# Key Management and Authentication

Daniel Bosk

Department of Information and Communication Systems,
Mid Sweden University, SE-851 70 Sundsvall.

keyauth.tex 2012 2014-10-01 08:26:03Z danbos

Mittuniversitetet
MID SWEDEN UNIVERSITY

# Overview

1. Symmetric Key Distribution
   - Symmetric Crypto
   - Key Distribution Centre (KDC)
   - Authentication
   - Kerberos IV
   - Kerberos V
2. Asymmetric Key Distribution
   - Asymmetric Crypto and Hash Functions
   - Diffie–Hellman Key Exchange
   - Public-key Certificates
3. Federated Identity Management
   - Identity Management
   - Identity Federation

# Symmetric Crypto

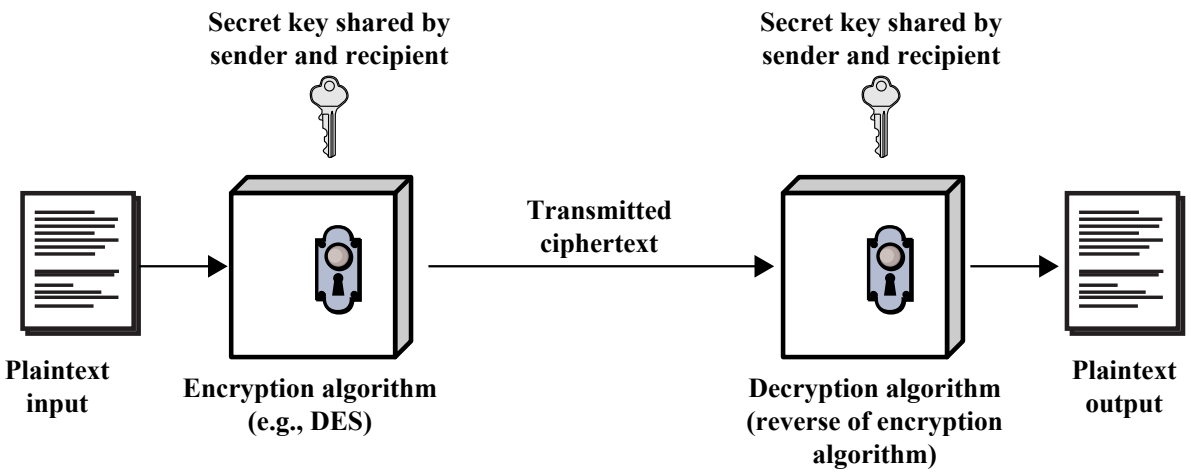



Figure: An overview of symmetric crypto. Image: [Sta13].

# Key Distribution Centre (KDC)

- Deliver a key $k$ from $A$ to $B$. By themselves or third party.
- If $A$ and $B$ share a key $k$, generate a key $k'$ and transmit it using $k$: $A \rightarrow B : E_k(k')$.
- Secure connection to third party $C$, $C$ delivers key to $A$ and $B$.

# Key Distribution Centre (KDC)

**Session Key** Temporary key used between $A$ and $B$.

**Permanent Key** Key used to distribute session keys.

**Key Distribution Centre** The central entity with which permanent keys are shared and by whom session keys are generated.

