Cryptography 101: From Theory to Practice

Chapter 16 – Key Management

Rolf Oppliger

March 14, 2023

Terms of Use

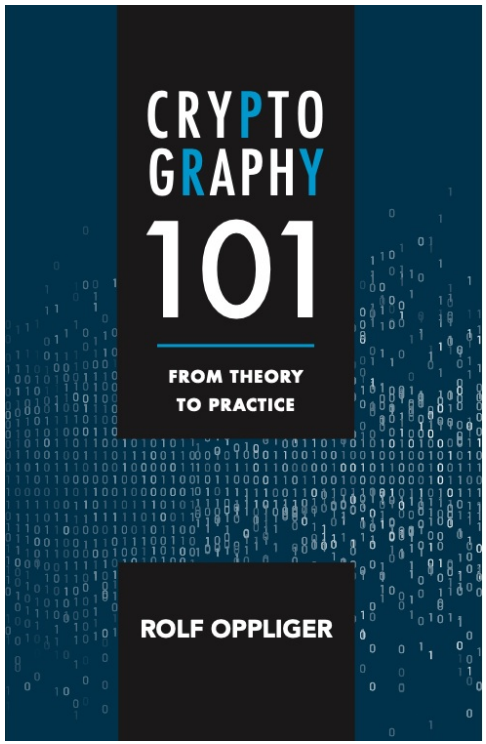
- This work is published with a CC BY-ND 4.0 license (cc by nd)
  - CC = Creative Commons (cc)
  - BY = Attribution (by)
  - ND = No Derivatives (nd)

whoami

rolf-oppliger.ch
rolf-oppliger.com

- Swiss National Cyber Security Centre NCSC (scientific employee)
- eSECURITY Technologies Rolf Oppliger (founder and owner)
- University of Zurich (adjunct professor)
- Artech House (author and series editor for information security and privacy)

Reference Book



ISBN 978-1-63081-846-3

`https://books.esecurity.ch/crypto101.html`

Challenge Me

Part IV

CONCLUSIONS

Outline

16. Key Management

16. Key Management

16. Key Management

16.1 Introduction

- According to RFC 4949, the term **key management** refers to "the process of handling and controlling cryptographic keys and related material (such as initialization values) during their life cycle in a cryptographic system, including ordering, generating, distributing, storing, loading, escrowing, archiving, auditing, and destroying the material"
- This process is complex and represents the Achilles' heel of all systems that employ cryptography (e.g., cryptocurrencies)
- Key generation, distribution, storage, and destruction are particularly challenging

16. Key Management

16.1 Introduction — Key generation

- Unless one is in the realm of unkeyed cryptosystems, the use of a cryptographic system always requires some keying material that needs to be generated in some way
- This requires the use of a random generator
- Either the random generator is used directly or it is used indirectly (e.g., to seed a PRG or a KDF)
- It is important to know and understand the realizations and implementations of random generators and PRGs
- The use of some ratcheting mechanisms may be needed

16. Key Management

16.1 Introduction — Key distribution

- If cryptographic keys are not generated where needed, they must be distributed in a secure way way
- It must be ensured that they are protected against passive and active attacks
- Some key establishment protocols are outlined in Chapter 12
- Many other protocols have been developed, proposed, implemented, and partly deployed in the field (including some home-grown and ad-hoc designs)

16. Key Management

16.1 Introduction — Key storage

- During its entire lifetime, a cryptographic key must be stored in a secure way
- This is particularly challenging for keys in actual use
- There are hardware-based or -supported solutions
  - Smartcards
  - Hardware security modules (HSMs)
  - Trusted platform modules (TPMs)
  - Trusted execution evironments (TEEs) and secure enclaves
  - ...
- Without hardware support, protecting a key that resides in memory is difficult and depends on the operating system

16. Key Management

16.1 Introduction — Key storage

- Stratgies to extract a key from memory
  - Try out all possible byte sequences (e.g., a 4GB memory has $4 \cdot 10^9 \approx 2^{48}$ possibilities)
  - Ignoring nonrandom-looking regions in memory
  - Exploiting the key schedule of the cipher in use
  - Exploiting the way the application stores keys (e.g., constant bit patterns as prefixes)
  - ...
- If there is no single place to securely store a key, then one may consider the use of secret splitting or sharing (see below)

