SNIA NSF | NETWORKING STORAGE

Storage Networking Security Series: Key Management 101

Live Webcast

June 10, 2020

10:00 am PT

Today's Presenters

Judy Furlong
Distinguished Engineer
Dell Technologies

J Metz
Field CTO
Rockport Networks Inc.

SNIA-At-A-Glance

SNIA-at-a-Glance

185
industry leading organizations

2,000
active contributing members

50,000
IT end users & storage pros worldwide

Learn more: **snia.org/technical** **@SNIA**

Technologies We Cover

- Ethernet
- iSCSI
- NVMe-oF
- InfiniBand
- Fibre Channel, FCoE
- Hyperconverged (HCI)
- Storage protocols (block, file, object)
- Virtualized storage
- Software-defined storage

SNIA NSF | NETWORKING STORAGE

SNIA Legal Notice

- The material contained in this presentation is copyrighted by the SNIA unless otherwise noted.
- Member companies and individual members may use this material in presentations and literature under the following conditions:
  - Any slide or slides used must be reproduced in their entirety without modification
  - The SNIA must be acknowledged as the source of any material used in the body of any document containing material from these presentations.
- This presentation is a project of the SNIA.
- Neither the author nor the presenter is an attorney and nothing in this presentation is intended to be, or should be construed as legal advice or an opinion of counsel. If you need legal advice or a legal opinion please contact your attorney.
- The information presented herein represents the author's personal opinion and current understanding of the relevant issues involved. The author, the presenter, and the SNIA do not assume any responsibility or liability for damages arising out of any reliance on or use of this information.

  NO WARRANTIES, EXPRESS OR IMPLIED. USE AT YOUR OWN RISK.

Agenda

- Why is Key Management Important?
- Key Lifecycle
  - Concepts and Terminology
  - Symmetric vs. Asymmetric Key Management
- Local vs. Centralized Key Management
- Certificate Management and Validation
- Key Management in Action: TLS Example
- Conclusions

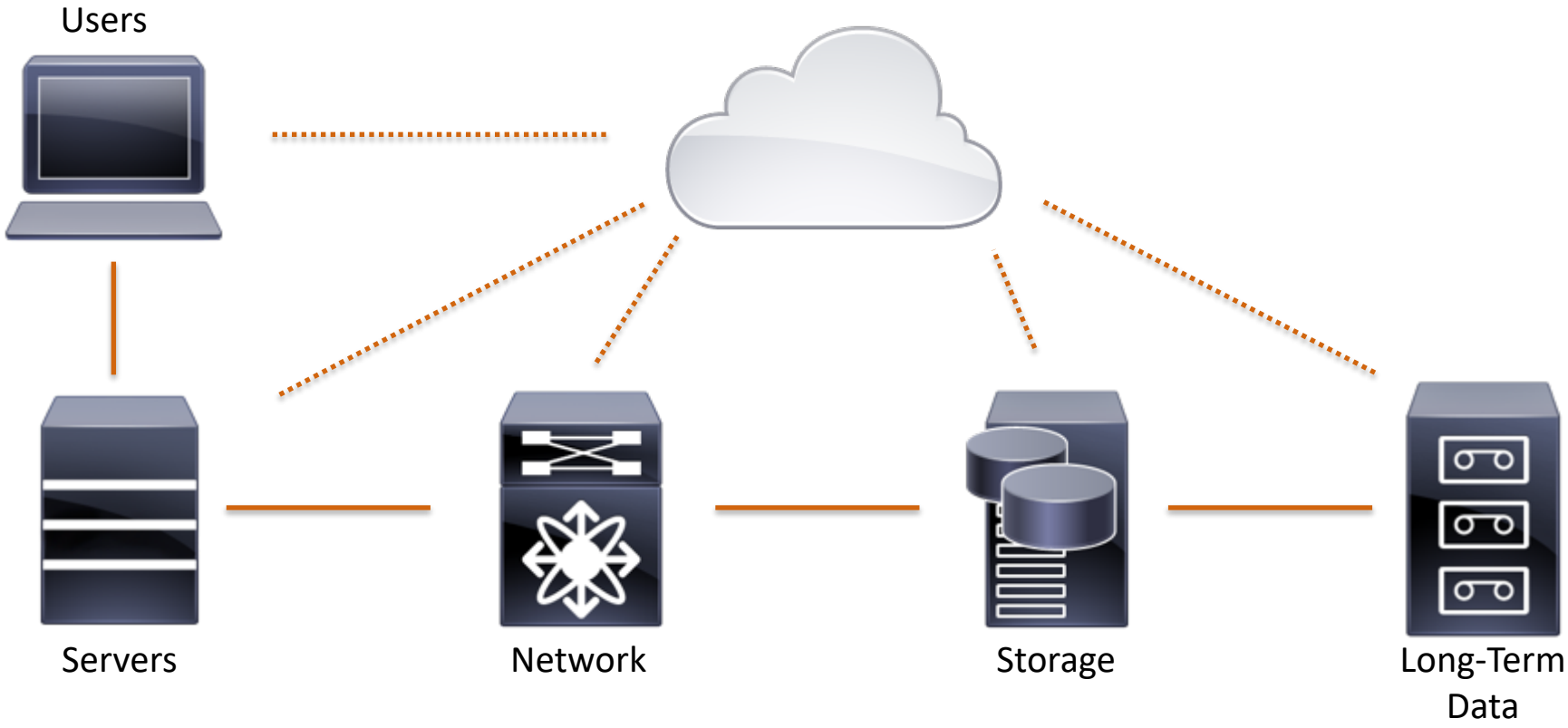
Why is Key Management Important?

