Introduction to Key Management Services
Managing keys in the data center

Landon Curt Noll

chongo@cisco.com

An espresso shot
served by
by Landon Curt Noll

Copyright © Landon Curt Noll & Cisco Systems, 2010.
All rights reserved. Permission for use by KMS2010.

2010-Apr-30 v1.30

Talk Outline

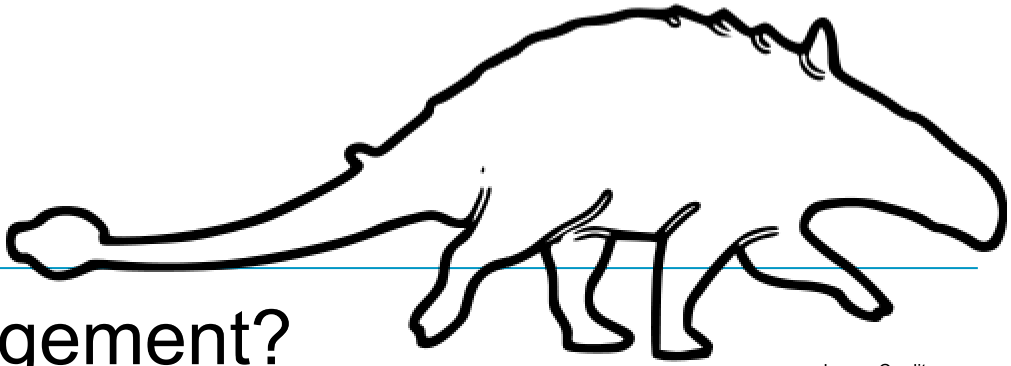


Image Credit:
Wiktionary definition of outline
Creative Commons License

- Review: What is Key Management?
- Concept: Data Center Class Key Management
- Need: The key importance of Standards

Copyright © Landon Curt Noll & Cisco Systems, 2010.
All rights reserved. Permission for use by KMS2010.

Review: What is Key Management?

Image Credit: t-cubesystems.com product catalog

Copyright © Landon Curt Noll & Cisco Systems, 2010.
All rights reserved. Permission for use by KMS2010.

Review: What is Key Management?

Image Credit:
Flickr user ul_Marga
Creative Commons License

- Key Management is the complete set of operations necessary to nurture and sustain encrypted data and its associated keys during the key life-cycle

- A Key Management Service is an implementation of all or parts of Key Management Operations

- The Key Management Policy translates business security requirements into Key Management Operations which are then executed by a Key Management Service

- Key Management Audit securely records all Key Management operations associated with keys under its control

Copyright © Landon Curt Noll & Cisco Systems, 2010.
All rights reserved. Permission for use by KMS2010.

Review: What Key Management is not

(a partial list)

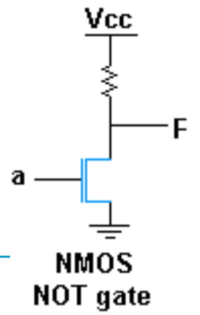


Image Credit:
Wikipedia
Creative Commons License

- Key Management is not about using keys
  - It is more about managing the use of keys
- Key Management is not how a protocol negotiates keys
  - Although it may track the use and life of a negotiated key
- Key Management is not SSL/TLS key negotiation
  - Although Key Management Clients and Servers may use SSL/TLS to protect their communication
- Key Management is not a key escrow service
  - Although an escrow service could be built in top of a Key Management Service

Copyright © Landon Curt Noll & Cisco Systems, 2010.
All rights reserved. Permission for use by KMS2010.

