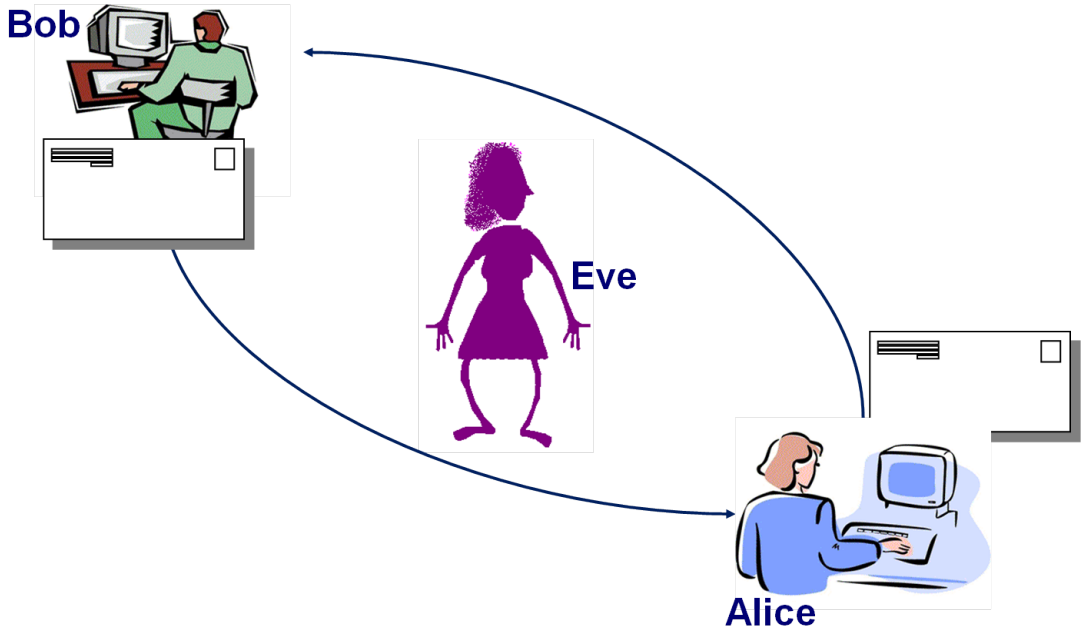
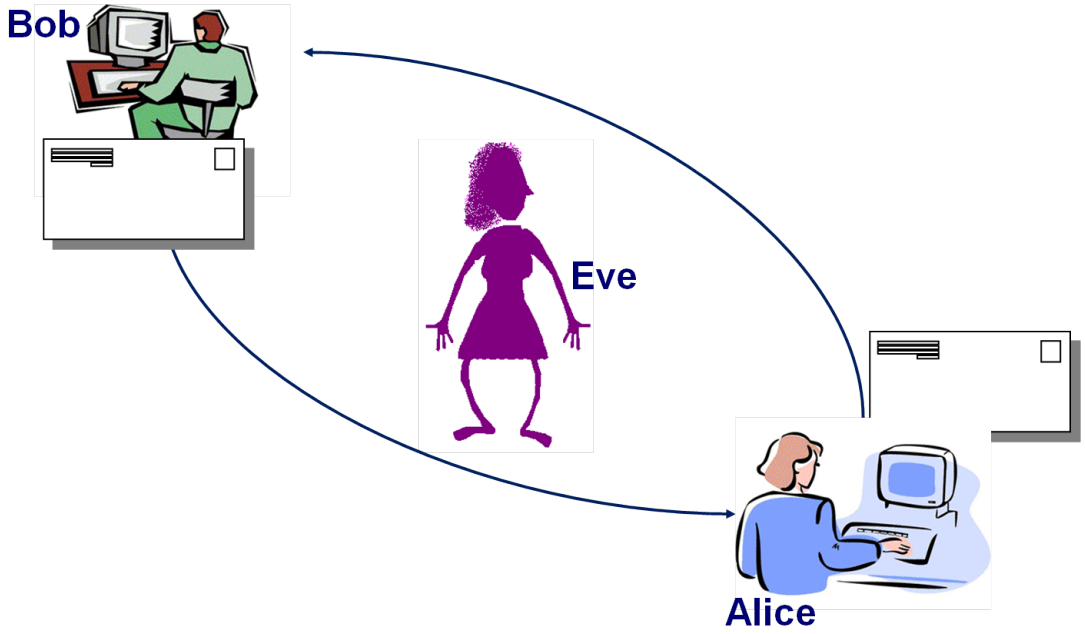
Vertraulichkeit und Authentizität