Why is Key Management Important?

- Cryptographic keys make cryptographic functions unique
  - To effectively use cryptography to protect information one needs to protect the cryptographic keys
- Key management focuses on **protecting keys from threats** and **ensuring keys are available** when needed
- A lot goes into effective key management
  - Attention must be paid to how keys are handled throughout their lifecycle
  - Different approaches are taken based on the type of keys (symmetric vs. asymmetric) being managed
  - It should seamless integrate with the deployment model and architecture of an application/product

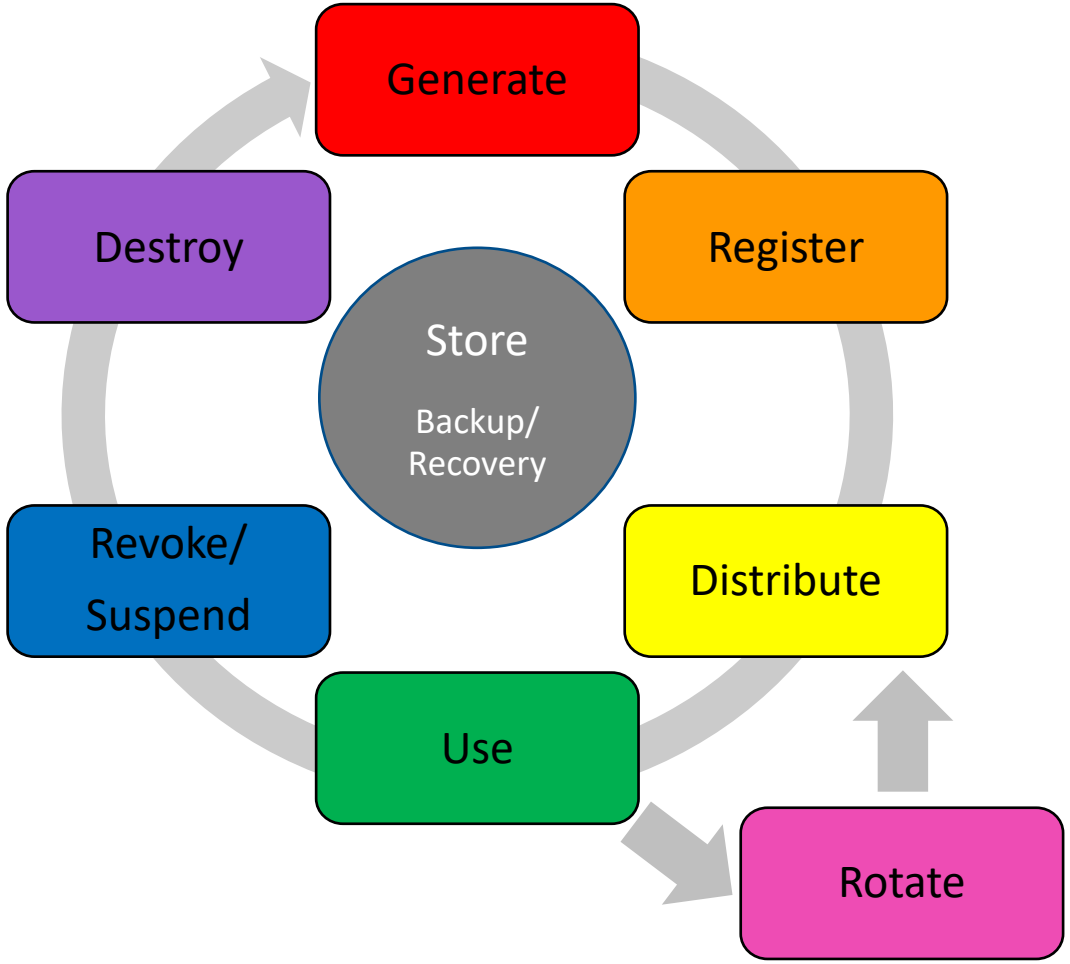
Key Management in the Big Picture

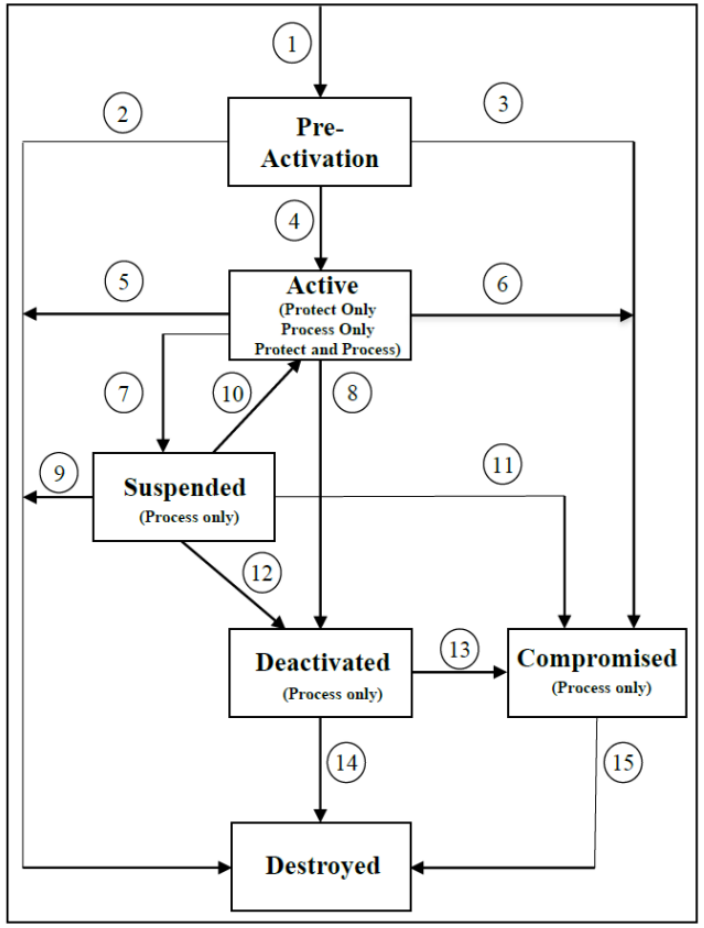
- Cryptography plays an important role in securing components and your architecture
- Key Management is essential to ensuring that cryptographic solutions are secure



Key Lifecycle

Key Lifecycle and Key State





Source:
NIST SP800-57
Part 1 Rev. 5

Key Generation

- Random Number Generations (RNGs) are leveraged to add unpredictability to key creation
- Generation location is important
  - Software vs. hardware
  - Validated cryptographic modules (e.g. FIPS 140)
