sec.gov/Archives/edgar/data/109198/000095013507005281/b66678tje10vq.htm

Why EKMI?

- Regulatory Compliance
  - PCI-DSS, PCSA, HIPAA, FISMA, SB-1386, etc.
  - Massachusetts H213 bill, EU Directive – Sec. 16
- Avoiding fines - ChoicePoint $15M, Nationwide Building Society £1M
- Avoiding lawsuits
  - Accenture, BofA, TD Ameritrade, TJX (multiple), Hannaford
- Avoiding negative publicity
  - VA, IRS, Fidelity, E&Y, Citibank, BofA, WF, Ralph Lauren, UC, 400+ others

Why EKMI?

- **Network security is <u>NOT</u> working**
  - PriceWaterhouseCoopers/CIO Magazine
    Global State of Information Security Survey 2007
    - 7,200 CEOs, CFOs, CIOs, CSOs, VP's, Directors
    - 100 Countries
    - 36% North America
    - 28% Europe
    - 23% Asia
    - 12% South America
    - 2% Middle-East/South Africa

Source: http://www.cio.com/article/133600/

Why EKMI?

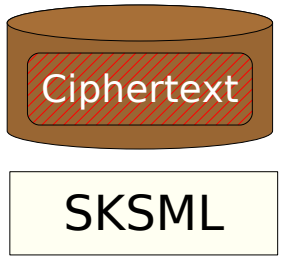
- 69% do NOT keep an inventory of user data
- 67% do NOT know where data is stored
- 45% do NOT know what type of attacks have occurred
- 40% do NOT know how many security incidents they have experienced
- 33% are NOT compliant with privacy laws

What does/will work?

- **Securing data**
  - Encrypted by application at the source
  - Decrypted by application at destination
  - Secure everywhere
    - In-motion: E-mail, FTP, HTTP, etc.
    - At-rest: Database, Log files, SAN/NAS, Tapes, Flash drives, PDAs, CDs, Laptops, etc.
  - Network is irrelevant
  - Storage media is irrelevant
  - Database is irrelevant

What is relevant?

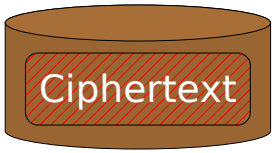
- Encryption & Key Management



What is relevant?

- Encryption & Key Management
- Identity Management

(IDM)^{IPF}

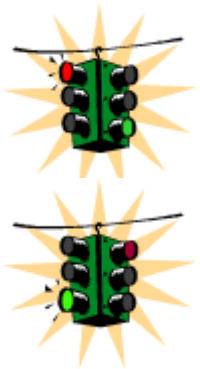


SKSML

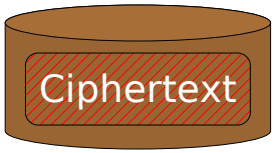
What is relevant?

- Encryption & Key Management
- Identity Management
- Access Control Management

(IDM)[IPF]