- Vertraulichkeit - Lauschen
- Authentizität - Tauschen des Datenursprungs
- Integrität - Änderung der Daten
- Zurechenbarkeit - Leugnen des Datenursprungs

Aufgaben



Drei mögliche Varianten für Vertraulichkeit und Authentizität:

1. **Encrypt-and-authenticate**
2. **Authenticate-then-encrypt**
3. **Encrypt-then-authenticate**

Drei Varianten

Verschlüsselungsverfahren $\Gamma = \left(\{0,1\}^*, \{0,1\}^*, K_1, E, D\right)$

Authentifizierungscode $M = \{h_k : k \in K_2\}$ mit Nachrichtenraum $\{0,1\}^*$

Bei Nachricht m und Schlüsseln k_1, k_2 berechnet und überträgt der Sender:

Encrypt-and-authenticate	$c := E_{k_1}(m), t := h_{k_2}(m)$
Authenticate-then-encrypt	$t := h_{k_2}(m), c := E_{k_1}(m \parallel t)$
Encrypt-then-authenticate	$c := E_{k_1}(m), t := h_{k_2}(c)$

Drei Varianten - Sicherheit

1. Encrypt-and-authenticate nicht sicher, da t Informationen über m enthalten kann.
   ⇒ Vertraulichkeit verletzt

2. Authenticate-then-encrypt nicht sicher, da Chosen-Plaintext-Angriffe möglich sein können.
   ⇒ Vertraulichkeit verletzt
   (wird in TLS/SSL genutzt!)

3. Encrypt-then-authenticate sicher, falls Γ und M sicher sind.

TLS – Transport Layer Security

- TLS (oder SSL) ist ein (hybrides) Verschlüsselungs-protokoll zur Datenübertragung im Internet.
- Eingesetzt von HTTPS.
- Erste Version 1994 kurz nach Erscheinen von Mosaic durch Netscape eingeführt.
- Seit 1999 standardisiert durch die IETF (Internet Engineering Task Force),
- Es existieren verschiedene Versionen des Standards.
- Seit Januar 2016 existiert ein Draft für TLS 1.3
- Betrachten die beiden wichtigsten Teile von TLS/SSL: Handshake und Record Protocol in einer von vielen Varianten.

