Enterprise Cryptographic Key Management Realities and Issues

Anthony J. Stieber

Systems Architect

IEEE KMS, Lake Tahoe, NV, USA

2010-05-05

Enterprise Cryptographic Key Management Realities and Issues

or

These Aren’t the Cryptographic Key Management Systems You’re Looking For

Agenda

- Introduction
- Terminology
- Why
- Issues
- Solutions
- Conclusion
- Questions?

Introduction

This presentation is not about:

- Ciphers
- Protocols
- Initialization vectors
- Block cipher modes of operation
- Random bit generators (deterministic or not)

Terminology

- Availability/Confidentiality/Integrity (ACI)
- Cleartext/Ciphertext
- Cryptology/Cryptography/Cryptanalysis
- Cryptographic System
- Public Key Infrastructure (PKI)
- Reliability/Availability/Serviceability (RAS)
- Risk Management
- Secret
- Validity

Why Cryptographic Key Management

- Cryptographic keys are secrets that keep secrets.

Why Cryptographic Key Management

- Cryptographic keys are secrets that keep secrets.
- Encrypt the secret that keeps the secrets:

Why Cryptographic Key Management

- Cryptographic keys are secrets that keep secrets.
- Encrypt the secret that keeps the secrets:
  - Encrypt the secret that keeps those secrets:

Why Cryptographic Key Management

- Cryptographic keys are secrets that keep secrets.
- Encrypt the secret that keeps the secrets:
    - Encrypt the secret that keeps those secrets:
        - Encrypt the secret that keeps those secrets:
            - Encrypt the secret that keeps those secrets:
                - Encrypt the secret that keeps those secrets.

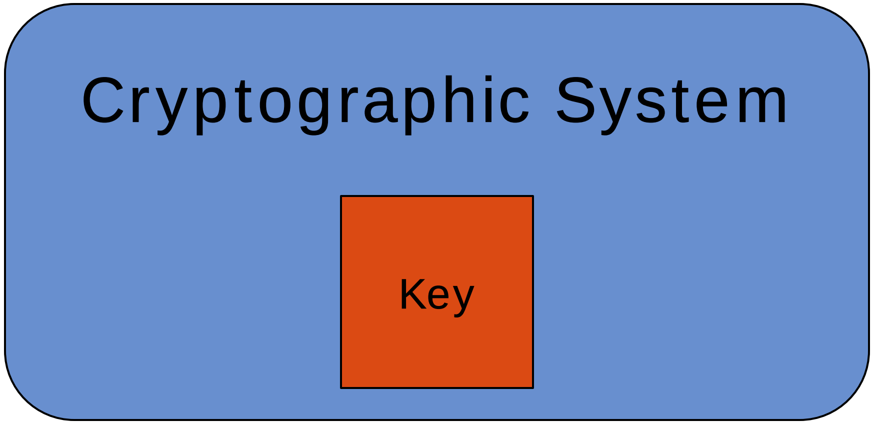
Why Cryptographic Key Management

- Cryptographic keys are secrets that keep secrets.
- Encrypt the secret that keeps the secrets:
  - Encrypt the secret that keeps those secrets:
    - Encrypt the secret that keeps those secrets:
      - Encrypt the secret that keeps those secrets:
        - Encrypt the secret that keeps those secrets.
- The final secret can't be encrypted.
- Risk starts at the top and goes all the way down.