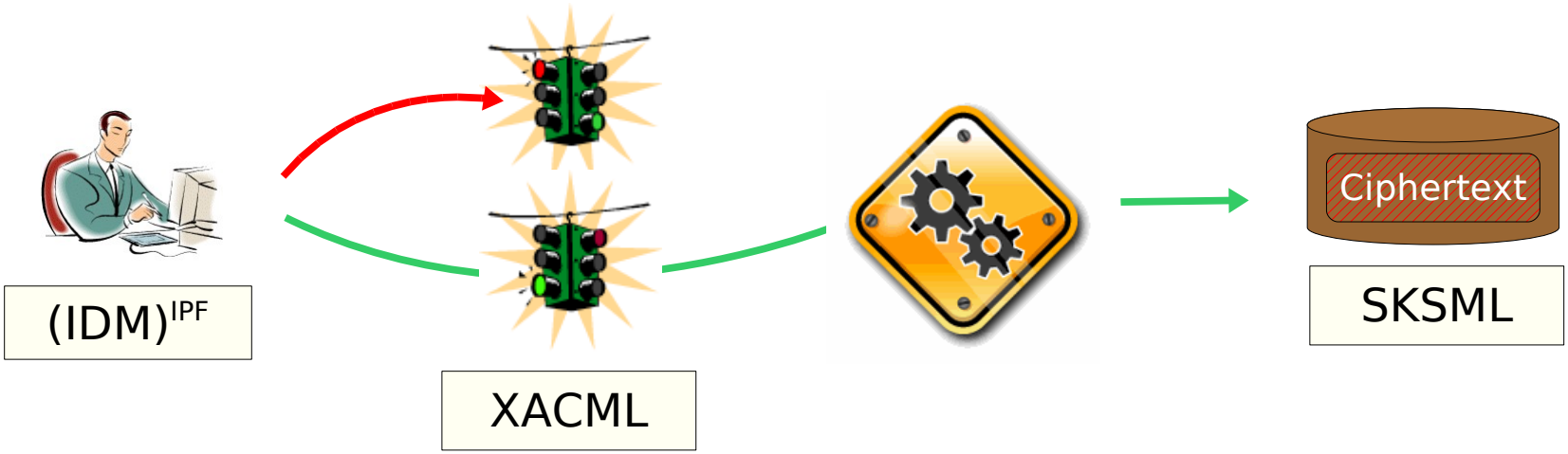
XACML



SKSML

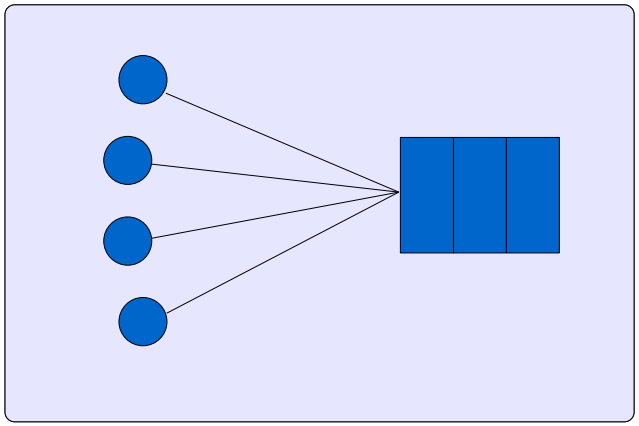
What is relevant?

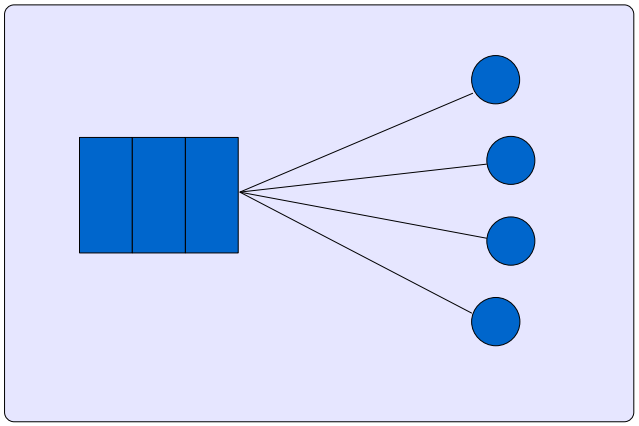
- Encryption & Key Management
- Identity Management
- Access Control Management
- Well designed and written software

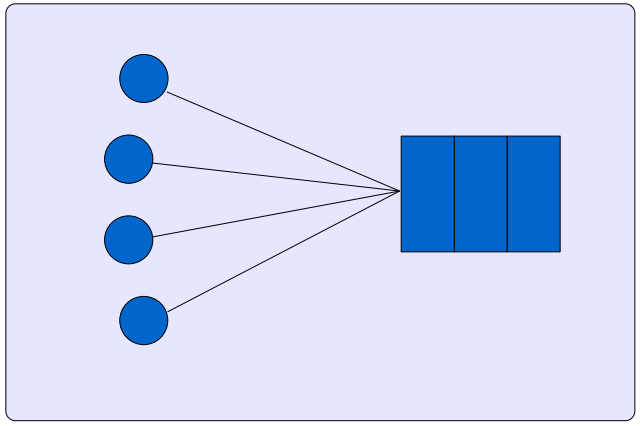


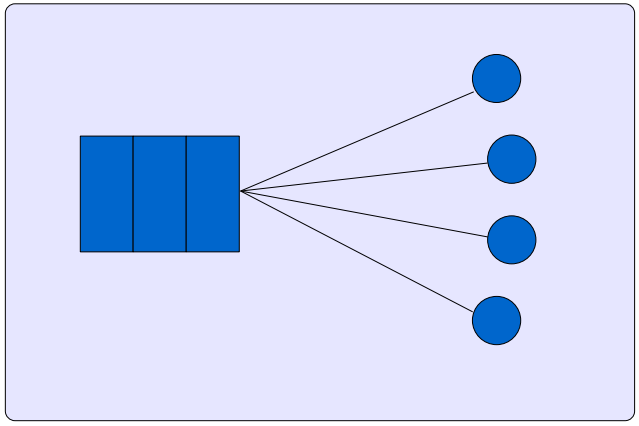
KM History – Current State

In the beginning..