16. Key Management

16.1 Introduction — Key destruction

- At the end of its life cycle, a cryptographic key may be archived and must be destroyed
- This is technically challenging (for all data stored electronically)
- The feasibility of recovering electronically stored data was demonstrated by the cold boot attack (and many follow-up attacks)
- Note that there may be (several) temporary copies of the key held in memory (shadow copies)

16. Key Management

16.2 Secret Sharing

- In some situations it may be useful to split a secret into multiple parts and have different parties manage them
- How to have n parties share a secret s
  - Randomly choose $n-1$ values $s_1, \ldots, s_{n-1}$
  - Compute $s_n = s \oplus s_1 \oplus \ldots \oplus s_{n-1}$
  - Distribute $s_1, \ldots, s_n$ to the n parties
- S can be recovered iff all n parties contribute their parts
- Such a **secret splitting system** requires all parties to be available and behave honestly

16. Key Management

16.2 Secret Sharing

- In 1979, Adi Shamir and George Blakley independently came up with the idea of secret sharing
- In a **secret sharing system**, it is not required that all parties are available and behave honestly
- Instead, the reconstruction of s requires only the parts of a well-defined subset of all parts (shares)
- Such a system allows a dealer to share s among a set P of n players, i.e., $P = \{P_1, \ldots, P_n\}$, such that only a qualified subset of P can reconstruct s from their shares

16. Key Management

16.2 Secret Sharing

Definition 16.1 (K-out-of-n secret sharing system)

A secret sharing system in which the access structure is

$$\Gamma = \{M \subseteq 2^P : |M| \geq k\}$$

- A k-out-of-n secret sharing system is **perfect** if $k-1$ players who collaborate (i.e., pool their shares) are not able to recover s or retrieve any useful information about s

16. Key Management

16.2 Secret Sharing — Shamir's System

- Shamir's system is perfect and based on polynomial interpolation
- It employs the fact that that a polynomial $f(x)$ of degree $k-1$ (over a field) can be uniquely interpolated from k points
- This means that a polynomial of degree 1 can be interpolated from 2 points, a polynomial of degree 2 can be interpolated from 3 points, and so on
- The respective interpolation algorithm is due to Lagrange

16. Key Management

16.2 Secret Sharing — Shamir's System

- Let

$$f(x) = r_0 + r_1 x + \ldots + r_{k-1} x^{k-1} = \sum_{i=0}^{k-1} r_i x^i \qquad (1)$$

be a polynomial of degree $k-1$ that passes through

$$(x_1, f(x_1) = y_1)$$
$$(x_2, f(x_2) = y_2)$$
$$\ldots$$
$$(x_k, f(x_k) = y_k)$$

16. Key Management

16.2 Secret Sharing — Shamir's System

- Lagrange's interpolating polynomial $P(x)$ is then given by

$$P(x) = \sum_{i=1}^{k} P_i(x)$$

where

$$P_i(x) = y_i \prod_{j=1; j \neq i}^{k} \frac{x - x_j}{x_i - x_j}$$

16. Key Management

16.2 Secret Sharing — Shamir's System

- Written explicitly,

$$
\begin{aligned}
P(x) &= P_1(x) + P_2(x) + \ldots + P_k(x) \\
&= y_1 \frac{(x-x_2)(x-x_3)\cdots(x-x_k)}{(x_1-x_2)(x_1-x_3)\cdots(x_1-x_k)} \\
&\quad + y_2 \frac{(x-x_1)(x-x_3)\cdots(x-x_k)}{(x_2-x_1)(x_2-x_3)\cdots(x_2-x_k)} \\
&\quad + \ldots \\
&\quad + y_k \frac{(x-x_1)(x-x_2)\cdots(x-x_{k-1})}{(x_k-x_1)(x_k-x_2)\cdots(x_k-x_{k-1})}
\end{aligned}
$$