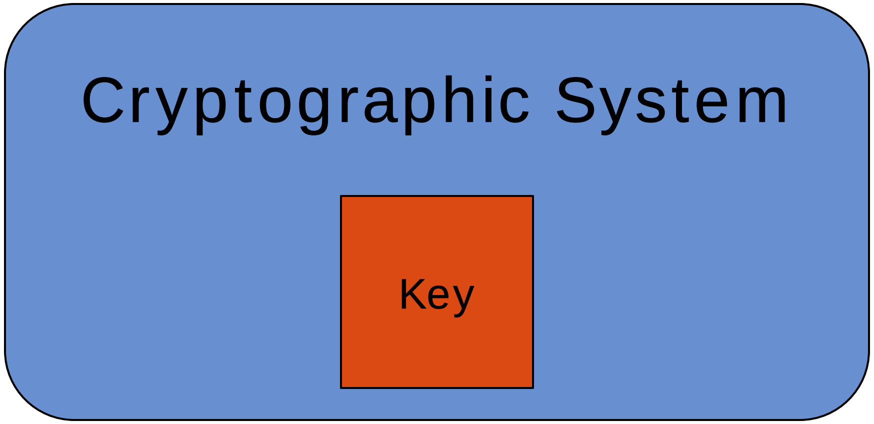
It’s really quite simple.

Cryptographic System

It’s more complicated.



It’s more complicated.