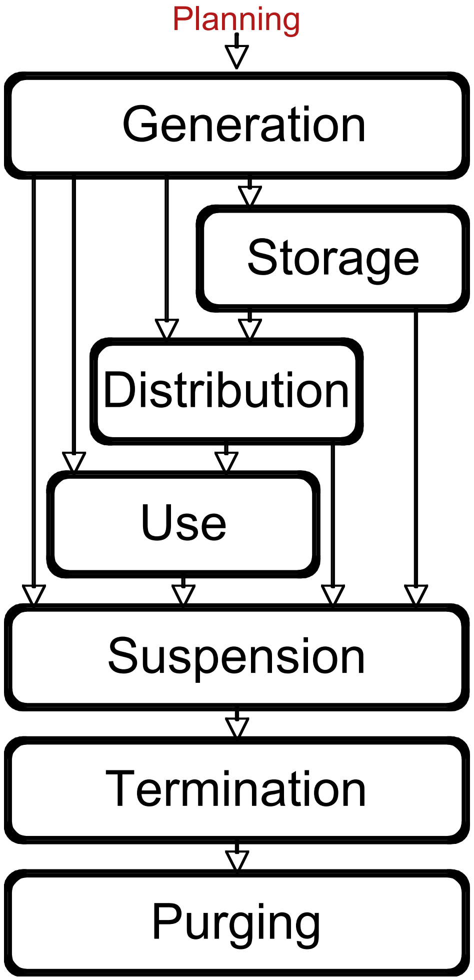
Review: One Model of a Key's Life Cycle

TIMTOWTDIBSCINABTE* (pronounced Tim Toady Bicarbonate)

Espresso Still Life
Public domain photo by Mark Prince

- Key Management helps throughout the life of a key

- Stage 0: Planning
- Stage 1: Key Generation
- Stage 2: Key Storage
- Stage 3: Key Distribution
- Stage 4: Key Use
- Stage 5: Key Suspension
- Stage 6: Key Termination
- Stage 7: Key Purging



*This Perl acronym is pronounced Tim Toady Bicarbonate:

"There is more than one-way to do it, but sometimes consistency is not a bad thing either"

Copyright © Landon Curt Noll & Cisco Systems, 2010.
All rights reserved. Permission for use by KMS2010.

Review: Policies that guide a key down life’s road

Image Credit:
Flickr user AceFrenzy
Creative Commons License

- Who may use a key
  - Device type, device class, application, application class, etc.
- What operations may be performed
  - Encrypt only, Decrypt only, Encrypt/decrypt, Sign, Verify, etc.
- Conditions of use
  - Time limit, usage count, HW and/or SW level, data size, etc.
- High level (usually more complex) business policy
  - Driven by legal, industry, business or customer requirements

Copyright © Landon Curt Noll & Cisco Systems, 2010.
All rights reserved. Permission for use by KMS2010.

Review: KM Audit Log

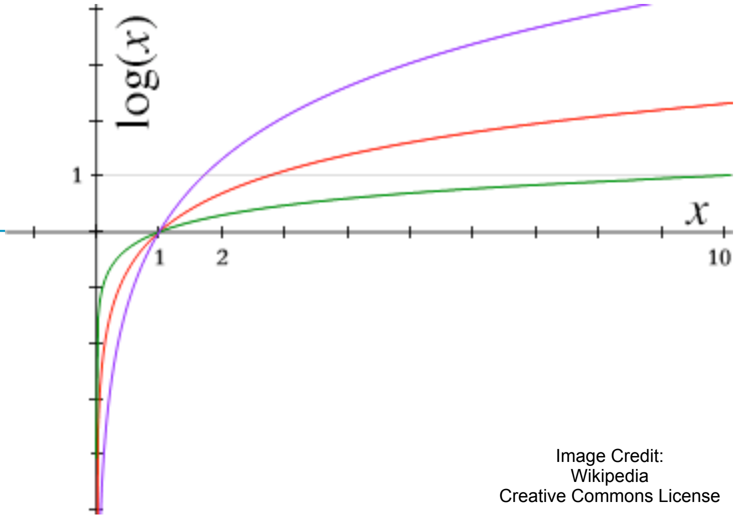


Image Credit:
Wikipedia
Creative Commons License

- Track all Key Management actions
  - Who asked for a key, when, etc.
- Under what conditions was a key used
  - Type of client, hardware/software environment, etc.
- Key life cycle state changes
  - When and perhaps why a change was made
- A secure audit log is part of a good Key Management Service

Copyright © Landon Curt Noll & Cisco Systems, 2010.
All rights reserved. Permission for use by KMS2010.

Review: Too many keys problem

Image Credit:
Flickr user simplerich
Creative Commons License

- Key counts are exploding due to increased pressure from
  - An increased need for security
  - More and more products using cryptography
  - Increasing legal and industry requirements
  - More data, more devices, more people, more …
- Manually managing keys is annoying at best
  - Manual management is more subject to human error
  - Manual activity does not scale well
  - Automation through a Key Management Service is the key :-)

Copyright © Landon Curt Noll & Cisco Systems, 2010.
All rights reserved. Permission for use by KMS2010.