16. Key Management

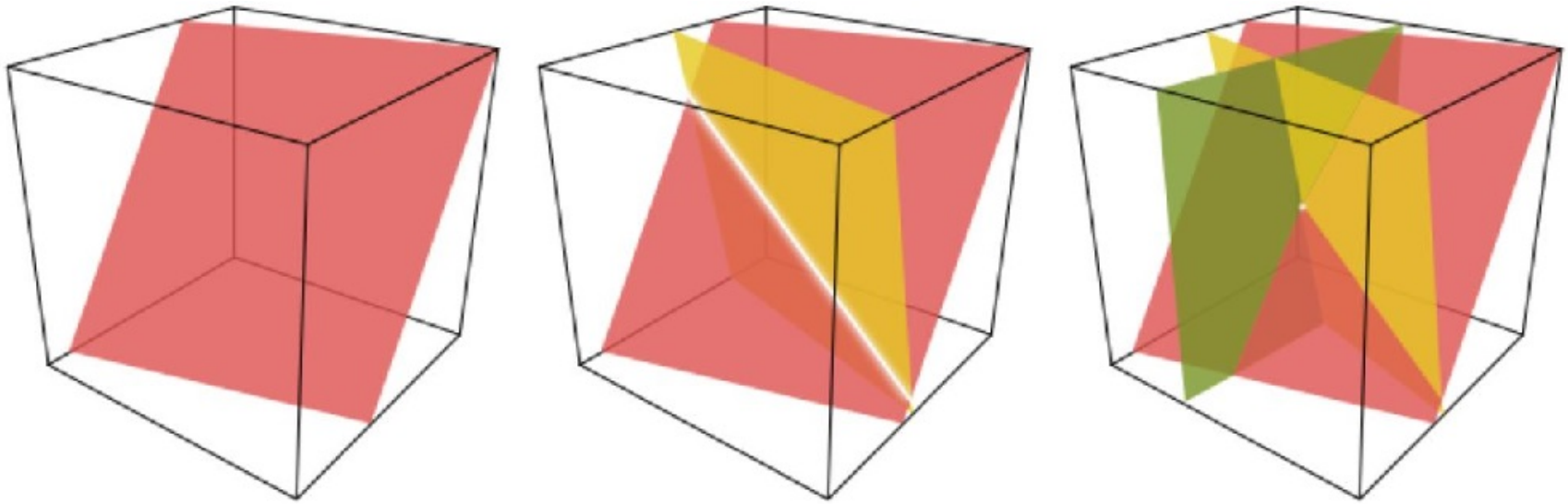
16.2 Secret Sharing — Shamir's System

- In Shamir's k-out-of-n secret sharing system, the secret (to be shared) represents the coefficient r_0
- The dealer randomly selects $k-1$ coefficients $r_1, \ldots, r_{k-1}$ to define a polynomial $f(x)$ of degree $k-1$
- For every player P_i, the dealer then assigns a fixed nonzero field element x_i and computes $y_i = f(x_i)$
- P_i's share is $(x_i, f(x_i))$
- Anybody who is given k shares can compute the secret r_0 by evaluating Lagrange's interpolating polynomial at zero, i.e., $r_0 = P(0)$

16. Key Management

16.2 Secret Sharing — Blakley's System

- Blakley's system is geometric (it is not perfect but can be modified to be so)