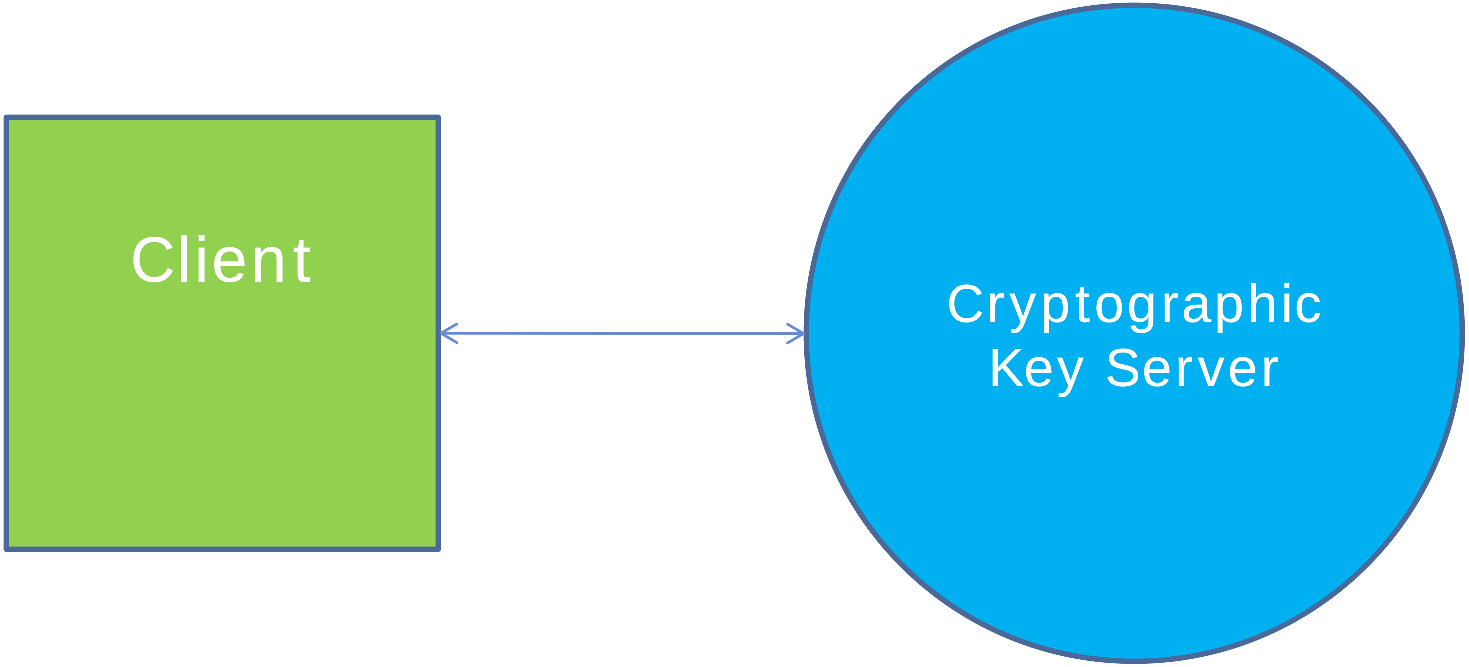


H. L. Mencken

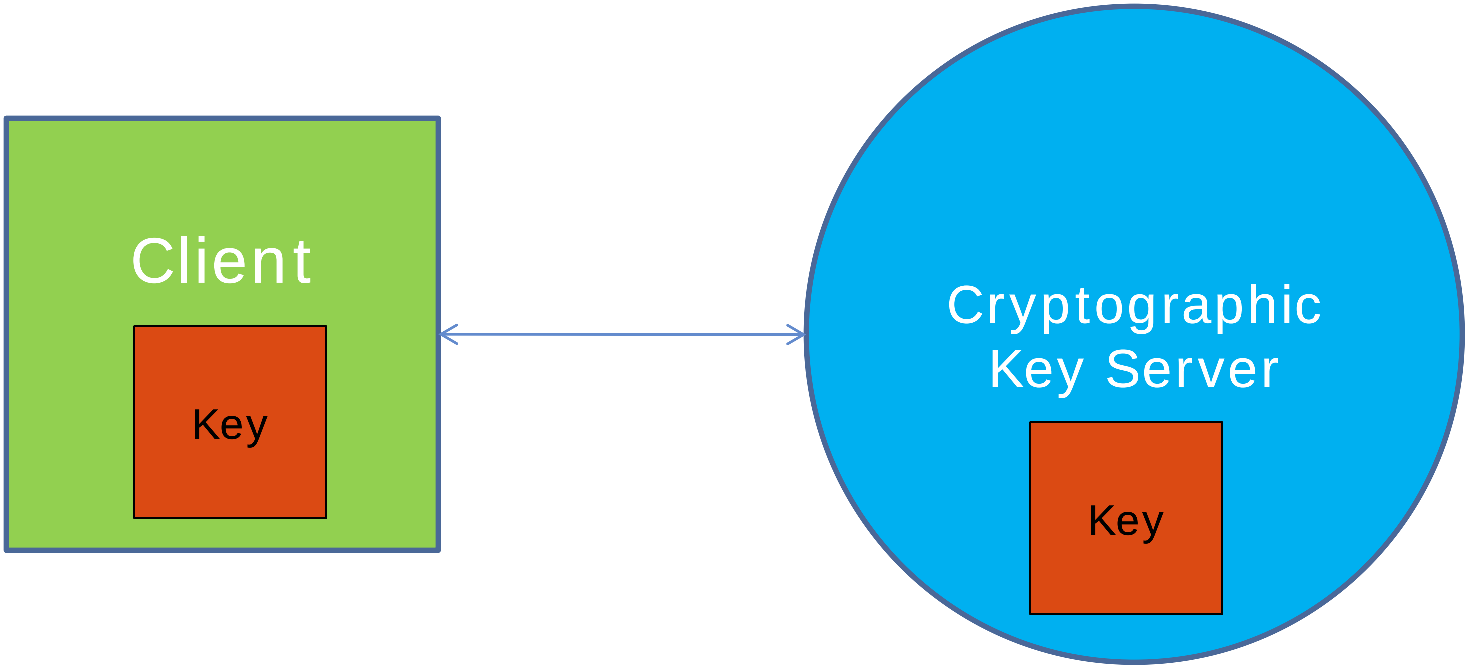
“...there is always a well-known solution to every human problem — neat, plausible, and wrong.”