- Understanding security strength
  - Amount work needed to break a cryptographic algorithm or system
  - Key strength based on algorithm, key size, generation process (RNG) and handling
    - Must be equal or greater than the data to be protected
    - Key strength recommendations found in NIST SP800-57 Part 1

Key Agreement and Key Derivation

Key Agreement

- Keys created using information contributed by two or more parties
- None of the parties can predetermine the key independent of the contributions of the other parties
- Example: Diffie-Hellman

Key Derivation

- Key is calculated from a secret or pre-shared key (e.g. from a key agreement exchange) combined with other information
- Examples: KBKDF, PBKDF2

Key Splitting

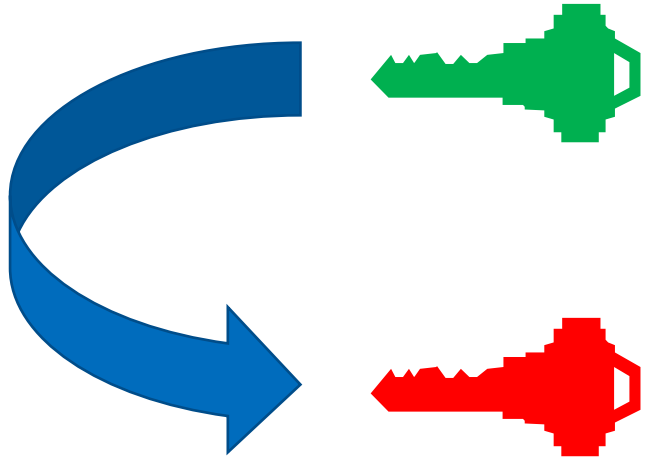
- Key is passed through an algorithm to create a set of mathematically related pieces (**key shares**)
  - Each key share provides no information about the original key
- M of N key shares need to be brought together to reconstitute the original key
- Uses
  - Protect a highly sensitive key (e.g. Root CA private key)
  - Automate access to a key
  - Multi-party/shared access
- Example: Shamir's Secret Sharing