© A. Shamsoshoara, "Overview of Blakley's Secret Sharing Scheme," 2019

16. Key Management

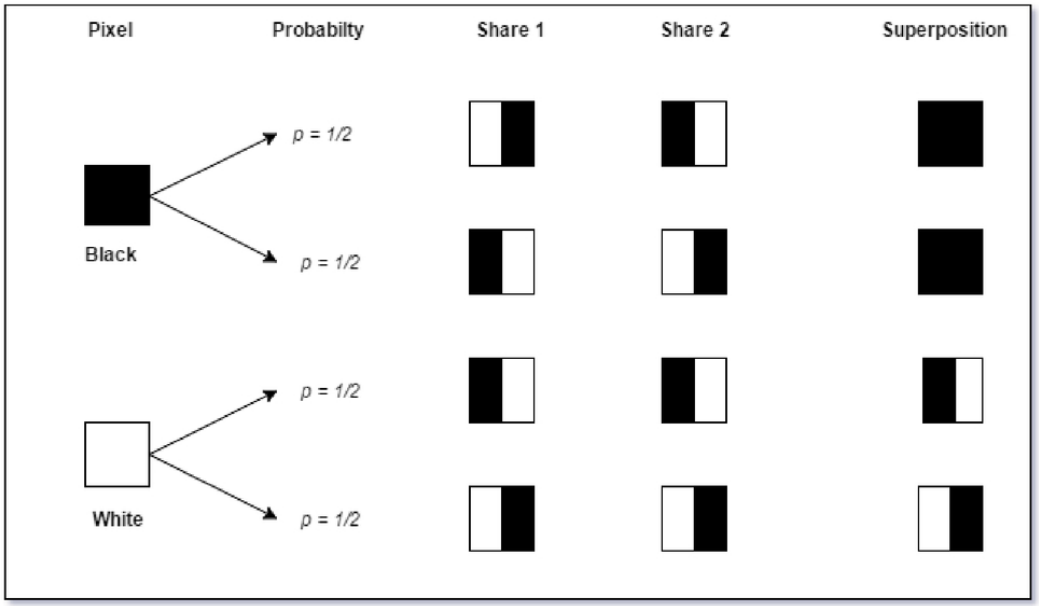
16.2 Secret Sharing

- K-out-of-n secret sharing systems are interesting from a theoretical viewpoint
- From a practical viewpoint, there are at least two problems
  - If a malicious player is not honest and provides a wrong share, then the secret that is reconstructed may be wrong
  - If the dealer is malicious or untrusted, the players may want to have a guarantee that they can put together the correct secret
- A **verifiable secret sharing system** may be needed here (so that the players can verify the shares)

16. Key Management

16.2 Secret Sharing

- In 1994, Moni Naor and Shamir proposed a visual variant of secret sharing known as **visual cryptography**



16. Key Management

16.3 Key Recovery

- If one uses cryptographic techniques for data encryption, then one may be concerned about the fact that keys get lost
- According to RFC 4949, the term **key recovery** refers to "a process for learning the value of a cryptographic key that was previously used to perform some cryptographic operation"
- Alternatively, it refers to "techniques that provide an intentional, alternate (i.e., secondary) means to access the key used for data confidentiality service"

16. Key Management

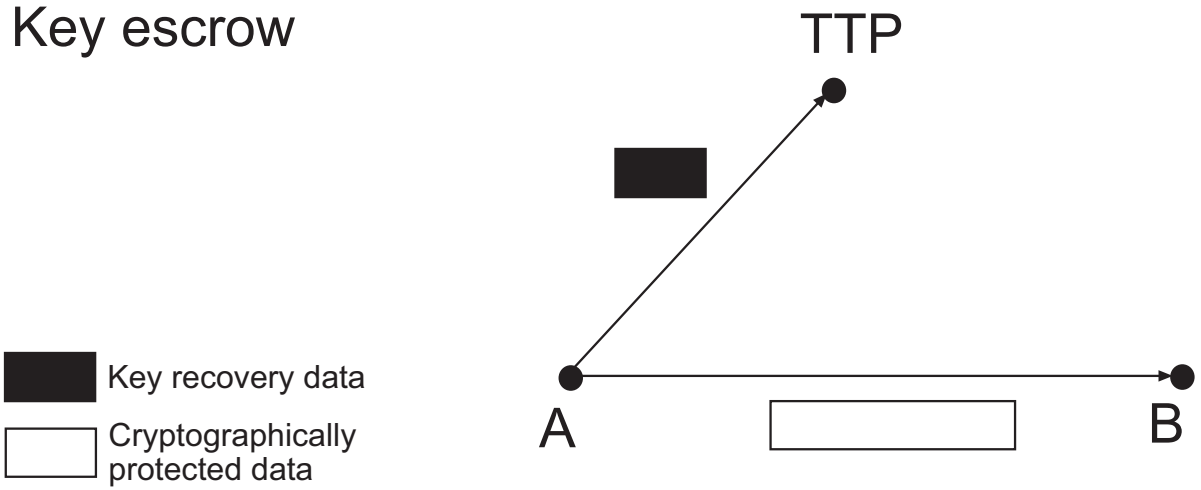
16.3 Key Recovery

- Classes of key recovery techniques
  - **Key escrow** is "a technique for storing knowledge of a cryptographic key or parts thereof in the custody of one or more third parties called escrow agents, so that the key can be recovered and used in specified circumstances"
  - **Key encapsulation** is "a technique for storing knowledge of a cryptographic key by encrypting it with another key and ensuring that only certain third parties called recovery agents can perform the decryption operation to retrieve the stored key"