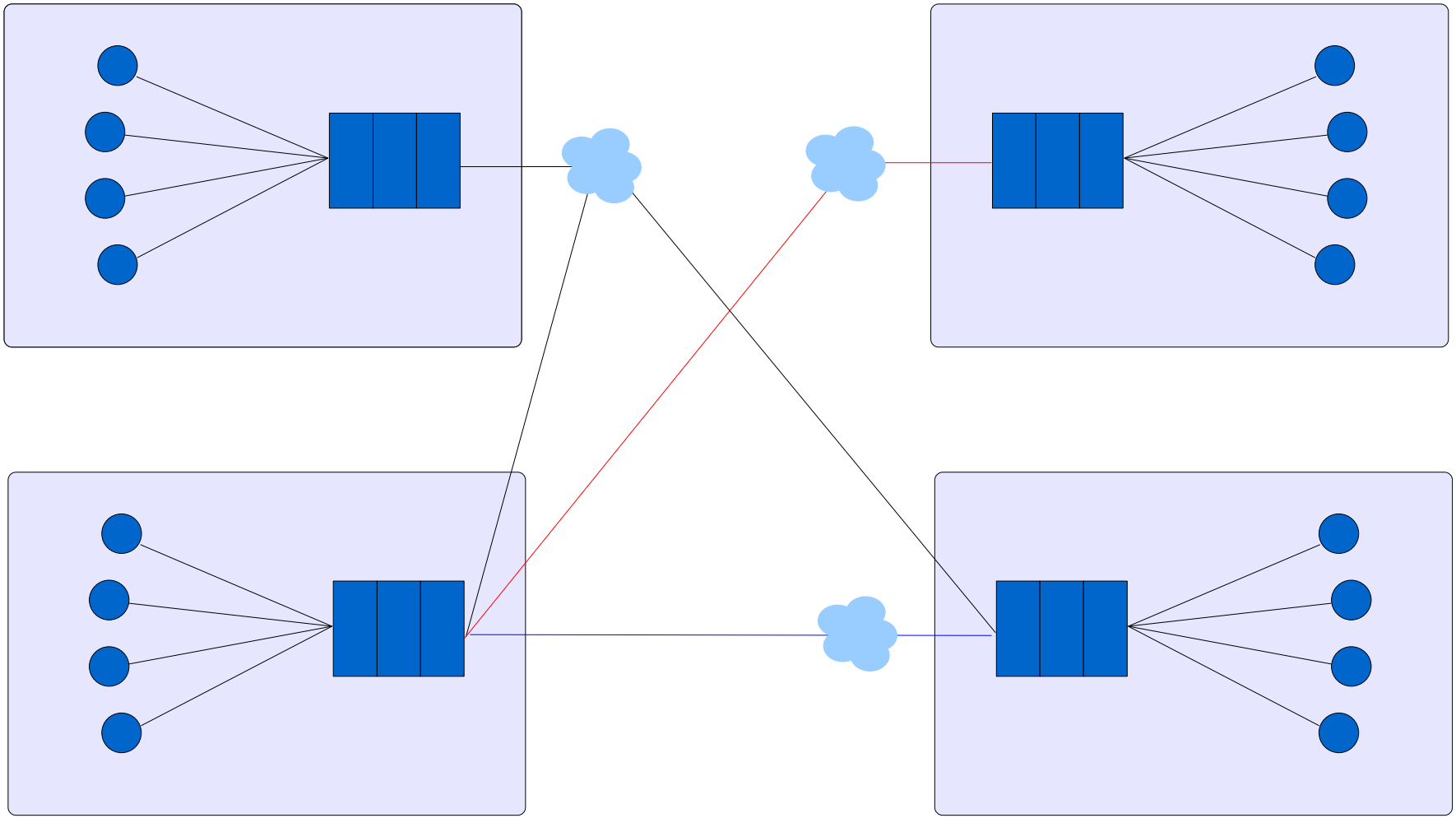




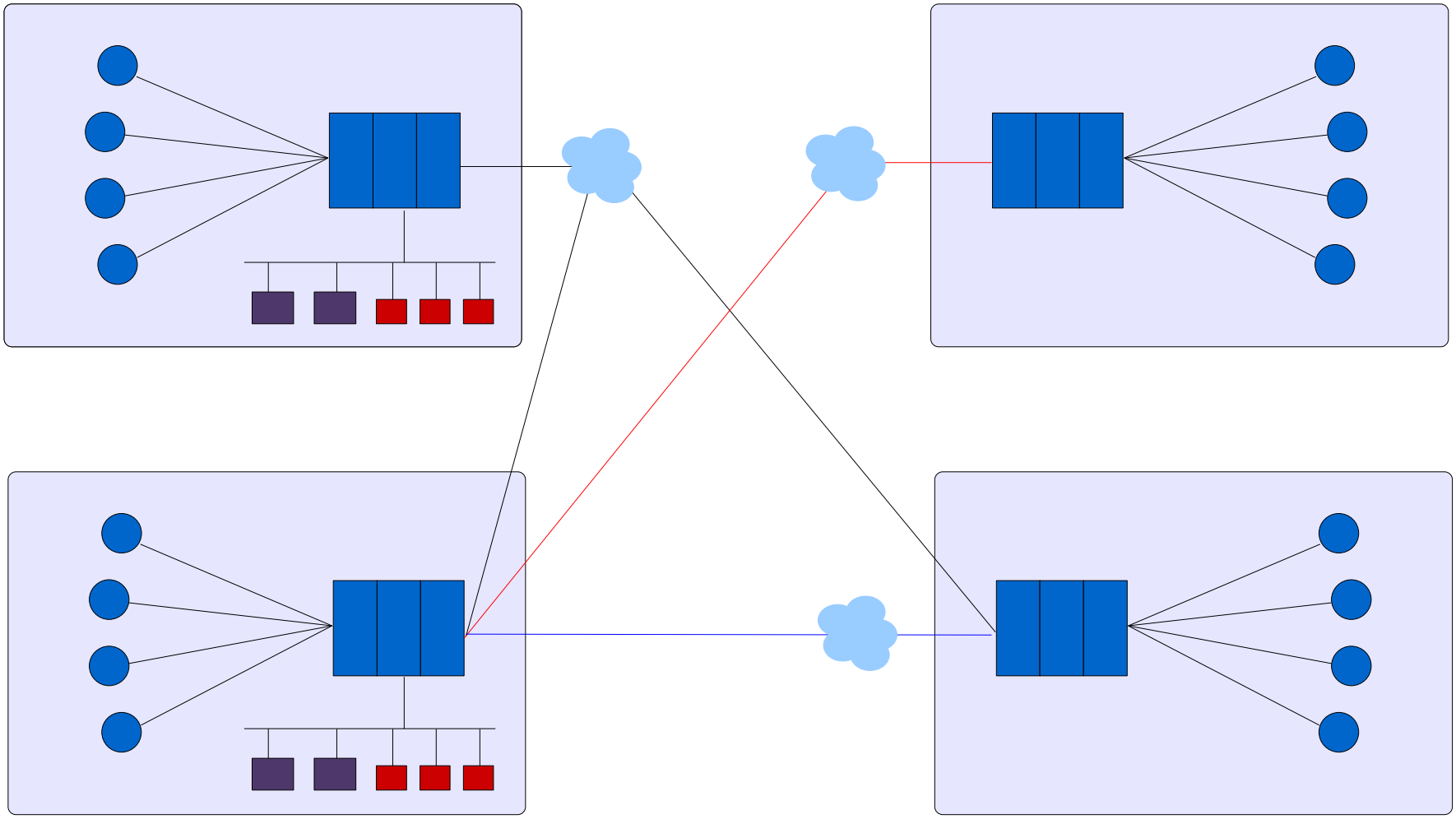




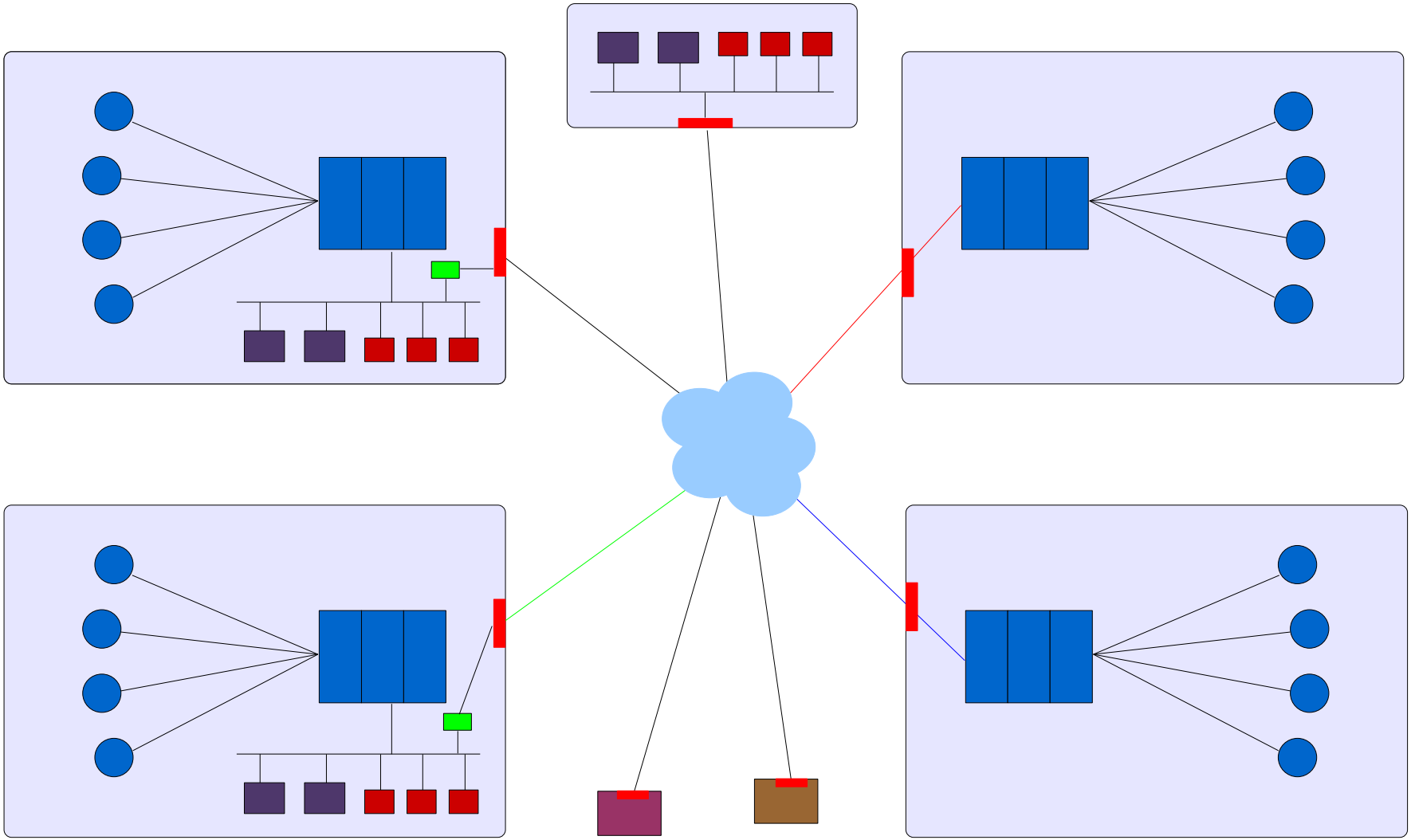
Private networks



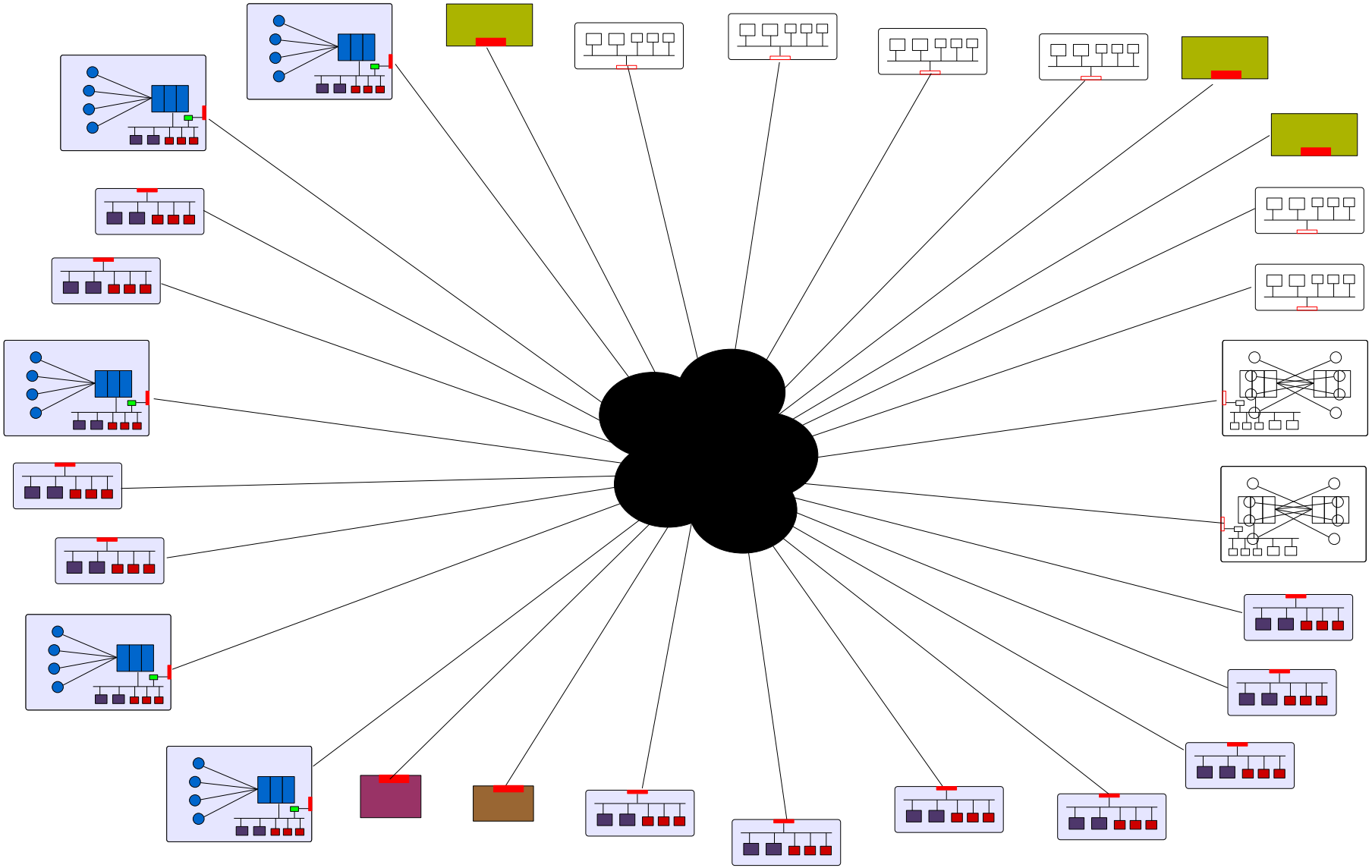