"The Divine Afflatus" in New York Evening Mail (16 November 1917)

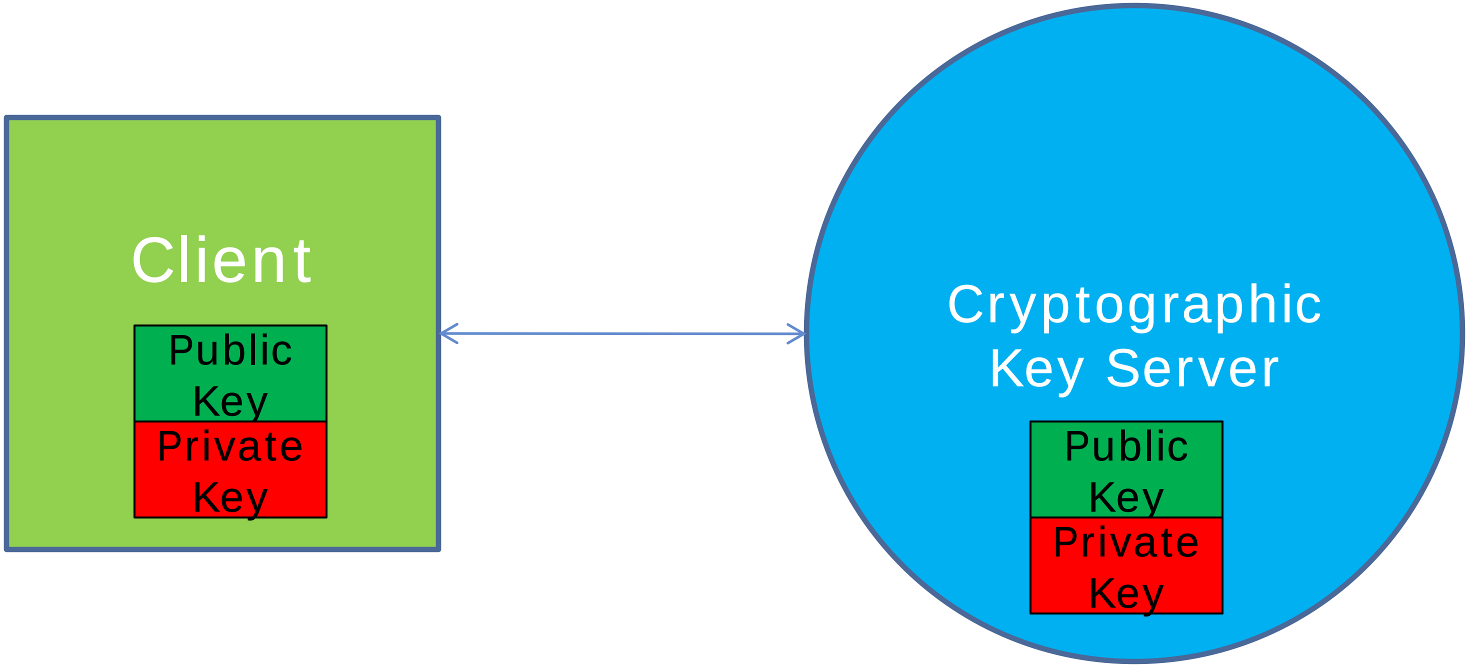
Maybe this is it



Forgot something important.



And one more thing.