# Authentication

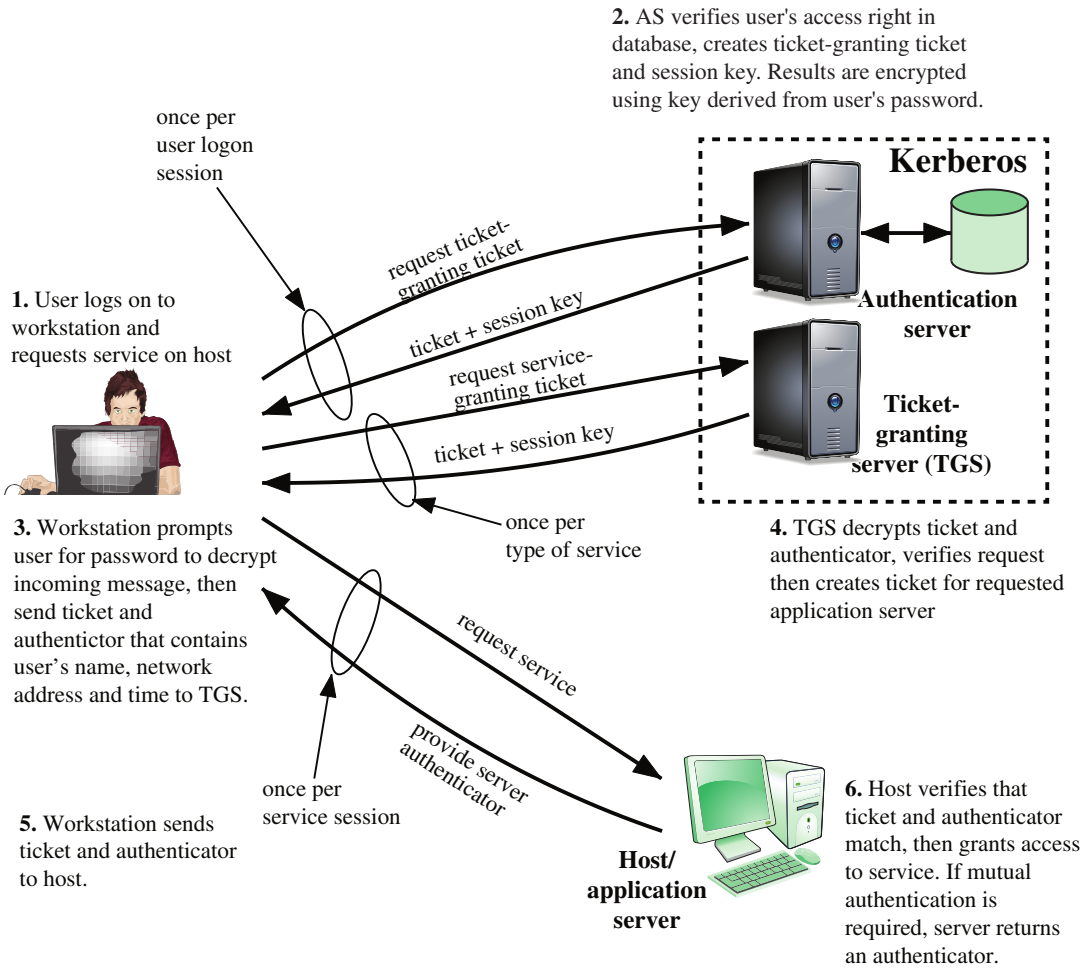



Figure: An overview of Kerberos. Image: [Sta13].

Mittuniversitetet
MID SWEDEN UNIVERSITY

# Kerberos IV

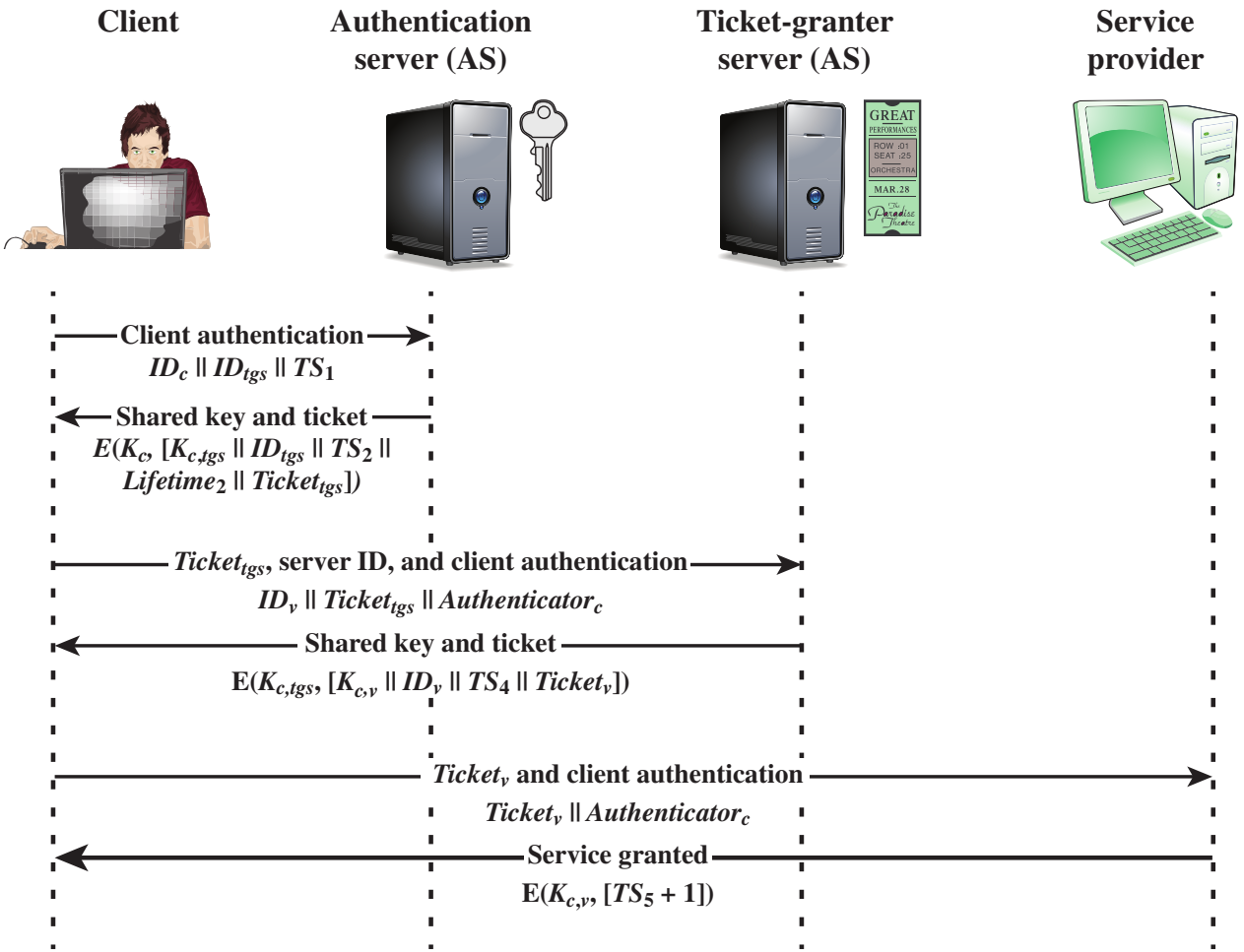



Figure: An overview of Kerberos IV authentication dialogue. Image: [Sta13].