LANs



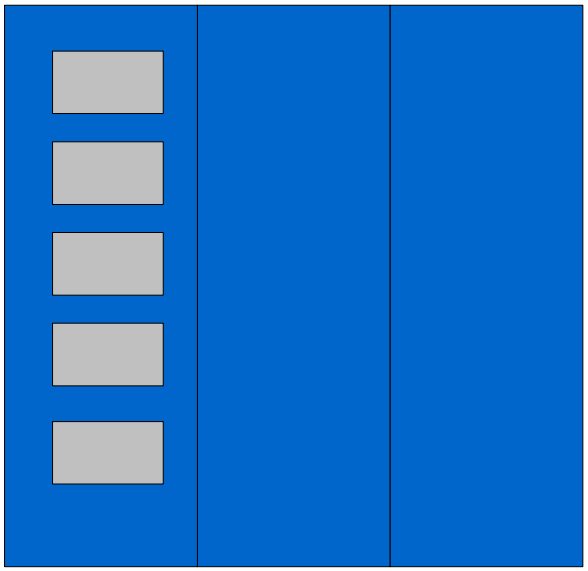
Internet



WWW

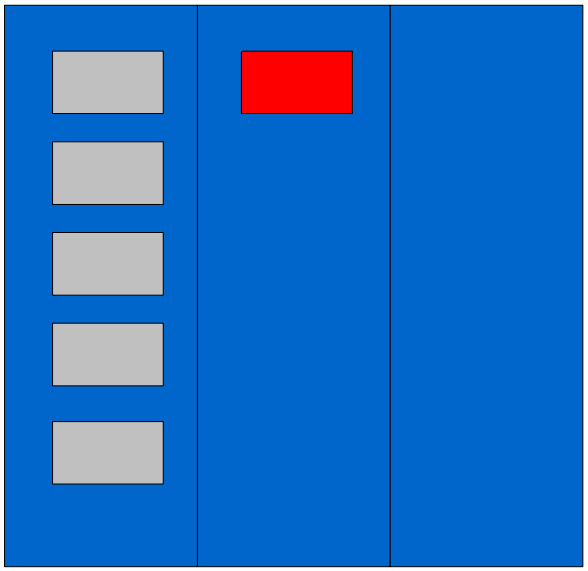


Before Encryption



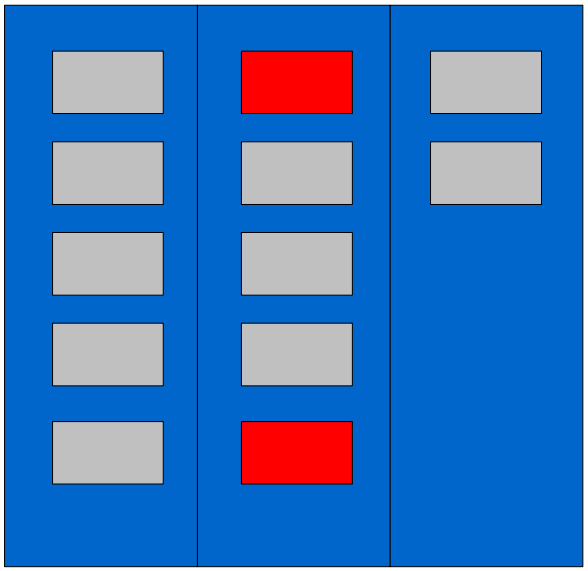
- No need to do anything because application just performed business functions
- Almost impossible to compromise a system unless you were an insider

Encryption – Early Days



- Application had to perform business function and "key management"
  - Generate
  - Encrypt
  - Decrypt
  - Protect
  - Destroy
  - (Implicit Policy)