Review: The scaling problem

Image Credit:
Flickr user sylvia@intrigue
Creative Commons License

NOTE: Scale value is in 0.1 kg units

- Without automation, the explosion in key counts will increasingly result in:
  - Improper duplication of key values
  - Loss of encrypted data
  - Theft of keys and data
  - Stale or compromised keys not being rotated (replaced)
  - Failure of security and/or regulatory audits
  - More compromises of the integrity of critical applications
  - Companies making the headlines for the wrong reasons!

Copyright © Landon Curt Noll & Cisco Systems, 2010.
All rights reserved. Permission for use by KMS2010.

Review: Helping with the scaling problem

- Key Management Service helps with the scaling problem of managing an increasing number of keys

- A Good Key Management Service
  - Scales as the number of keys grows
  - Allows for consistent treatment of keys in keeping with best practices
  - Provides Audit logs,
    key inventory & accountability

Image Credit:
Flickr user stopnlook
Creative Commons License

Copyright © Landon Curt Noll & Cisco Systems, 2010.
All rights reserved. Permission for use by KMS2010.

Concept: Data Center Class Key Management

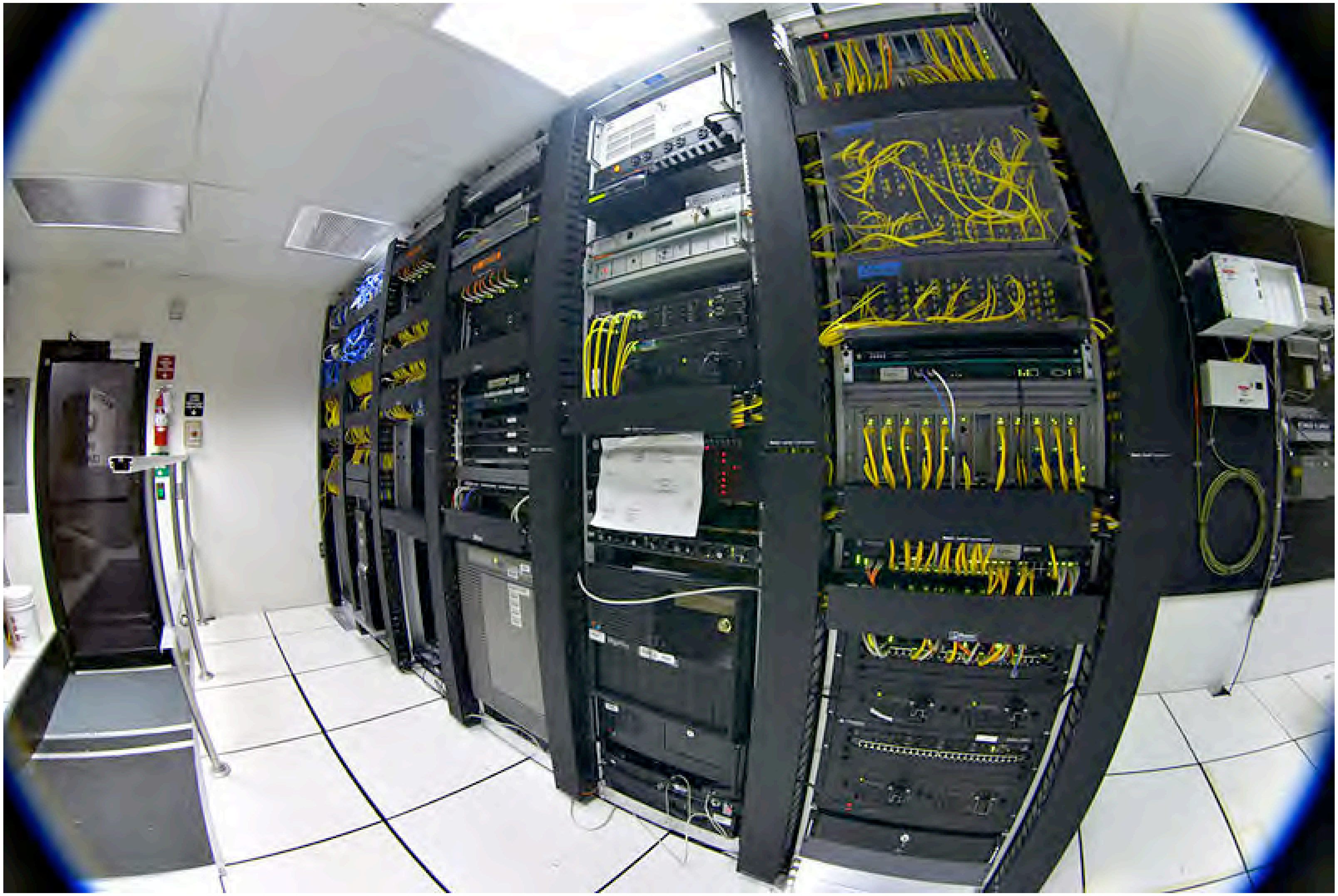


Image Credit:
Wikipedia
Creative Commons License

Copyright © Landon Curt Noll & Cisco Systems, 2010.
All rights reserved. Permission for use by KMS2010.