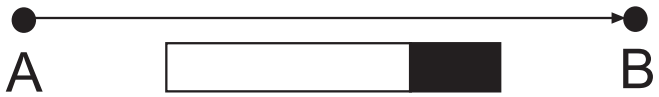
16. Key Management

16.3 Key Recovery

Key escrow



Key encapsulation



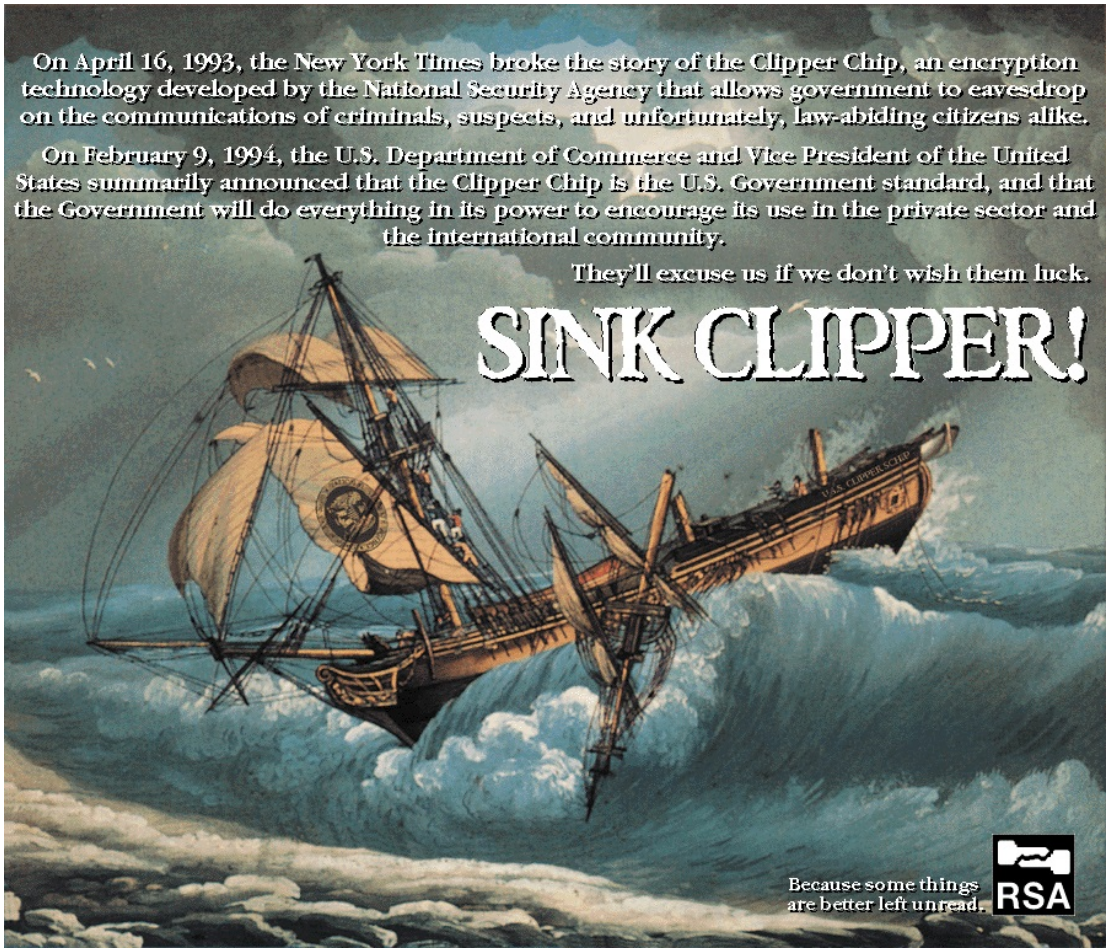
16. Key Management

16.3 Key Recovery

- Key recovery and key escrow became hotly debated topics in the mid-1990s, when the U.S. government published the **Escrowed Encryption Standard (EES)** and released the **Clipper Chip**
- It was a secret splitting system with two governmental bodies acting as escrow agents
- It was argued that key escrow on transmitted data is neither necessary nor particularly useful
- The controversy suddenly came to an end when it was shown that the original design of the EES was flawed

