Dokumentation IT Linux

STAND: 06.11.2016

Apache SSL - http-over-SSL

Der SSL-Kanal sichert die

Vertraulichkeit

- Daten sind vor einem Mithören geschützt
- (Symmetrische Verschlüsselung)
- (Asymmetrische Verschlüsselung)
- Hybride Verschlüsselung

Integrität

- Daten können unterwegs nicht manipuliert werden
- Checksummen etc.

Authentizität

- Authentifizierung mit Zertifikaten
- Schutz vor gefälschten Webservern

Symmetrische Verschlüsselung

Beispiele: AES (aka Rijndael), DES, 3DES, Twofish

- Sender und Empfänger über einen gemeinsamen (geheimen) Schlüssel verfügen
- Vor Beginn der eigentlichen Kommunikation muss dieser ausgetauscht werden
- Sender benutzt diesen Schlüssel, um die Nachricht zu verschlüsseln
- Empfänger, um die Nachricht zu entschlüsseln

Symmetrische Verschlüsselung

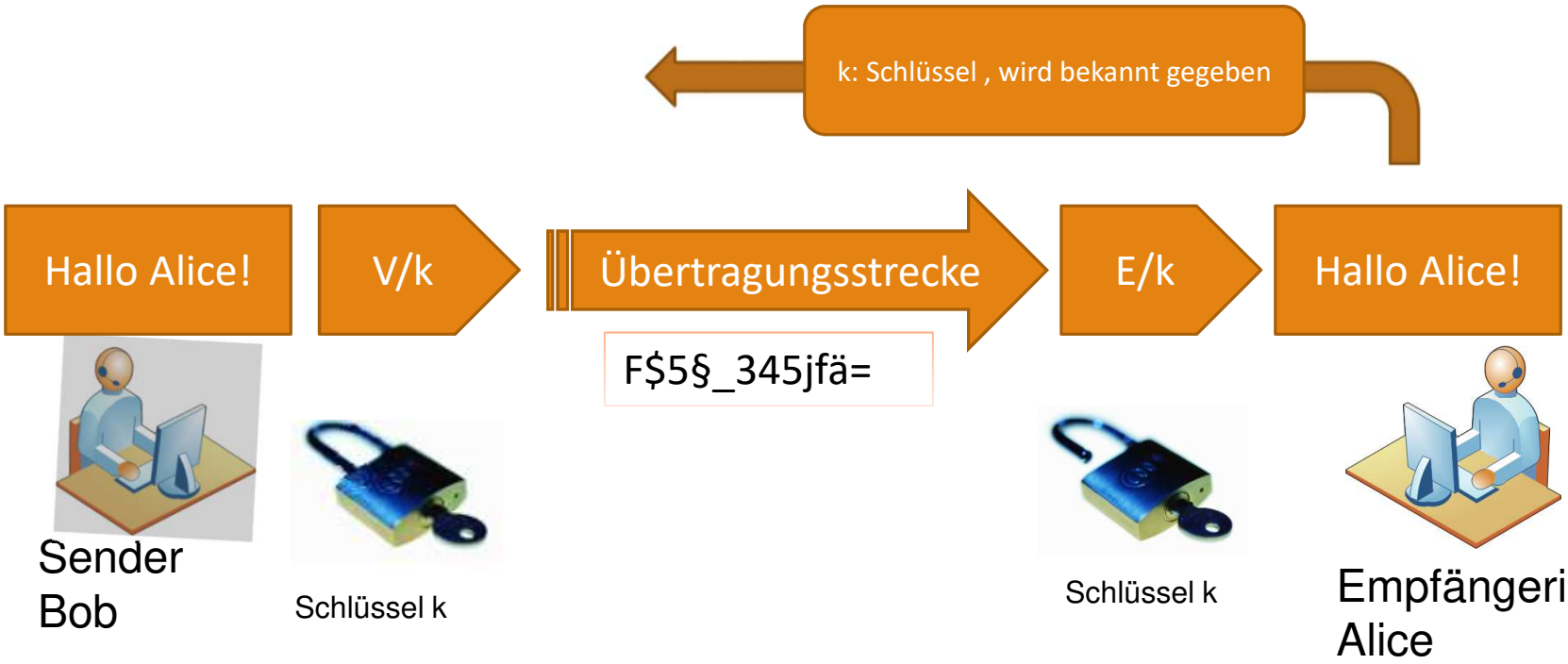
Vorteile

- hohe Geschwindigkeit, mit denen Daten ver- und entschlüsselt werden

Nachteil

- Schlüsselmanagement
  - Sender und Empfänger müssen vor Beginn der eigentlichen Kommunikation über einen sicheren Kanal einen Schlüssel ausgetauscht haben

Symmetrische Verschlüsselung



Asymmetrische Verschlüsselung

- Ver- und Entschlüsselung werden mit unterschiedlichen Schlüssel verwendet
- (Private und Public Key).
- Sender verschlüsselt Nachricht mit Public Key des Empfängers
- Empfänger entschlüsselt mit Privat Key
- Private Keys müssen sicher gespeichert werden

Beispiele: RSA, ElGamal, Diffie-Hellman Schlüsselaustausch

Asymmetrische Verschlüsselung

Vorteile

- einfacheres Schlüsselmanagement
- kein sicherer Kanal notwendig für Austausch nötig
- Hier ist lediglich auf die Unverfälschtheit (Integrität und Authentizität) des öffentlichen Schlüssels zu achten.

Nachteile

- Im Vergleich zu symmetrischen Verfahren sind reine asymmetrische Verfahren jedoch um ein Vielfaches langsamer.