Key Wrapping

- Encrypting one key with another in order to protect the (wrapped) key for distribution and/or storage
- KEK: Key Encryption Key
- DEK: Data Encryption Key
- MEK: Media Encryption Key

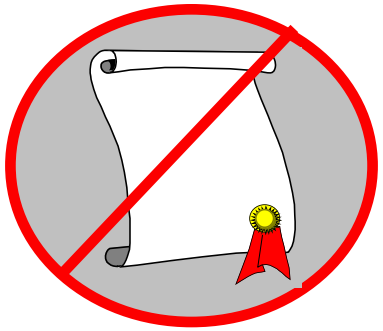
Rotation

- Cryptoperiod
  - The timeframe during which a cryptographic key is approved for use
- Validity
  - The timeframe of a certificate, during which the issuing CA guarantees to provide status of the certificate
- Rotation
  - Retiring a key from use and replacing it with a new key
  - May be referred to as Rekey
- Renewal
  - Replacing an old certificate with a new certificate



Compromise, Revocation, Suspension

- Compromise
  - Unauthorized disclosure, modification or substitution of a key
- Revocation
  - Notice that a key or certificate is being removed from use prior to the end of its cryptoperiod (or expiration date)
- Suspension
  - Temporarily removing a key or certificate from use prior to the end of its cryptoperiod (or expiration date)



- Compromised Key List
  - A list of keys that have been compromised (e.g. Black List)
- Certificate Revocation List (CRL)
  - A list of revoked, unexpired certificates issued by a Certification Authority (CA)
- OCSP Responder
  - Server which can be queried to provide the status of a certificate
  - OCSP defined in RFC 6960

Local vs. Centralized Key Management

Local vs Centralized Key Management

Local

- Key management supports single encryption solution
- Persistent key repository is located within encryption solution
- Backup and/or recovery of key repository is responsibility of encryption solution
- Administration of local key manager is integrated part of encryption solution
- Small scale
  - Number of keys in repository
  - Number of key policies being used/managed

Centralized

- Separate Key Manager that supports needs of multiple encryption solutions
  - Supports standard (e.g. KMIP) and/or proprietary protocols for communication with encryption solutions
- Persistent key repository is part of Key Manager
- Backup and/or recovery of key repository is a feature of the key manager
- Dedicated UI for administration of the Key Manager
- Large scale
  - Number of keys in repository
  - Number of key policies being used/managed
  - Number of encryption solutions supported

Anatomy of an Encryption Solution

Encryption Capability

Performs encryption/ decryption

Software or Hardware Based

(Optional) Local cache of essential cryptographic keys

Co-located with Encryption

Key Store (Cache)

Key Management

Local Key Manager

KM Client

Central Key Manager

Key Management Protocol (KMIP, Proprietary)

Provides full lifecycle management of encryption keys

May be co-located with Encryption or External

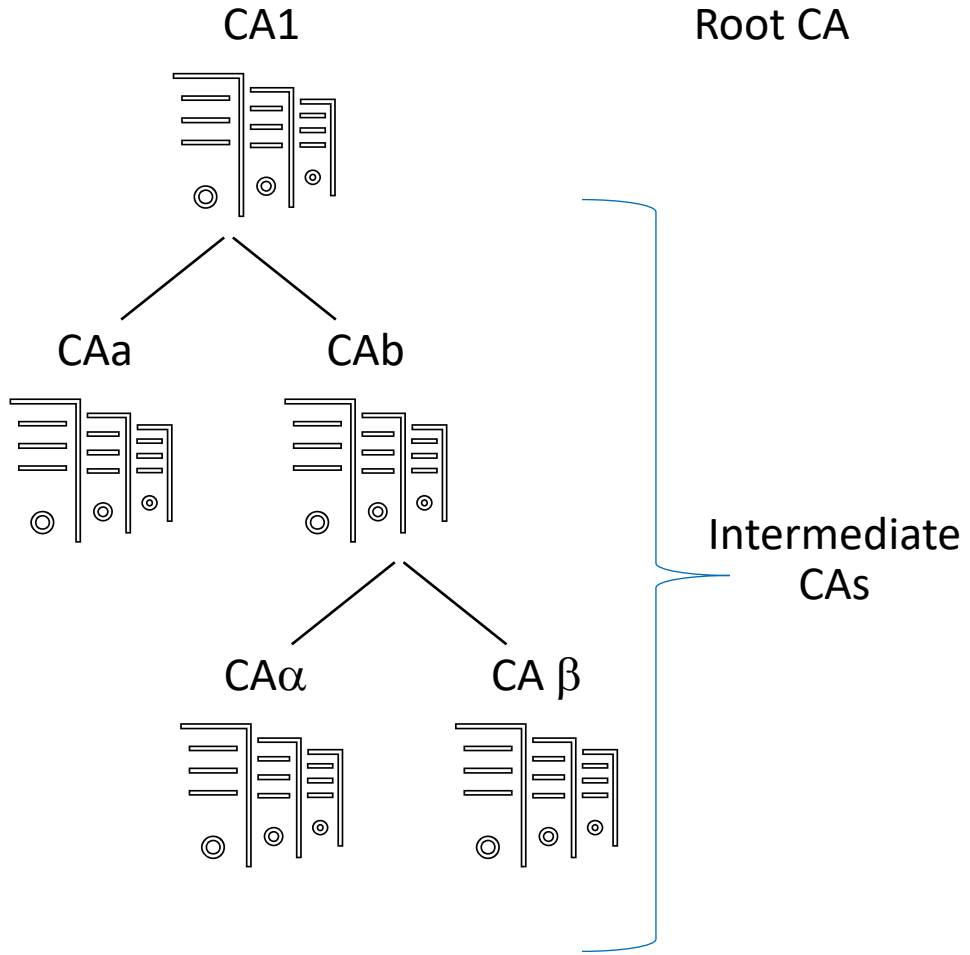
External server access via KMIP or proprietary protocol