16. Key Management

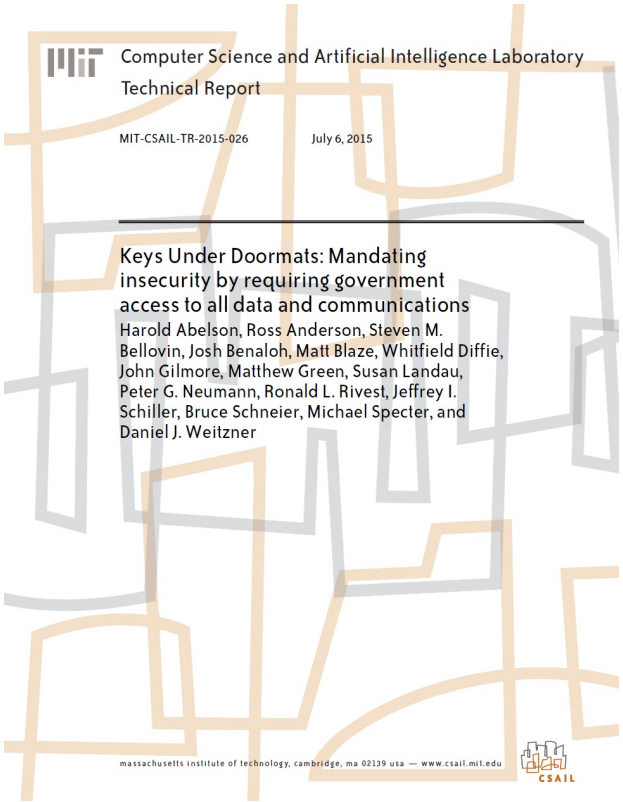
16.3 Key Recovery



16. Key Management

16.3 Key Recovery

- In 1997, a group of cryptographers wrote a paper about the risks related to key recovery, key escrow, and TTP encryption
- Today, the U.S. export controls are relaxed, but state-controlled cryptography prevails
- A follow-up paper appeared in 2015
- It can be used as starting point to discuss the Crypto Wars


Computer Science and Artificial Intelligence Laboratory
Technical Report

MIT-CSAIL-TR-2015-026 July 6, 2015

Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications

Harold Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael Specter, and Daniel J. Weitzner

massachusetts institute of technology, cambridge, ma 02139 usa — www.csail.mit.edu

CSAIL

16. Key Management

16.4 Certificate Management

- Most cryptographic technologies and protocols in use today employ public key cryptography and public key certificates
- According to RFC 4949, a **certificate** refers to "a document that attests to the truth of something or the ownership of something"
- In the realm of pubic key cryptography, the term (public key) certificate was coined by Loren M. Kohnfelder to refer to a digitally signed record holding a name and a public key (as a replacement for a public file)
- There are also attribute certificates

16. Key Management

16.4 Certificate Management

- Public key ertificates are issued by **certification authorities (CAs)**, whereas attribute certificates are issued by **attribute authorities (AAs)**
- A CA and an AA may be the same organization
- Also, a CA can have one or several **registration authorities (RAs)** — sometimes called **local registration authorities** or **local registration agents (LRAs)**
- The certificates generated by the CAs may be made available in online directories or certificate repositories

16. Key Management

16.4 Certificate Management

- According to RFC 4949, a **public key infrastructure (PKI)** is "a system of CAs that perform some set of certificate management, archive management, key management, and token management functions for a community of users," that employ public key cryptography
- As such, it is as an infrastructure that can be used to issue, validate, and revoke public keys and public key certificates
- It comprises a set of agreed-upon standards, CAs, structures among multiple CAs, methods to discover and validate certification paths, operational and management protocols, interoperable tools, and supporting legislation

16. Key Management

16.4 Certificate Management

- In the past, PKIs have experienced a great deal of hype, and many companies and organizations have started to provide certification services on a commercial basis
- Most of these service providers have failed to become commercially successful
- In fact, the PKI business has turned out to be particularly difficult to make a living from
- There are only a few CAs that are self-feeding, and most CAs have other sources of revenue

16. Key Management

16.4 Certificate Management

- Many standardization bodies are working in the field
- Most importantly, the Telecommunication Standardization Sector of the International Telecommunication Union (ITU-T) has released a recommendation (ITU-T X.509)
- ITU-T X.509 has been adopted by many other standardization bodies, including the International Organization for Standardization (ISO) and International Electrotechnical Committee (IEC) Joint Technical Committee 1 (JTC1) and the IETF PKIX WG
- There are only a few alternatives to X.509 certificates, such as PGP certificates and SDSI/SPKI