TLS – Record Protokoll

Nachricht
in Blöcken

komprimierte
Nachricht

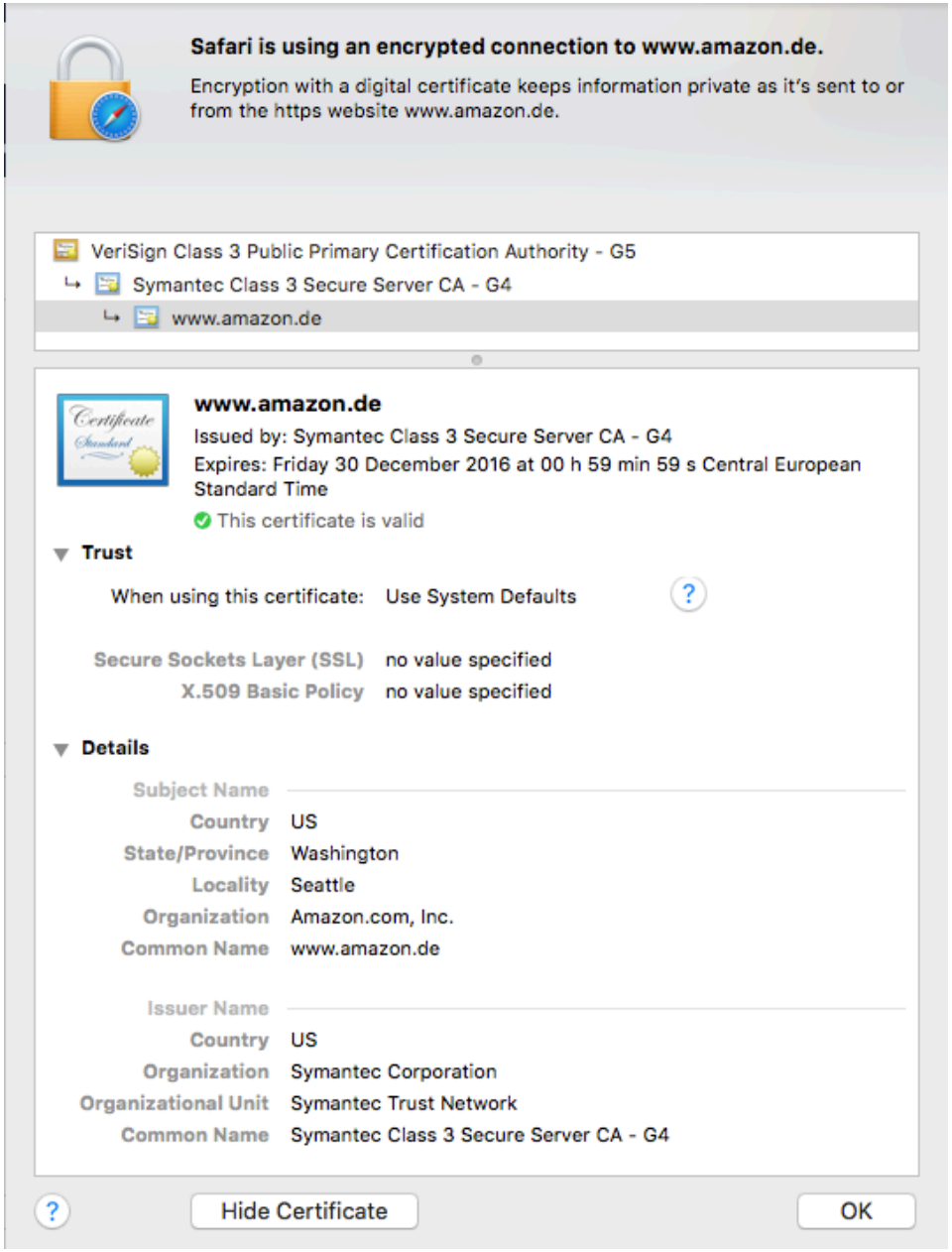
mit MAC und
verschlüsselt

Kompressionsalgorithmus, MAC, Verschlüsslungs-verfahren und Schlüssel im Handshake festgelegt.

Zertifkate

- Binden Schlüssel an Entitäten und verbürgen deren Gültigkeit.
- Realsisiert durch digitale Unterschrift vertrauenwürdiger Instanzen.
- Deren Schlüssel durch Zertifikate ausgestellt durch übergeordnete Instanzen bestätigt.
- Führt zu Kette von Zertifikaten und Unterschriften.

Zertifkate


Safari is using an encrypted connection to www.amazon.de.
Encryption with a digital certificate keeps information private as it's sent to or from the https website www.amazon.de.
VeriSign Class 3 Public Primary Certification Authority - G5
Symantec Class 3 Secure Server CA - G4
www.amazon.de
www.amazon.de
Issued by: Symantec Class 3 Secure Server CA - G4
Expires: Friday 30 December 2016 at 00 h 59 min 59 s Central European Standard Time
This certificate is valid
Trust
When using this certificate: Use System Defaults
Secure Sockets Layer (SSL) no value specified
X.509 Basic Policy no value specified
Details
Subject Name
Country US
State/Province Washington
Locality Seattle
Organization Amazon.com, Inc.
Common Name www.amazon.de
Issuer Name
Country US
Organization Symantec Corporation
Organizational Unit Symantec Trust Network
Common Name Symantec Class 3 Secure Server CA - G4
Hide Certificate
OK

TLS – Handshake Protokoll (Runde 1)

Client

Server

Hello Server
Version||$rand_1$||Session_Id||Cipher_List||
Compression_List

Version||$rand_2$||Session_Id||Cipher||Compression

Initiierung und Festlegung der Verfahren

TLS – Handshake Protokoll (Runde 2)

- Server_Certificate enthält öffentliche Schlüssel von S.

TLS – Handshake Protokoll (Runde 3)

- Client_Certificate enthält öffentliche Schlüssel von C.
- pre zufällig (48 Bytes)
- mastr aus pre abgeleitet

TLS – Handshake Protokoll (Runde 4)

Client

Server

change cipher spec
hash(mastr||opad||hash(messages||0x434C4E54||mastr||ipad))

change cipher spec
hash(mastr||opad||hash(messages||0x53525652||mastr||ipad))

Abschluss und Integritätsprüfung

- mastr = MD5(pre||SHA('A'||pre||pre||$rand_1$||$rand_2$)||
  MD5(pre||SHA('BB'||pre||pre||$rand_1$||$rand_2$)||
  MD5(pre||SHA('CCC'||pre||pre||$rand_1$||$rand_2$)||
- mastr genutzt für Record Protokoll