Cryptographic Life Cycle

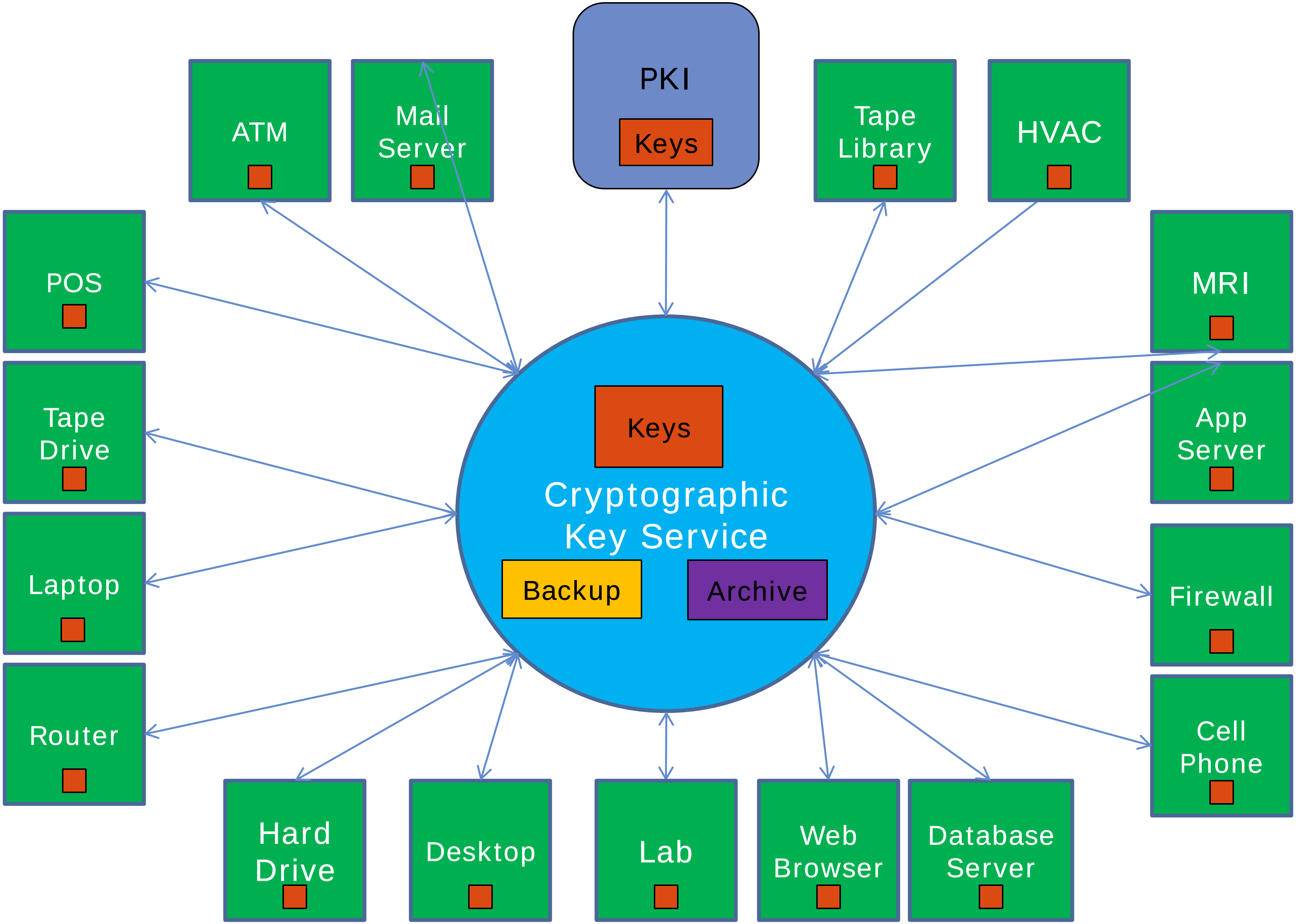
1. Generation
2. Backup
3. Distribution
4. Operation
5. Compromise
6. Recovery
7. Re-key/Update
8. Revocation
9. Archive
10. Destruction

Cryptographic Life Cycle

1. Generation
2. Backup
3. Distribution
4. Operation
5. **Compromise**
6. Recovery
7. Re-key/Update
8. Revocation
9. Archive
10. Destruction