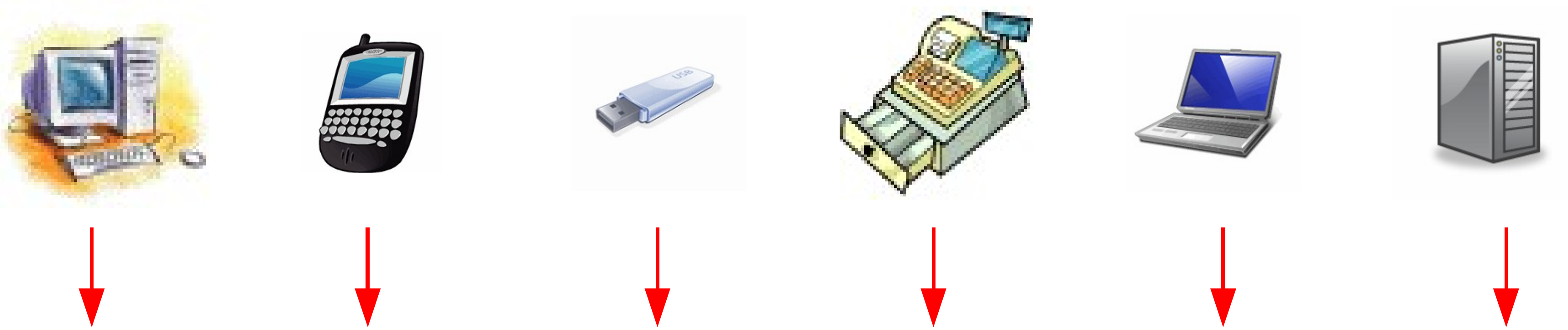
Encryption – Early Days



- New application had to perform business function and "key management"
  - Generate
  - Encrypt
  - Decrypt
  - Protect
  - Destroy
  - (Implicit Policy)