Concept: Key Management is a Authenticated Service

Image Credit:
Flickr user William Couch
Creative Commons License

- KM Client connects to a KM Server
  - Server found by a standard discovery protocol (e.g., DHCP), pre-configured, or uses hardware discovery
  - KM Server presents credentials when KM Client connects

- KM Client login to a KM Server
  - KM Client evaluates the KM Server’s credentials
  - KM Client presents credentials to the KM Server
    - The hard truth: entities must maintain one secret - their login credentials
    - KMS helps here with generation, backup storage, logs, key rotation
  - KM Client may use multiple KM Servers to improve service availability

Copyright © Landon Curt Noll & Cisco Systems, 2010.
All rights reserved. Permission for use by KMS2010.

Concept: Key Management is Session Based Request / Response protocol

- KM Client sends requests to the KM Server
  - KM Server evaluates the KM Client’s request
  - KM Server sends a response to the KM Client
- KM Clients may work synchronically or asynchronously
- Sessions may consist of multiple request / responses
- KM Client connection to KM Server may be terminated by either side
  - Termination by explicit request, policy, or communication failure

Copyright © Landon Curt Noll & Cisco Systems, 2010.
All rights reserved. Permission for use by KMS2010.

Concept: Key Management as a Distributed Network Service

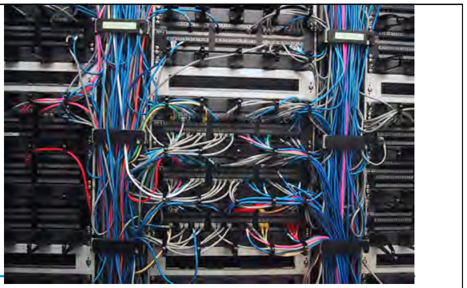


Image Credit:
Flickr user benben
Creative Commons License

- KM Servers work together to provide KM Clients a common service
- KM Clients to not have to know where a key resides
  - If a KM Server does not have a requested key, then it attempts to find the the key on behalf of the KM Client
    - Allows for one enterprise to request a key from another
    - KM Servers mutually authenticate (access policies control here)
- Complexity is pushed away from the KM client toward the KM Servers

Copyright © Landon Curt Noll & Cisco Systems, 2010.
All rights reserved. Permission for use by KMS2010.

Concept: Building a Highly Reliable and Available Data Center Service

Image Credit:
Flickr user skreuzer
Creative Commons License

- Keys are stored on multiple KM Servers
  - Multiple KM Servers per network
  - KM Server clusters are geographically distributed
- Key material is protected
  - Keys not stored in plain text
  - Client / Server protocol protected: nothing goes in the clear
  - KM Servers may use hardened master key storage methods
- Key Management disaster recovery
  - KM Servers push keys to failover KM Servers
  - When a disaster occurs, a KM Admin (or alarm) with appropriate credentials declares an emergency to able their use

Copyright © Landon Curt Noll & Cisco Systems, 2010.
All rights reserved. Permission for use by KMS2010.

Concept: Key points for a Sound Data Center Class Service

- KM Servers maintain key storage in a distributed encrypted database
- Multiple KM Servers per network
  - Load balancing, failover, etc.
- Keys never stored in the clear
  - Use of client side key wrapping can prevent KM Servers from knowing the value of the key
- Audit logging and key inventory
  - Trace use and provide accountability
  - Cryptographic data management

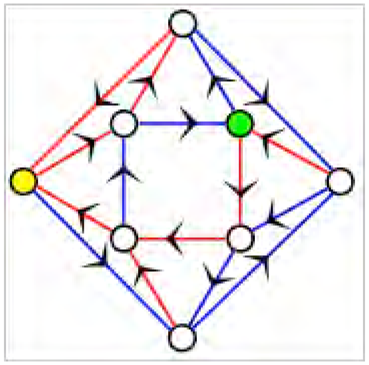


Image Credit:
Wikipedia
Creative Commons License

Copyright © Landon Curt Noll & Cisco Systems, 2010.
All rights reserved. Permission for use by KMS2010.