# Kerberos IV

(1) C → AS $ID_c \| ID_{tgs} \| TS_1$

(2) AS → C $E(K_c, [K_{c,tgs} \| ID_{tgs} \| TS_2 \| Lifetime_2 \| Ticket_{tgs}])$

$Ticket_{tgs} = E(K_{tgs}, [K_{c,tgs} \| ID_C \| AD_C \| ID_{tgs} \| TS_2 \| Lifetime_2])$

(a) Authentication Service Exchange to obtain ticket granting ticket

(3) C → TGS $ID_v \| Ticket_{tgs} \| Authenticator_c$

(4) TGS → C $E(K_{c,tgs}, [K_{c,v} \| ID_v \| TS_4 \| Ticket_v])$

$Ticket_{tgs} = E(K_{tgs}, [K_{c,tgs} \| ID_C \| AD_C \| ID_{tgs} \| TS_2 \| Lifetime_2])$

$Ticket_v = E(K_v, [K_{c,v} \| ID_C \| AD_C \| ID_v \| TS_4 \| Lifetime_4])$

$Authenticator_c = E(K_{c,tgs}, [ID_C \| AD_C \| TS_3])$

(b) Ticket Granting Service Exchange to obtain service granting ticket

(5) C → V $Ticket_v \| Authenticator_c$

(6) V → C $E(K_{c,v}, [TS_5 + 1])$ (for mutual authentication)

$Ticket_v = E(K_v, [K_{c,v} \| ID_C \| AD_C \| ID_v \| TS_4 \| Lifetime_4])$

$Authenticator_c = E(K_{c,v}, [ID_C \| AD_C \| TS_5])$

(c) Client/Server Authentication Exchange to obtain service

Figure: Kerberos IV authentication protocol. Image: [Sta13].

Mittuniversitetet
MID SWEDEN UNIVERSITY

# Kerberos V

(1) C → AS $Options \| ID_c \| Realm_c \| ID_{tgs} \| Times \| Nonce_1$

(2) AS → C $Realm_c \| ID_C \| Ticket_{tgs} \| E(K_c, [K_{c,tgs} \| Times \| Nonce_1 \| Realm_{tgs} \| ID_{tgs}])$

$Ticket_{tgs} = E(K_{tgs}, [Flags \| K_{c,tgs} \| Realm_c \| ID_C \| AD_C \| Times])$

(a) Authentication Service Exchange to obtain ticket granting ticket

(3) C → TGS $Options \| ID_v \| Times \| \| Nonce_2 \| Ticket_{tgs} \| Authenticator_c$

(4) TGS → C $Realm_c \| ID_C \| Ticket_v \| E(K_{c,tgs}, [K_{c,v} \| Times \| Nonce_2 \| Realm_v \| ID_v])$

$Ticket_{tgs} = E(K_{tgs}, [Flags \| K_{c,tgs} \| Realm_c \| ID_C \| AD_C \| Times])$

$Ticket_v = E(K_v, [Flags \| K_{c,v} \| Realm_c \| ID_C \| AD_C \| Times])$

$Authenticator_c = E(K_{c,tgs}, [ID_C \| Realm_c \| TS_1])$

(b) Ticket Granting Service Exchange to obtain service granting ticket

(5) C → V $Options \| Ticket_v \| Authenticator_c$

(6) V → C $E_{K_{C,V}} [ TS_2 \| Subkey \| Seq\# ]$

$Ticket_v = E(K_v, [Flags \| K_{c,v} \| Realm_c \| ID_C \| AD_C \| Times])$

$Authenticator_c = E(K_{c,v}, [ID_C \| Realm_c \| TS_2 \| Subkey \| Seq\#])$

(c) Client/Server Authentication Exchange to obtain service

Figure: Kerberos V authentication protocol. Image: [Sta13].

Mittuniversitetet
MID SWEDEN UNIVERSITY

# Kerberos V

## Environmental Differences

- Encryption system dependence.
- Internet protocol dependence.
- Byte ordering.
- Ticket lifetime.
- Authentication forwarding.
- Interrealm authentication.

# Kerberos V
## Technical differences

- Double encryption.
- Propagating Cipher Block Chaining instead of CBC.
- Session and subsession keys.
- Password attacks.

# Asymmetric Crypto and Hash Functions

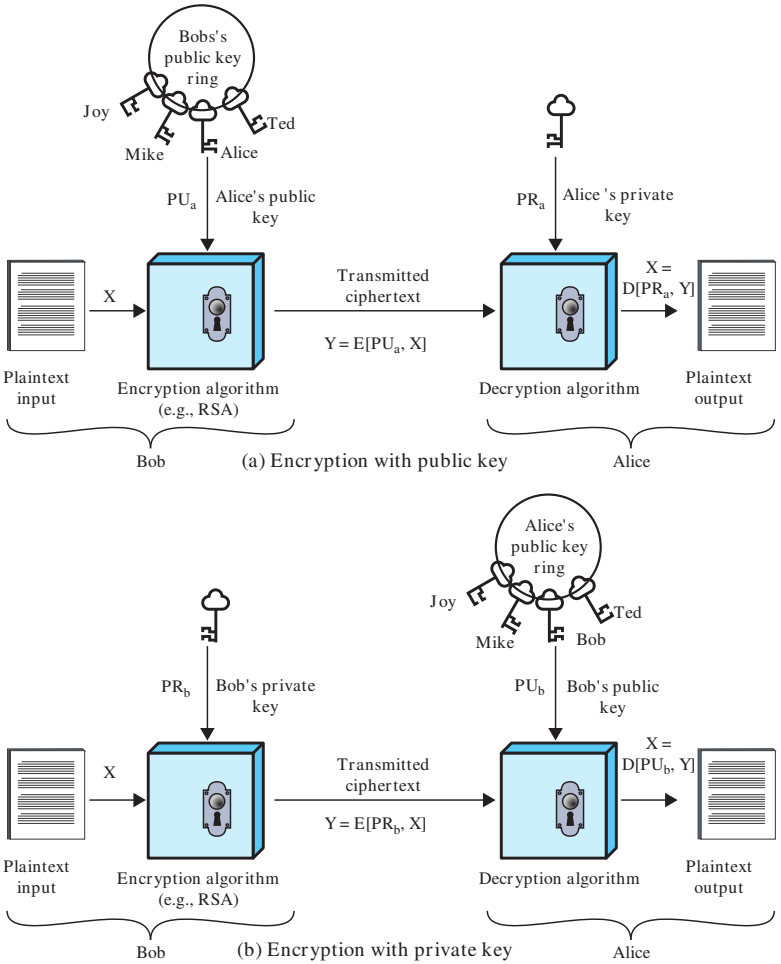



Figure: An overview of asymmetric crypto. Image: [Sta13].