Cryptographic Life Cycle

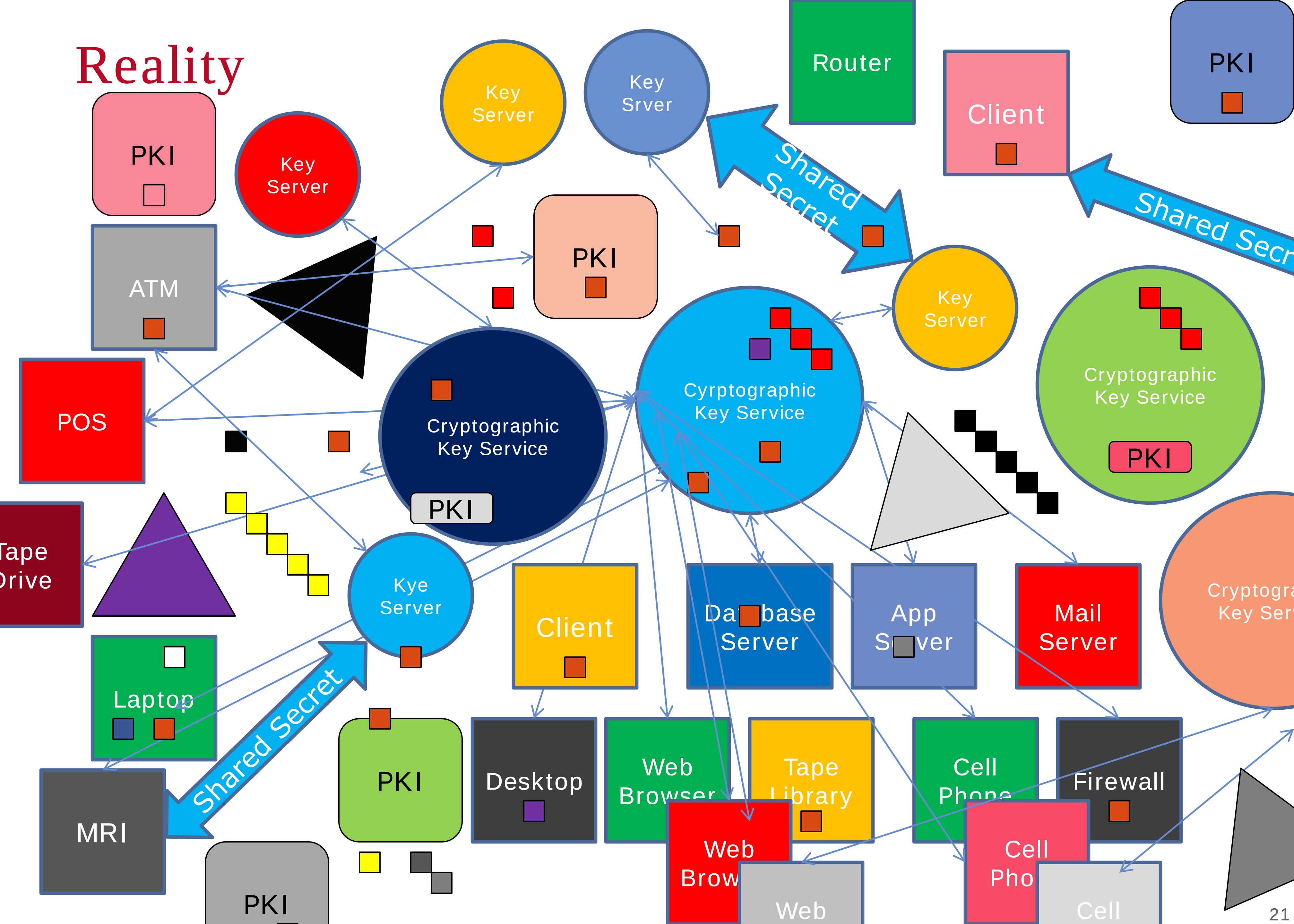
1. Generation → **Product specific**
2. Backup → DRP/BCP
3. Distribution → **Product specific**
4. Operation → **Product specific**
5. Compromise → Incident Response, Legal
6. Recovery → DRP/BCP
7. Re-key/Update → Incident Response
8. Revocation → Incident Response
9. Archive → Records Management, Legal
10. Destruction → Records Management, Legal


PKI
Keys
ATM
Mail Server
Tape Library
HVAC
POS
MRI
Tape Drive
App Server
Laptop
Firewall
Router
Cell Phone
Keys
Cryptographic Key Service
Backup
Archive
Hard Drive
Desktop
Lab
Web Browser
Database Server

Karel Čapek, author of R.U.R.