[OASIS Key Management Interoperability Protocol (KMIP)]

Certificate Management and Validation

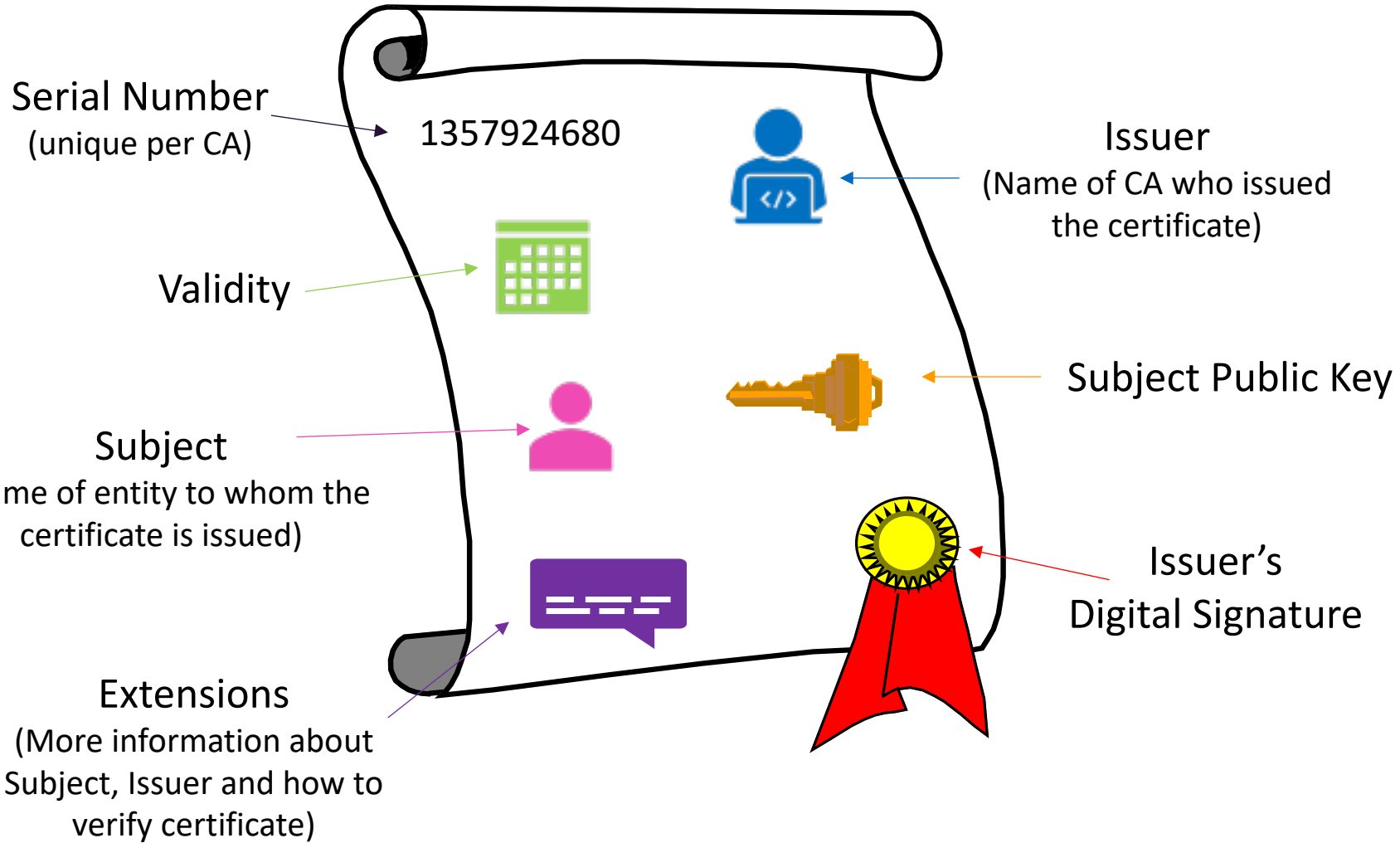
Public Key Infrastructure (PKI)