# Asymmetric Crypto and Hash Functions

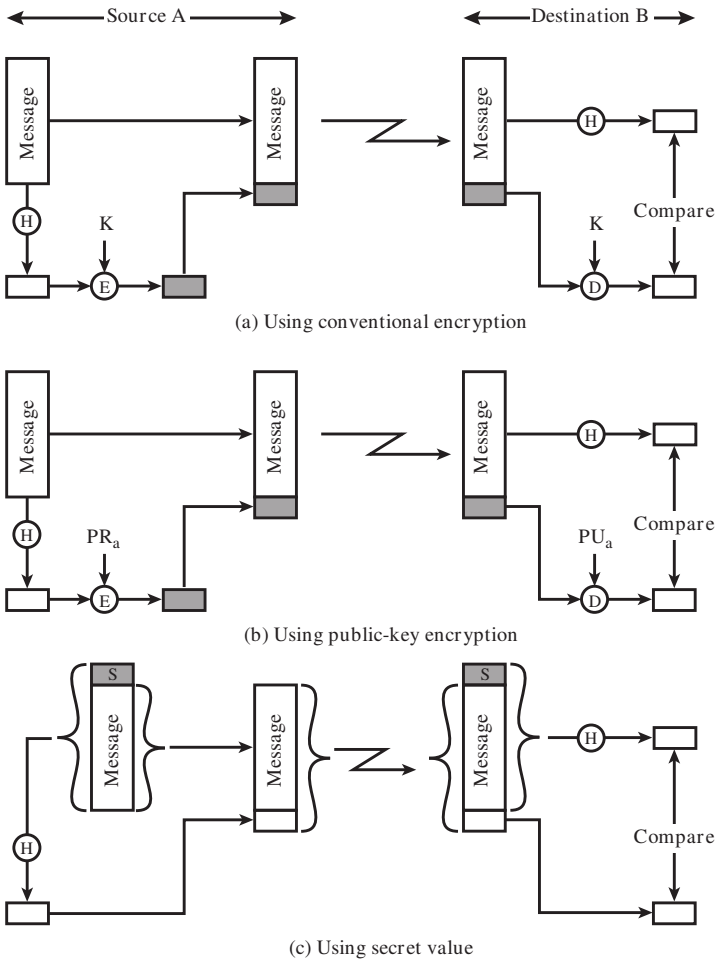



Figure: An overview of using hash functions for message integrity and authentication. Image: [Sta13].

Mittuniversitetet
MID SWEDEN UNIVERSITY

# Diffie–Hellman Key Exchange

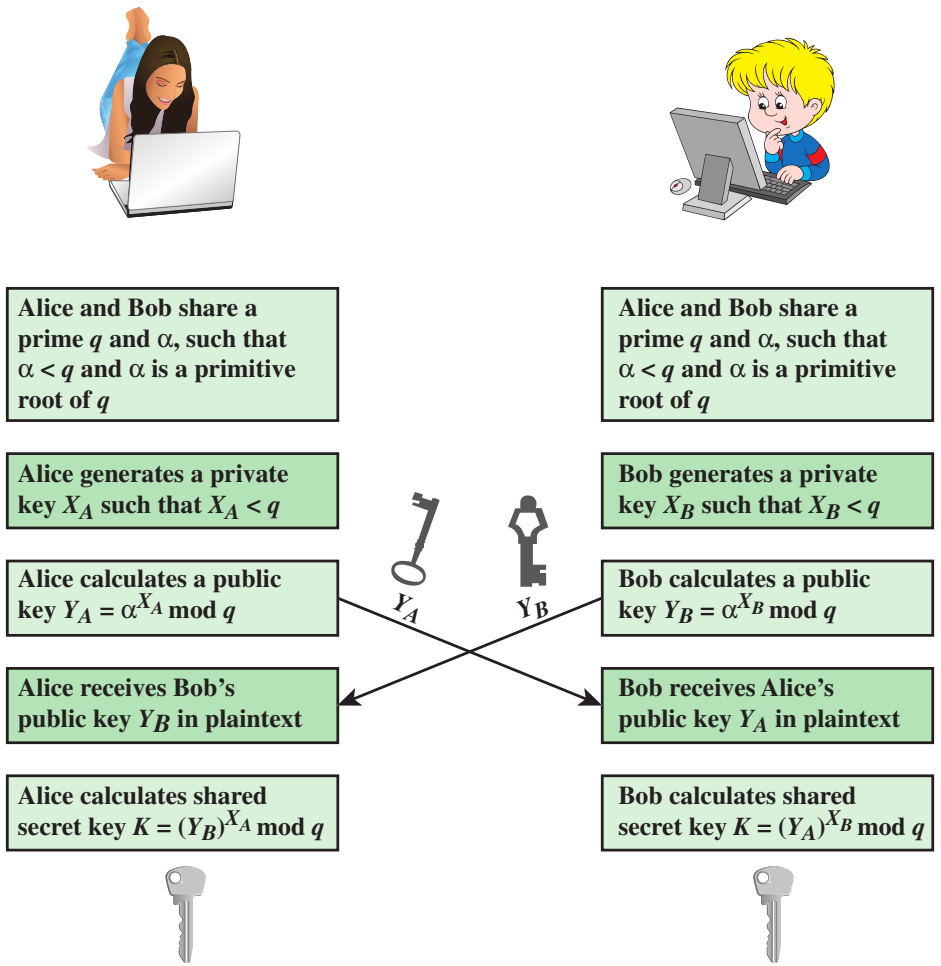



Figure: A schematic overview of the Diffie–Hellan Key Exchange algorithm. Image: [Sta13].