Asymmetrische Verschlüsselung

kA: öffentlicher Schlüssel von Alice, wird jedem bekannt gegeben

Hallo Alice! → V/kA → Übertragungsstrecke → E/kA‘ → Hallo Alice!

F$5§_345jfä=

Sender
Bob

Schlüssel kA

Schlüssel kA‘
Privater Schlüssel
von Alice

Empfängerin
Alice

Hybridverfahren

- Daten werden mit symmetrischen Verfahren verschlüsselt
- Sitzungsschlüssel (session key) gültig für eine Nachricht
- Sitzungsschlüssel mit Hilfe des asymmetrischen Verfahrens verschlüsselt und zusammen mit der Nachricht an den Empfänger übertragen.
- Empfänger kann den Sitzungsschlüssel mit Hilfe seines geheimen Schlüssels bestimmen und mit diesem dann die Nachricht entschlüsseln
- Schlüsselmanagement asymmetrischer Verfahren,
- Schnelligkeit symmetrischer Verfahren

Beispiel **EFS** (**E**ncrypting **F**ile **S**ystem)

Hybridverfahren

kA: öffentlicher Schlüssel von Alice, wird jedem bekannt gegeben

Session Key → V/kA → Übertragungsstrecke → E/kA‘ → Session Key

F$5§_345jfä=

Erzeugung Sitzungs-schlüssel kS

Verschlüsselung Sitzungs-schlüssel kS mit kA

Entschlüsselung Sitzungs-schlüssel kS mit kA‘

Anforderung Sitzungs-schlüssel kS

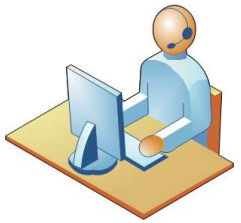
Hallo Alice! → V/kS → Übertragungsstrecke → E/kS → Hallo Alice!

345jfzfztzvzuv

Sender Bob

Verschlüsselung mit Sitzungs-schlüssel kS

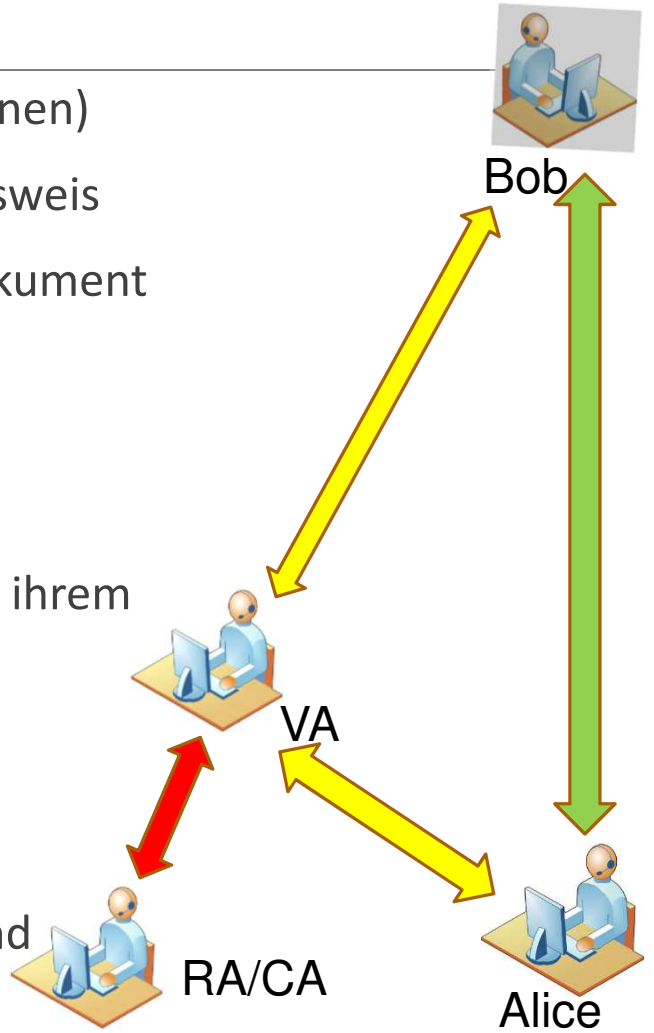
Entschlüsselung mit Sitzungs-schlüssel kS



Empfängerin Alice

Zertifikat

- X.509-Zertifikat (öffentlicher Schlüssel für reale Personen)
- Antrag an Registration Authority (RA) mit Personalausweis
- Certfication Autority (CA) stellt ein elektronisches Dokument (Zertifikat) aus, mit folgenden Informationen:
  - Name des Zertifikatnehmers und der Name der CA
  - öffentliche Schlüssel des Zertifikatnehmers
  - Gültigkeitszeitraum des Zertifikats
- Die CA unterzeichnet das Zertifikat anschließend mit ihrem geheimen Schlüssel
- Anfrage an Validation Authority (VA) über:
  - Echtheit des PK
  - Zertifikat unverfälscht
- CA garantiert also die Zugehörigkeit von Benutzer und öffentlichem Schlüssel.



Handshake SSL (Beispiel)

1. Client stellt Anfrage an Server und sendet unterstützte Verschlüsselungsverfahren
2. Server wählt Verfahren[1] und sendet Zertifikat und öffentlichen Schlüssel
3. Client generiert nach Überprüfung den session key für symmetrisches Verschlüsselungsverfahren. Dieser wird mit dem öffentlichen Schlüssel des Servers verschlüsselt und zum Server übertragen. Nur der Server kann ihn mit seinem privaten Schlüssel entschlüsseln.
4. Optional: Client authentisiert sich mit Zertifikat
5. Verschlüsselung und Datenübertragung
6. Verbindungsabbau

[1](Verwendete Cipher Suite mit RSA Schlüsselaustausch)

Handshake SSL