STRONGKEY® Securing the Core

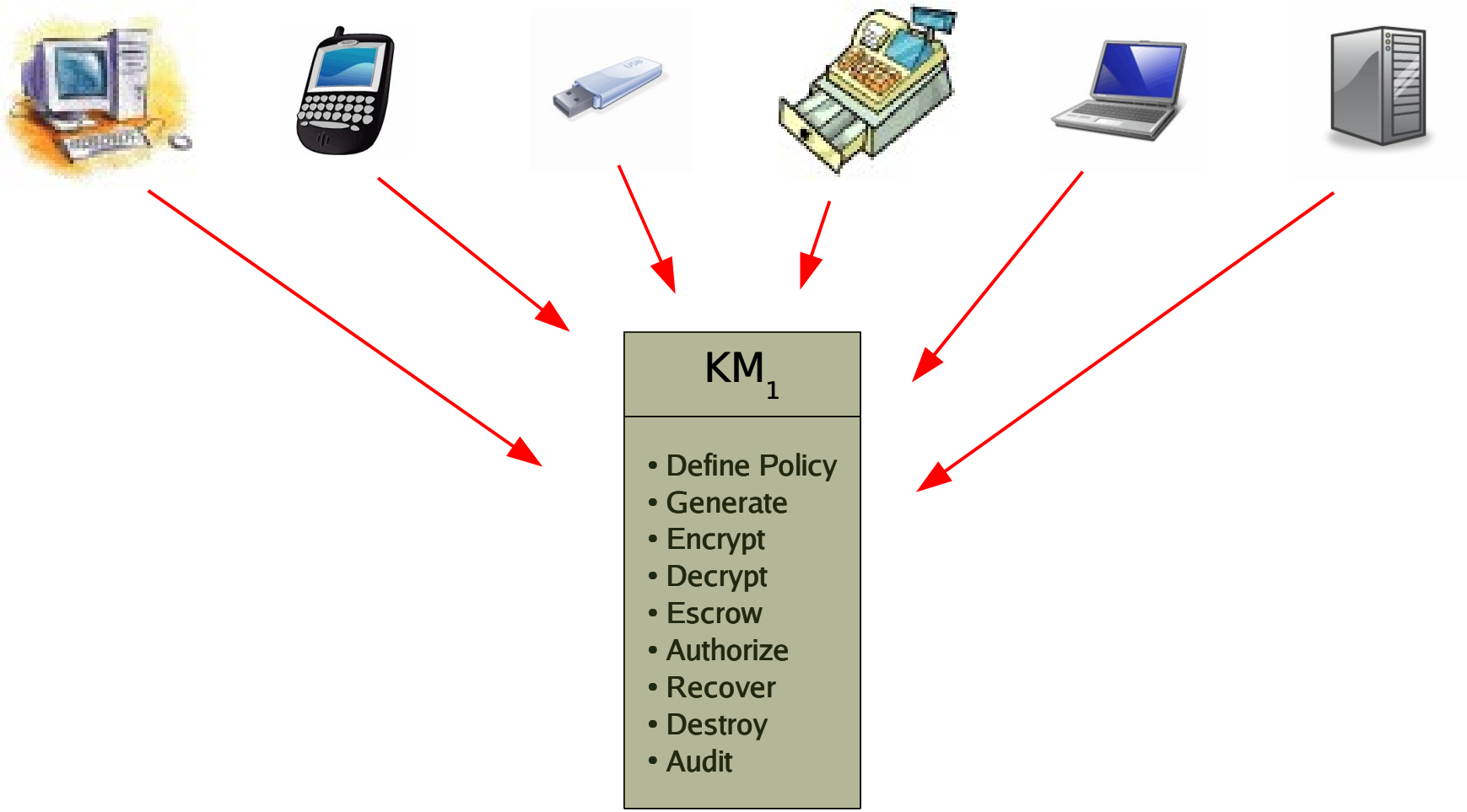
The current problem



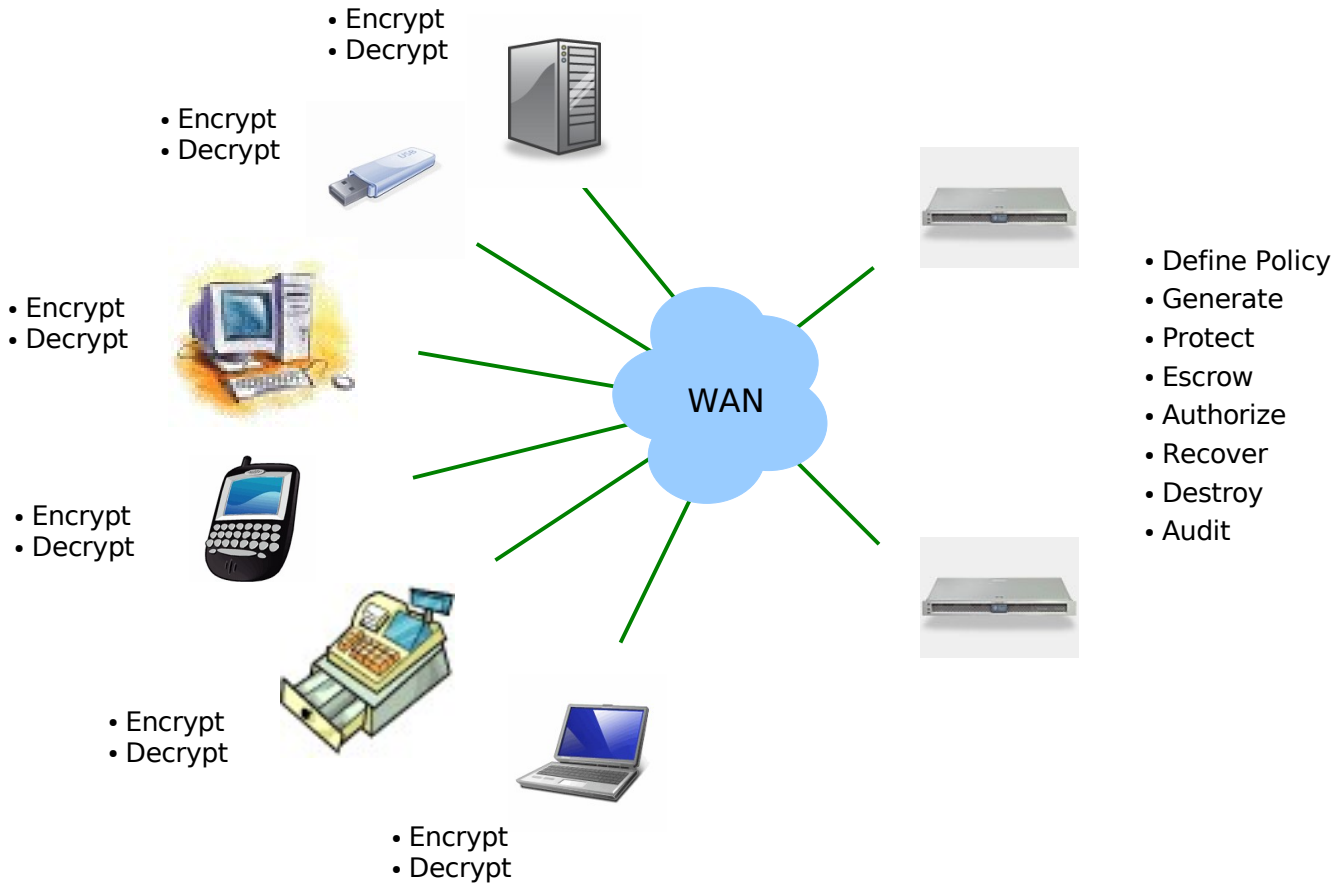
KM_1	KM_2	KM_3	KM_4	KM_5	$KM_{6, 7, 8}$
• Define Policy • Generate • Encrypt • Decrypt • Escrow • Authorize • Recover • Destroy • Audit	• Define Policy • Generate • Encrypt • Decrypt • Escrow • Authorize • Recover • Destroy • Audit	• Define Policy • Generate • Encrypt • Decrypt • Escrow • Authorize • 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

What you really want is..



Objective of EKMI



OASIS EKMI TC

- 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
- FundServ* (Canada)
- MISMO
- NuParadigm Government Systems
- PA Consulting (UK)
- PrimeKey (Sweden)
- Red Hat
- StrongAuth*
- US Dept. of Defense
- 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

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.

Other KM efforts

- IEEE 1619.3 Working Groups
  - Key Management protocol for storage devices
  - Including a namespace for EKMI so that they can accept keys/policies from an EKMI
- IETF KEYPROV
  - Provisions “symmetric keys”
  - Credentials for one-time password tokens

Conclusion

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