Mittuniversitetet
MID SWEDEN UNIVERSITY

# Diffie–Hellman Key Exchange

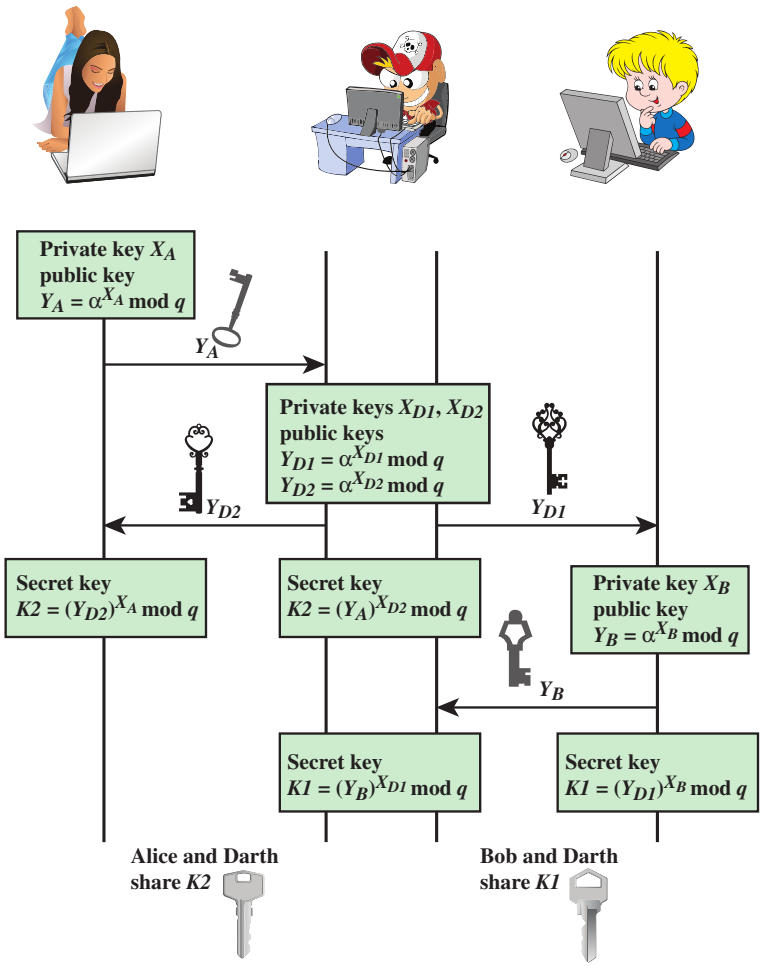



Figure: Schematic overview of a Man-in-the-Middle Attack. Image: [Sta13].

# Public-key Certificates

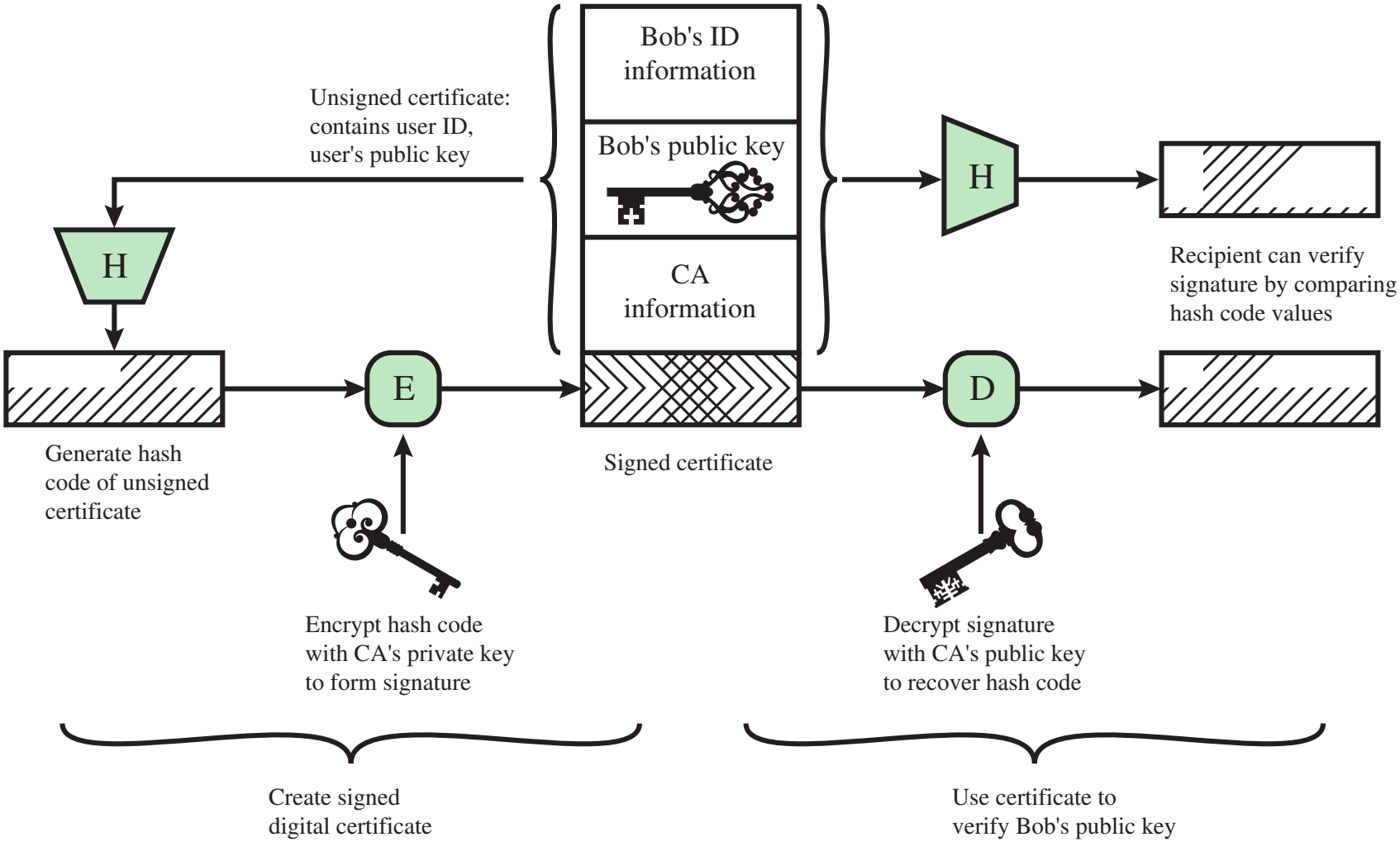
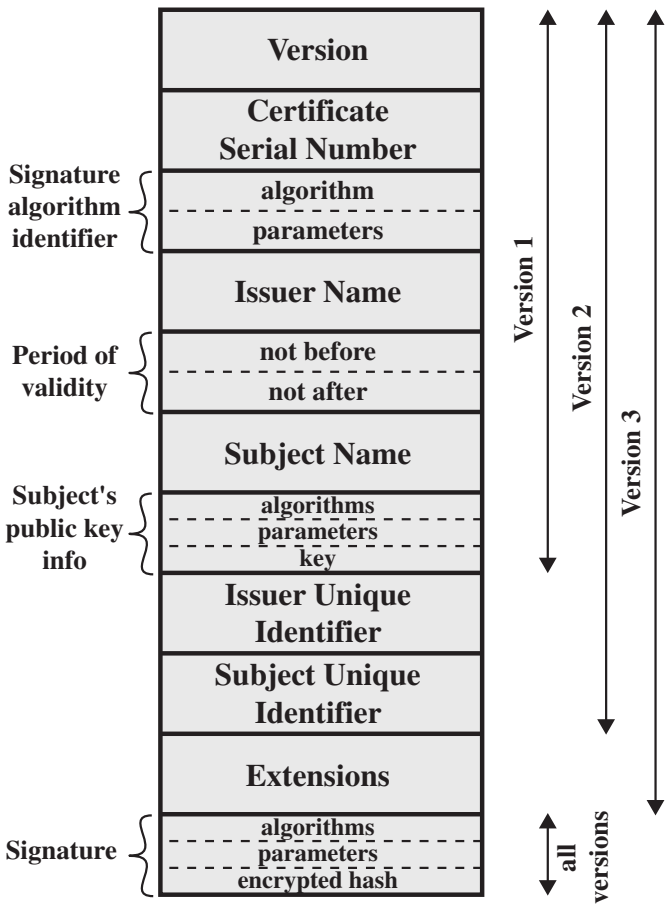