Need: The key importance of Standards

OASIS

IEEE 1619 SISWG
Security in Storage
Working Group

IEEE

1619
SISWG

A standards body
debating espresso standards?

Public domain photo of a coffee house in 1900
1900 = 1 B.E. (Before Espresso)

Copyright © Landon Curt Noll & Cisco Systems, 2010.
All rights reserved. Permission for use by KMS2010.

Need: OASIS KMIP and P1619.3

Image Credit:
Wikipedia
Creative Commons License

- Standards are complementary
  - KMIP focuses on the exchange protocol
  - P1619.3 focuses on the higher level architecture
  - P1619.3 / KMIP map shows no major disconnects
- Server to Server standards work critical for interoperability

Copyright © Landon Curt Noll & Cisco Systems, 2010.
All rights reserved. Permission for use by KMS2010.

Need: Grand unified interoperating product space

- Multiple KM clients and KM servers cooperate in the same data center
- Avoid lock-in to a single KM server vendor

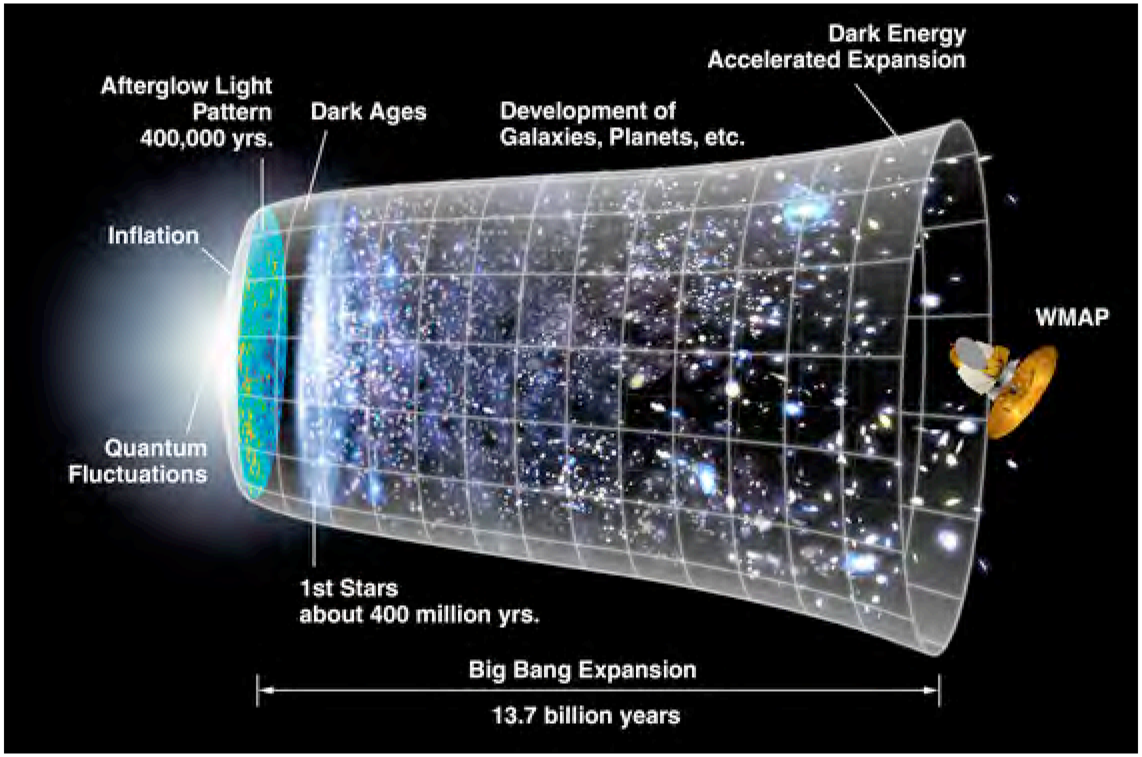


Image Credit:
Wikipedia
Creative Commons License

Copyright © Landon Curt Noll & Cisco Systems, 2010.
All rights reserved. Permission for use by KMS2010.

Thank you

- Questions? Comments? Flames? Artwork?

Image Credit:
Landon Curt Noll

Copyright © Landon Curt Noll & Cisco Systems, 2010.
All rights reserved. Permission for use by KMS2010.