- (Public Key) Certificate
  - A digitally signed format which binds a public key to specific identity
- Certification Authority (CA)
  - A trusted entity that issues ***certificates*** which bind a public key to a specific identity
- Registration Authority (RA)
  - A trusted entity that establishes or vouches for the identity of the subject of a certificate
  - Normally a component of a CA
- PKI
  - A set of CAs responsible for issuing certificates for a specific environment (e.g. a company, a government agency, an application)



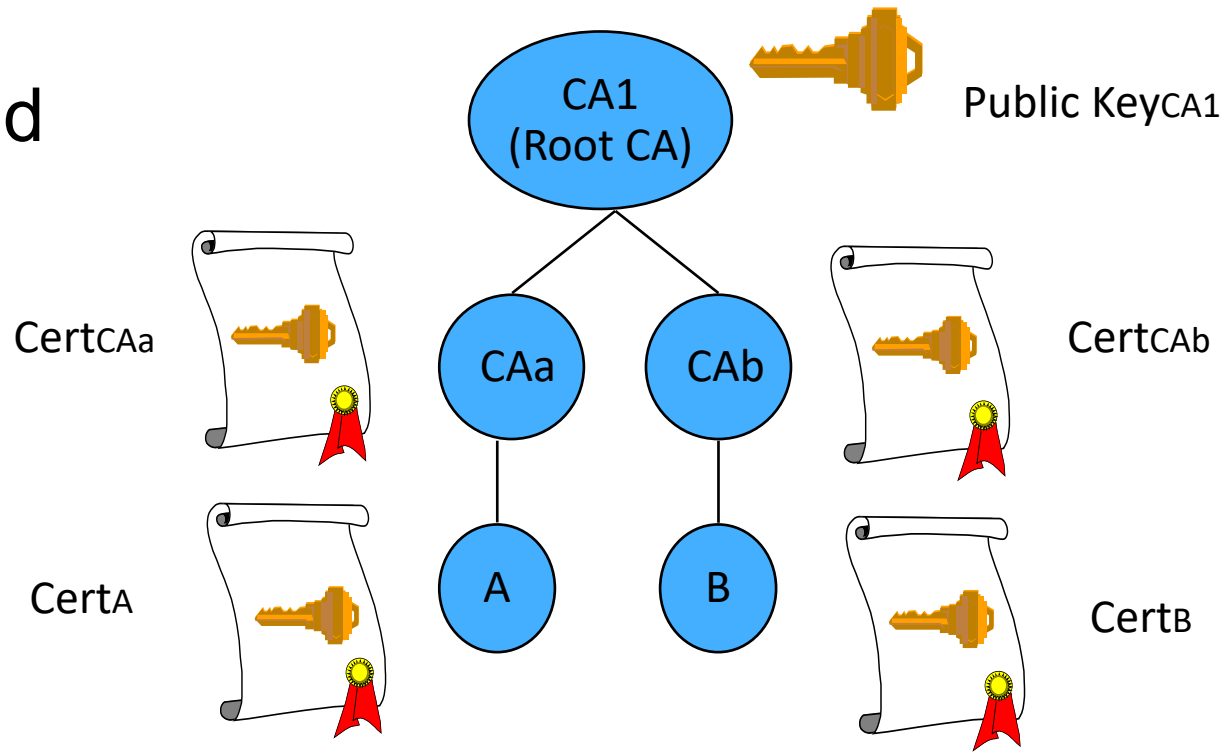
Anatomy of a Certificate

ITU-T X.509 (ISO/IEC 9594-8)
IETF PKIX - RFC 5280, RFC6818



Certification Path

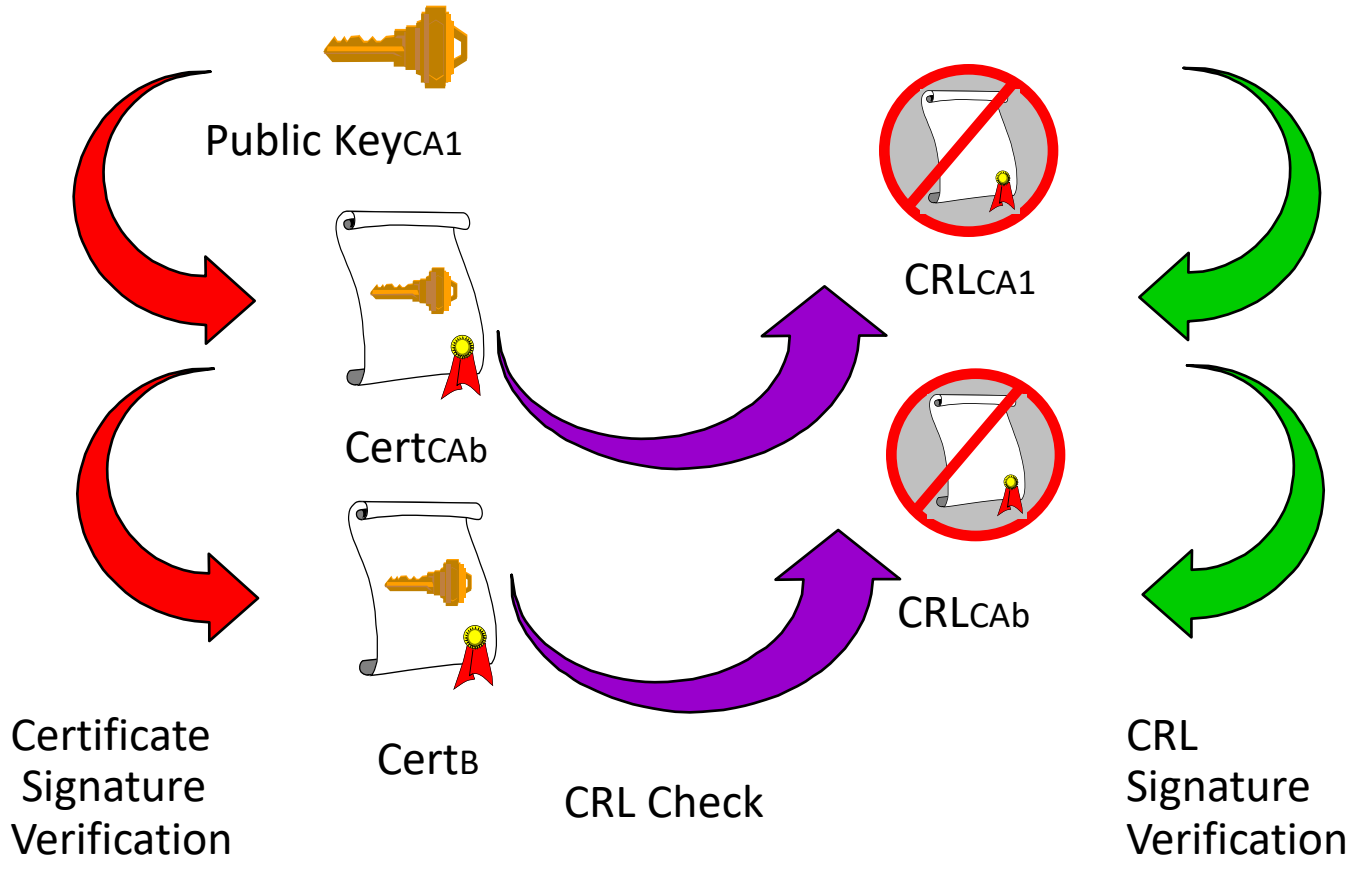
- An unbroken chain of trusted points between two parties
- Path from A to B
  - Includes CertB, CertCAb
  - Assume that A and B have Public KeyCA1



Certification Path Validation (CRLs)