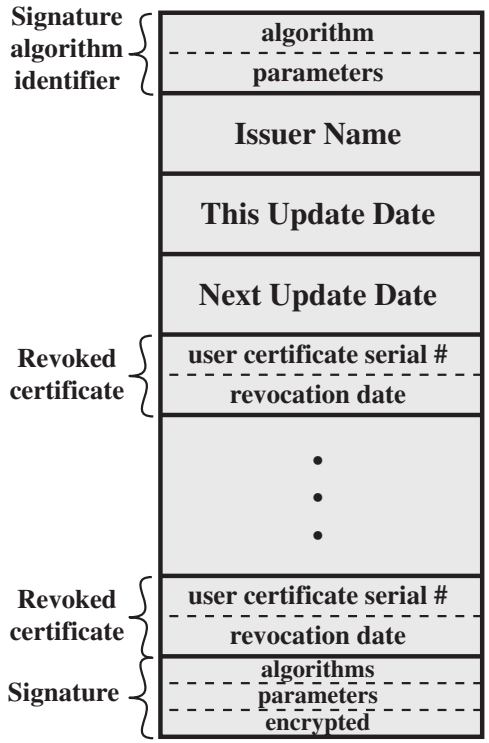

Figure: An overview of use of public-key certificates. Image: [Sta13]

# Public-key Certificates

## X.509




(a) X.509 Certificate




(b) Certificate Revocation List

Figure: An overview of X.509 certificate format. Image: [Sta13].