16. Key Management

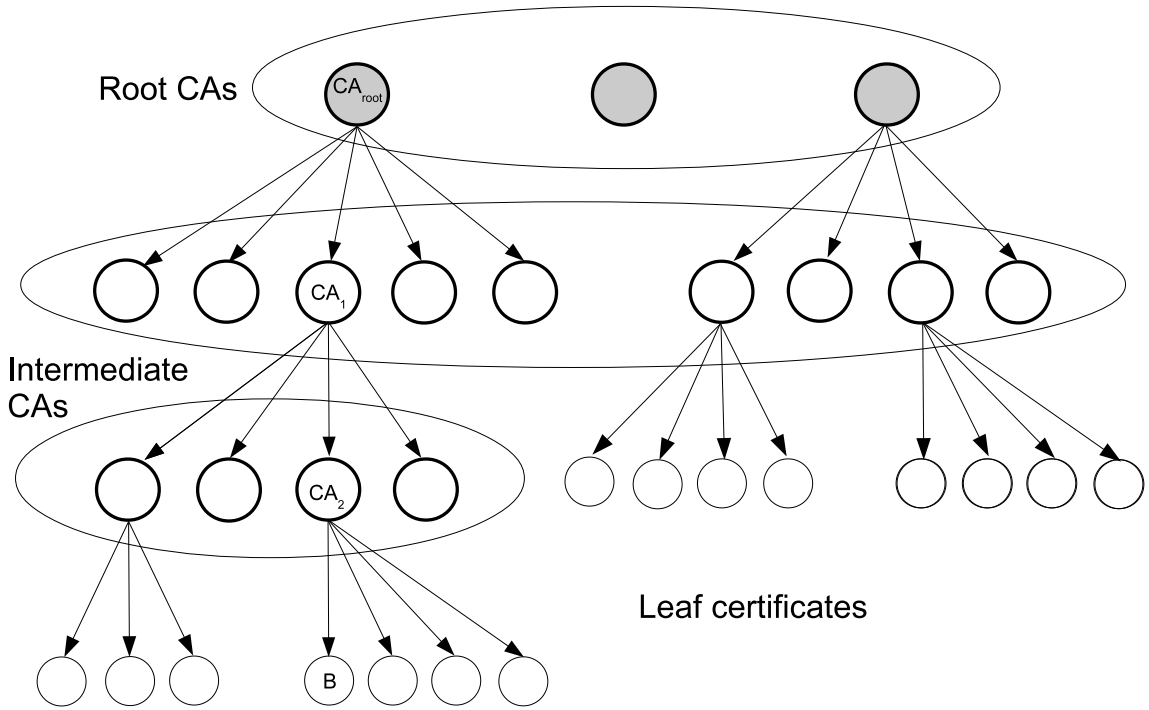
16.4 Certificate Management

- An X.509 (version 3) certificate may have several fields
  - Version
  - Serial number
  - Algorithm ID
  - Issuer
  - Validity
  - Subject
  - Subject Public Key Info
  - Issuer Unique Identifier
  - Subject Unique Identifier
  - Extensions

16. Key Management

16.4 Certificate Management

- X.509 certificates are based on the hierarchical trust model



16. Key Management

16.4 Certificate Management

- Challenges in public key certification
  - Naming
  - ASN.1 and encoding rules (i.e., BER or DER)
  - Management of root CAs
  - Certificate path validation
  - Certificate revocation and misuse detection(e.g., CRL, OCSP ± stapling, Certificate Transparency, CAA/DANE, . . .)
- PKI technologies have only been successful, if they are put in place and used in stealth mode (e.g., invisible to the user)

16. Key Management

16.5 Final Remarks

- Key management is complex and the Achilles' heel of almost every system that employs cryptographic techniques
- This is also true if data is stored in the cloud (i.e., BYOK, CYOK, or HYOK)
- The key life cycle includes many important phases, such as key generation, distribution, storage, and destruction
- Secret splitting and sharing, as well as key recovery yield important technologies
- Certificate management is a topic of its own

Questions and Answers

Thank you for your attention