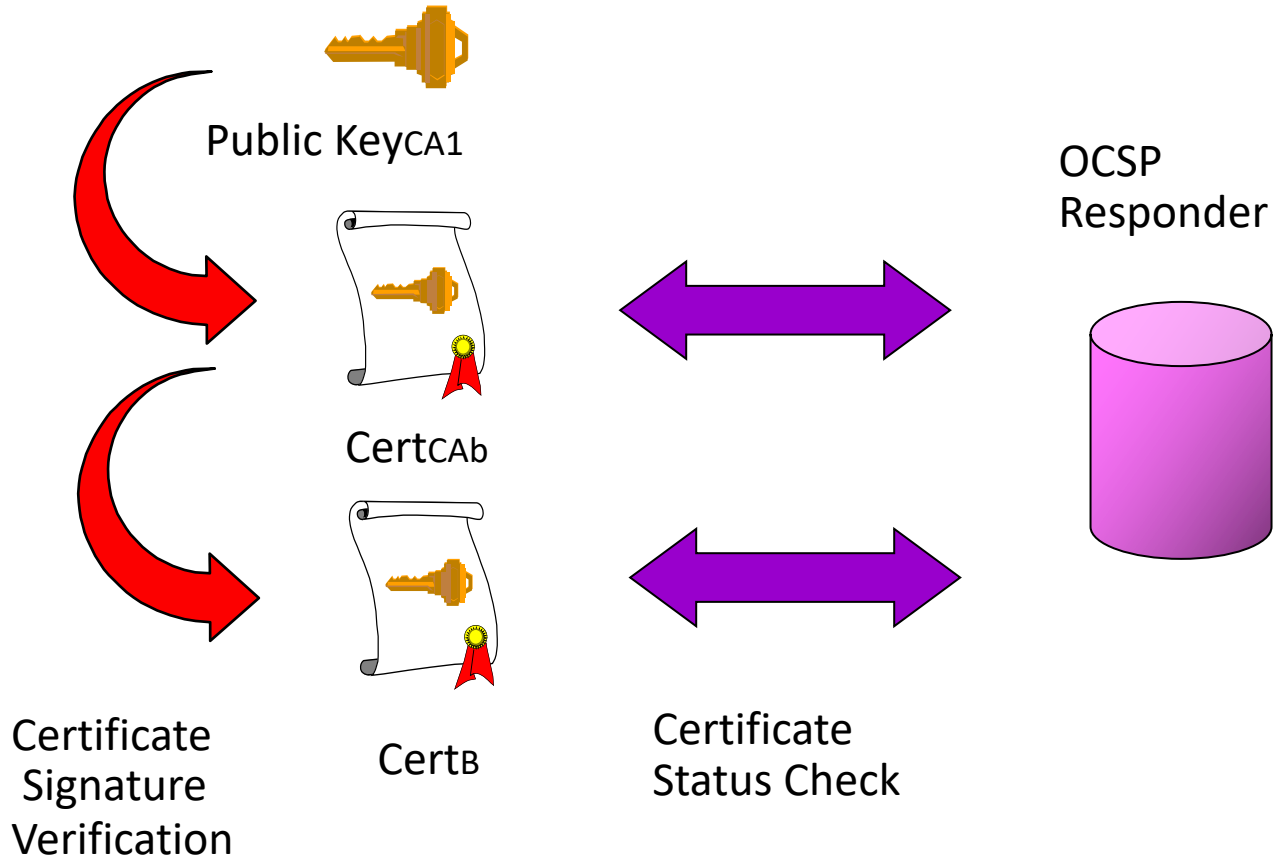
Key:

CA	Certification Authority
Cert	Certificate
CRL	Certificate Revocation List



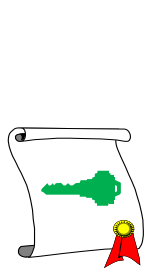
Certification Path Validation (OCSP)

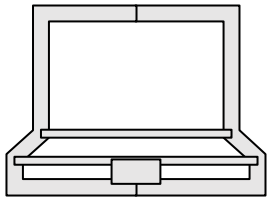
Key:	CA	Certification Authority
	Cert	Certificate
	OCSP	Online Certificate Status Protocol



Key Management in Action

Mutually Authenticated Transport Layer Security (TLS)

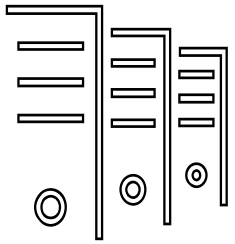




Client

1. Client Makes Connection to Server

2. Client and Server Negotiate Cipher Suite



Server

4. Client Verifies Server Certificate

3. Server Sends Certificate to Client

5. Client Sends Certificate and Pre-Master Secret to Server

6. Server Verifies Client Certificate

NOTE:
This diagram simplifies/combines steps in the TLS Handshake

7. Client and Server Derive Session Key

8. Encrypted Session Established

Conclusion

Conclusion

- Keys make cryptographic functions unique
- Key management focuses on protecting keys from threats and ensuring keys are available when needed
- Different approaches are taken for managing symmetric vs. asymmetric keys
- Key management needs to seamless integrate with the deployment model and architecture of a application/product
- Most applications/products incorporate multiple encryption and key management capabilities

More SNIA Security Resources

- Storage Networking Security Webcast Series: On-demand at the SNIA Educational Library: snia.org/educational-library
  - Understanding Storage Security and Threats
  - Protecting Data at Rest
  - Encryption 101
- Follow us on Twitter @SNIANSF for dates and times of others planned:
  - Applied Cryptography
  - Protecting Data in Transit
  - Securing the Protocol
  - Security Regulations
  - Securing the System: Hardening Methods
- SNIA Technical White Paper: Storage Security: Encryption and Key Management

After this Webcast

- Please rate this webcast and provide us with your feedback
- This webcast and a copy of the slides will be available at the SNIA Educational Library https://www.snia.org/educational-library
- A Q&A from this webcast, including answers to questions we couldn't get to today, will be posted on our blog at https://sniansfblog.org/
- Follow us on Twitter @SNIANSF