# Public-key Certificates

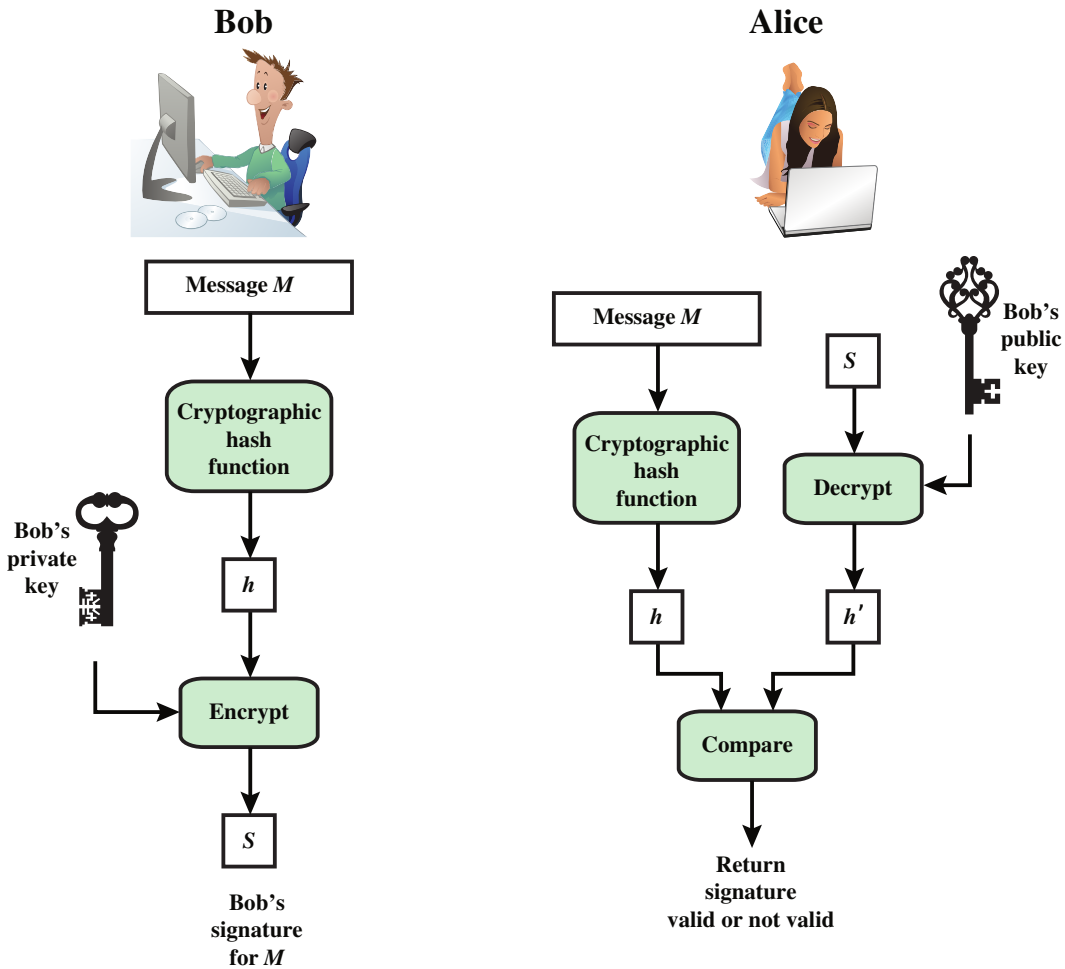



Figure: An overview of the digital signature process. Image: [Sta13].

# Public-key Certificates

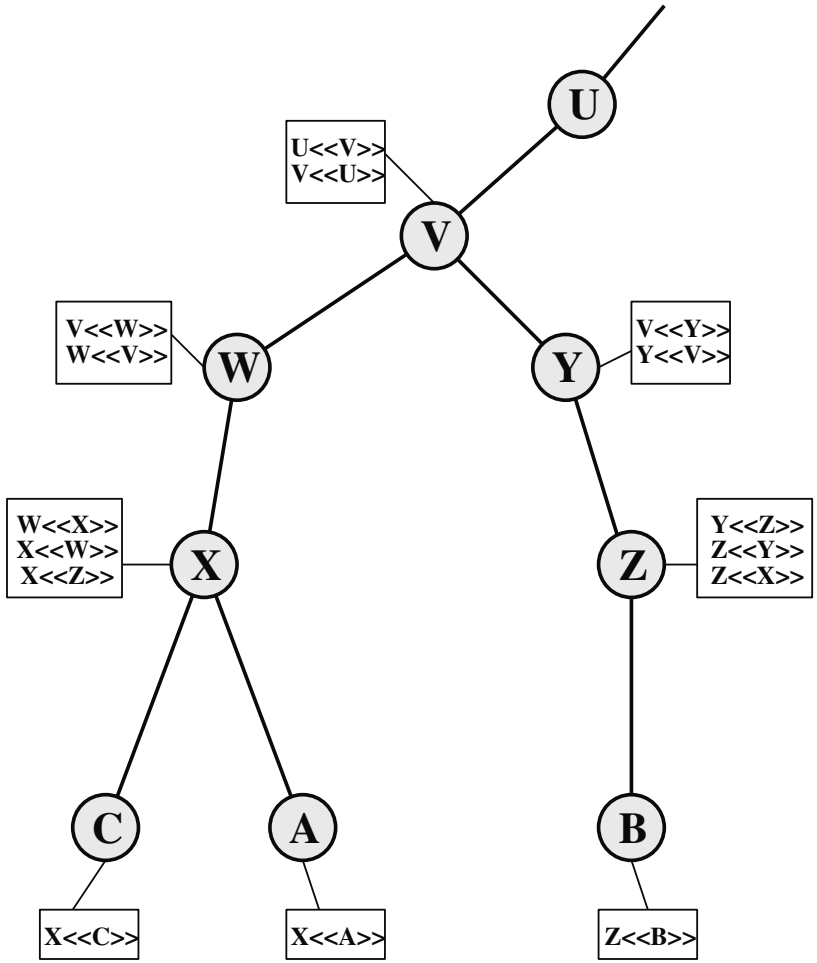



Figure: The X.509 certificate hierarchy. Image: [Sta13].