“There came into the world an unlimited abundance of everything people need. But people need everything except unlimited abundance.”
The Absolute at Large (1921)

Reality


Key Server
Key Srver
Router
Client
PKI
PKI
Key Server
Shared Secret
Shared Secr
ATM
PKI
Key Server
POS
Cryptographic Key Service
PKI
Cyrptographic Key Service
Cryptographic Key Service
PKI
Tape Drive
Kye Server
Client
Database Server
App Server
Mail Server
Cryptogra Key Serv
Laptop
Shared Secret
PKI
Desktop
Web Browser
Tape Library
Cell Phone
Firewall
MRI
Web Brow
Cell Pho
PKI
Web
Cell

Andrew S. Tanenbaum, author of Minix

“The nice thing about standards is that you have so many to choose from.”

Computer Networks, 2nd edition, page 254

There are standards?

Andrew S. Tanenbaum, author of Minix

“The nice thing about standards is that you have so many to choose from.”

Computer Networks, 2nd edition, page 254

- ASC X9.*
- GlobalPlatform
- IEEE P1619.*
- IETF RFC*
- ITU-T X.509
- PKIX X.509
- NIST FIPS & SP
- OASIS KMIP & EKMI
- OpenPGP
- ISO/IEC*
- Passwords
- PKCS#*
- WC3 XKMS
- Vendors

Different Needs

- Individuals
- SOHO
- Small Business
- Enterprise
- Government

- Finance/Insurance
- Health/Medical
- Manufacturing
- Retail/Merchant
- Technical

Reliability, Availability, Serviceability, Scalability

- Time to Failure
- Time to Recovery
- Operations (backup, rekeying, etc.) downtime
- Downtime affects downstream systems

Reliability, Availability, Serviceability, Scalability

- Hundreds of thousands of users and computers
- Millions of keys
- Life of the patient/product/loan + 7 years

What doesn’t work

- Can’t create own keys
- Can’t renew/replace keys
- Can’t renew/replace keys without major downtime

What doesn’t work

- Can’t store enough keys
- Can’t manage enough keys
- Can’t scale without high administrative effort

What doesn’t work

- Can’t recover from failure
- Can’t recover from compromise
- Which means it doesn’t work

Cryptographic key management failures

Alfred E. Neuman, mascot
“What, me worry?”
Mad #24 (July 1955)

- Extinct DRM (various)
- Netscape SSL RNG (1994)
- Single DES (1997)
- MD5 integrity (2004)
- Debian OpenSSL RNG (2008)
- SHA-1 integrity (2011?)
- RSA/DH 1024 (2014?)

What to do?

- Manage risks
- Short term: BCP/DRP
- Long term: Exit plan or plan data jail
- Longer term: Complain to vendors
- Beware of NIST FIPS 140 and Common Criteria
- Passwords aren’t cryptographic keys
- Current Year - 2000 auth password length

Who do you need?

The critical people for success:

- Management and Business support
- Cryptographic Key Management Team
- BCP/DRP people and plan
- Legal
- Physical Security
- Records Management
- Vendors

A Better Future

- Secure
- Usable
- Suite of complementary standards
- Multi-vendor and vendor-agnostic
- Unified
- Centralized
- If you want it

Questions?

References

Karel Čapek

http://en.wikiquote.org/wiki/Karel_%C4%8Capek

OASIS KMIP

http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=kmip

H. L. Mencken

http://en.wikiquote.org/wiki/H._L._Mencken

Alfred E. Neuman

http://en.wikipedia.org/wiki/Alfred_E._Neuman

NIST SP800-57 “Recommendation for Key Management”

http://csrc.nist.gov/publications/PubsSPs.html

Andrew S. Tanenbaum

http://en.wikiquote.org/wiki/Andrew_S._Tanenbaum

Bart Preneel

http://homes.esat.kuleuven.be/~preneel/