Mittuniversitetet
MID SWEDEN UNIVERSITY

# Identity Management

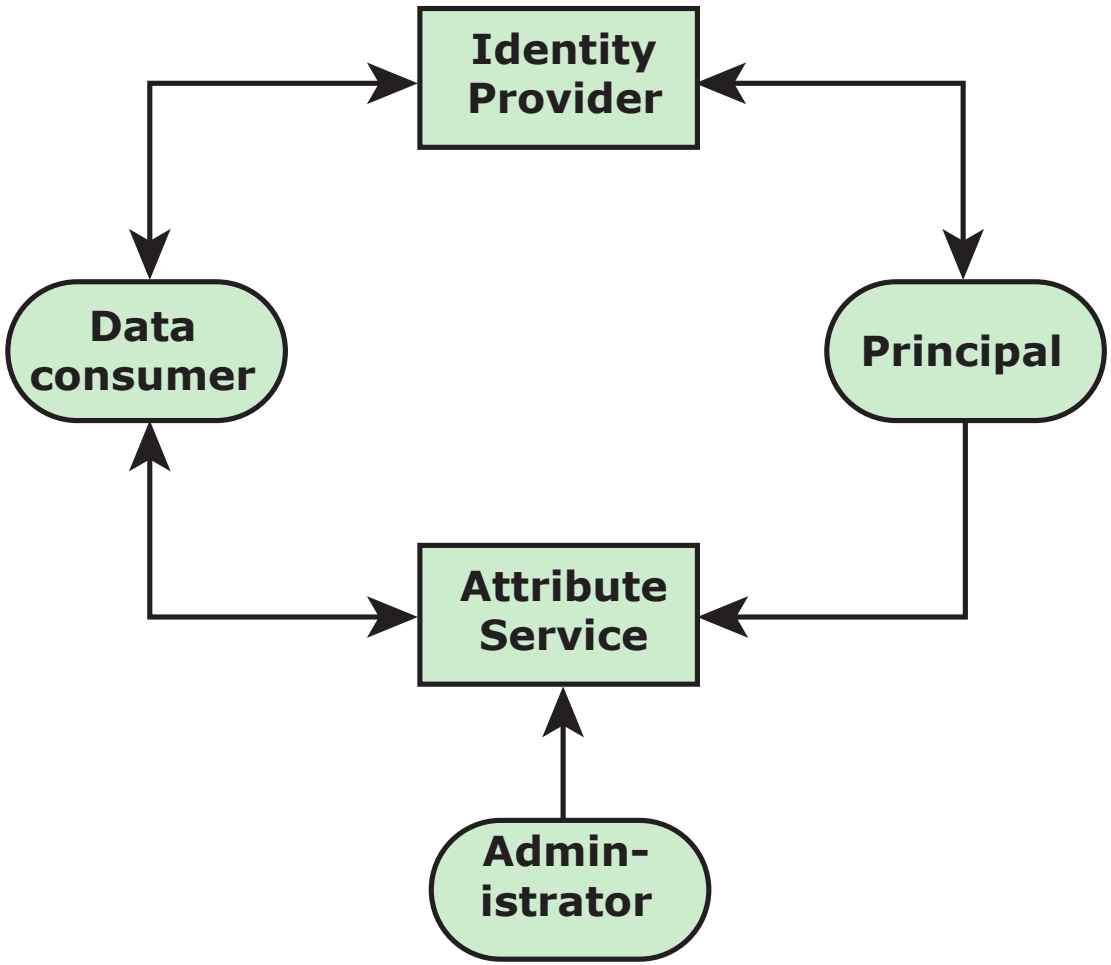



Figure: An overview of a generic identity management system. Image: [Sta13].

# Identity Federation

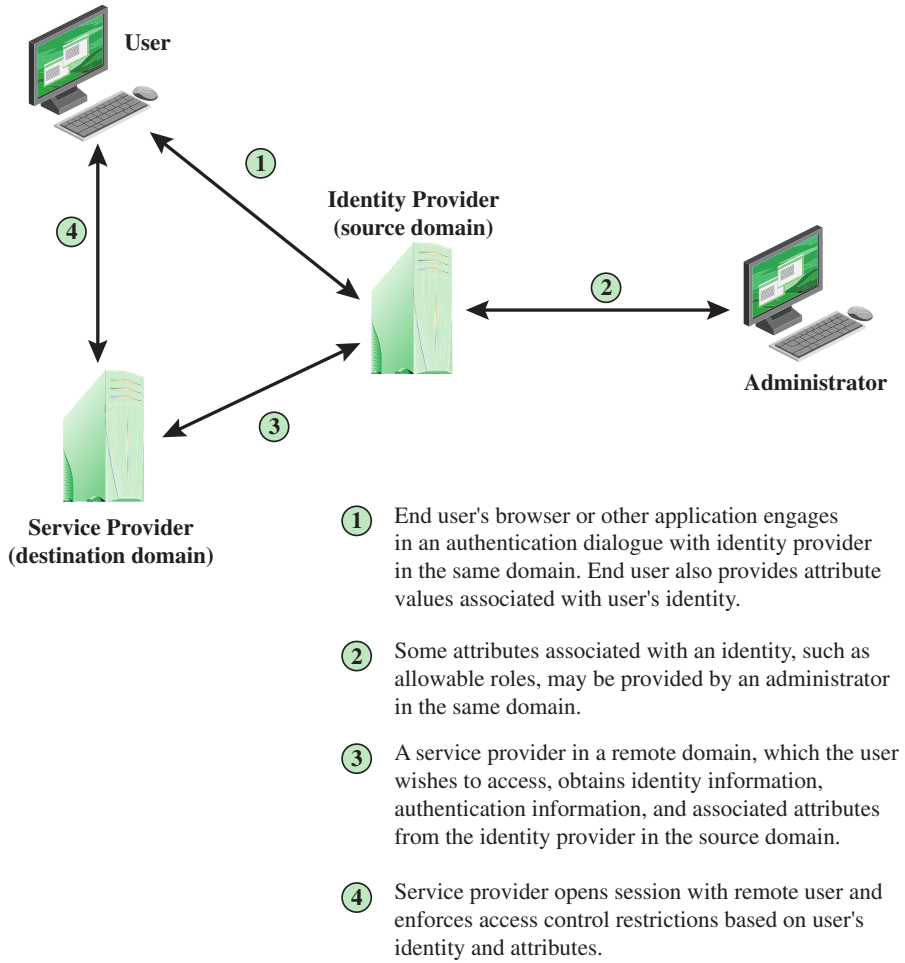



Figure: An overview of federated identity systems. Image: [Sta13].

Mittuniversitetet
MID SWEDEN UNIVERSITY

# Referenser I

[Sta13] William Stallings. *Network security essentials : applications and standards*. 5th ed. International Edition. Pearson Education, 2013. ISBN: 978-0-273-79336-6.

Mittuniversitetet
MID SWEDEN UNIVERSITY