Informationssicherheit, Datenschutz, Urheberrecht

ISDS

Themenübersicht

06
Verschlüsselung Signatur

Grundlagen

Symmetrische & Asymmetrische Verschlüsselung

Verschlüsselungs-protokolle und ihre Anwendung

Signaturen

07
IDS, IPS, Firewalls

Intrusion Detection System

Intrusion Prevention System

Honeypot

Firewall

Sandbox

08
Proaktive Sicherheit

Defensive Programmierung

Gehärtete Betriebssysteme

Patches

Vulnerability Assessment

Aktive Sicherheit von Netzwerk-komponenten

09
Urheberrecht

Der Urheber

Das Werk

Urheber-persönlichkeitsrecht

Verwertungsrechte

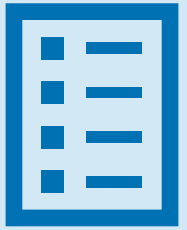
Nutzungsrechte

Ausnahmen

Dauer

Recht am eigenem Bild

10
Lernstands-messung



Agenda

1. Verschlüsselung
    1. Grundlagen
    2. symmetrische Verschlüsselung
    3. asymmetrische Verschlüsselung
    4. weitere Verschlüsselungen
    5. Verschlüsselungsprotokolle und ihre Anwendung
2. Signaturen
    1. Digitales Zertifikat
    2. Digitale Signatur
    3. Public Key Infrastructure

1 Verschlüsselung

1.1 Grundlagen

1 Verschlüsselung

1.1 Grundlagen

- Verschlüsselung nennt man den Vorgang, bei dem ein klar lesbarer Text mit Hilfe eines Verschlüsselungsverfahrens in einer „unleserliche“, das heißt nicht einfach interpretierbare Zeichenfolge umgewandelt wird.

- Ziele
  - Vertraulichkeit
  - Integrität
  - Authentizität
  - Verbindlichkeit

1 Verschlüsselung

1.1 Grundlagen

- Verschlüsselungsalgorithmus
  - mathematische Funktion, der man den Klartext und einen Schlüssel übergibt
  - Ausgabe ist ein Geheimtext, der keinen Rückschluss auf den Klartext erlaubt
  - nur mit Kenntnis des Schlüssels kann man mit der selben mathematischen Funktion den Geheimtext wieder in den Klartext umwandeln

1 Verschlüsselung

1.1 Grundlagen

- Verschlüsselungsverfahren
  - Algorithmus zum Verschlüsseln und Entschlüsseln, sowie Verfahren zum Schlüsselaustausch, Prüfung der Authentizität und Integrität
  - symmetrische, asymmetrische und hybride Verschlüsselungsverfahren
  - hybriden Verschlüsselungsverfahren kombinieren symmetrische und asymmetrische Verschlüsselungsverfahren miteinander

1 Verschlüsselung

1.1 Grundlagen

- Hashverfahren
  - ist eine Verschlüsselungsform, die nicht wieder rückgängig gemacht werden kann
  - dient häufig zum Vergleich einer gespeicherten, verschlüsselten Information mit einer aktuell eingegebenen, z. B. Kennwörter
  - das gespeicherte Kennwort wird als Hash-Wert hinterlegt, das bei der Anmeldung eingegebene Kennwort wird in den Hash-Wert verschlüsselt und beide Werte werden verglichen
  - wenn diese übereinstimmen, wurde die Eingabe als richtig angesehen

1 Verschlüsselung

1.1 Grundlagen

- Hashverfahren
  - Anwendungsfelder:
    - Prüfsummen
    - Digitale Signatur
    - Speichern von Passwörtern
  - Verfahren:
    - MD5 (veraltet unsicher)
    - SHA (Secure Hash Algorithm), z.B. SHA1, SHA2, SHA3
    - RIPEMD-160

1 Verschlüsselung

1.1 Grundlagen

- Kriterien für gute Schlüssel
  - Je länger desto besser
  - Je komplexer desto besser

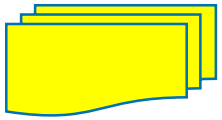
1 Verschlüsselung

1.2 symmetrische Verschlüsselung

1 Verschlüsselung

1.2 symmetrische Verschlüsselung

- Ziel
  - Sender sendet eine verschlüsselte Nachricht zum Empfänger.
  - Empfänger erhält eine verschlüsselte Nachricht und kann sie lesen



1 Verschlüsselung

1.2 symmetrische Verschlüsselung

- Lösungsansatz
  - Es wird EIN Schlüssel erzeugt.
  - Der Schlüssel muss dem Sender und Empfänger vorliegen

1 Verschlüsselung

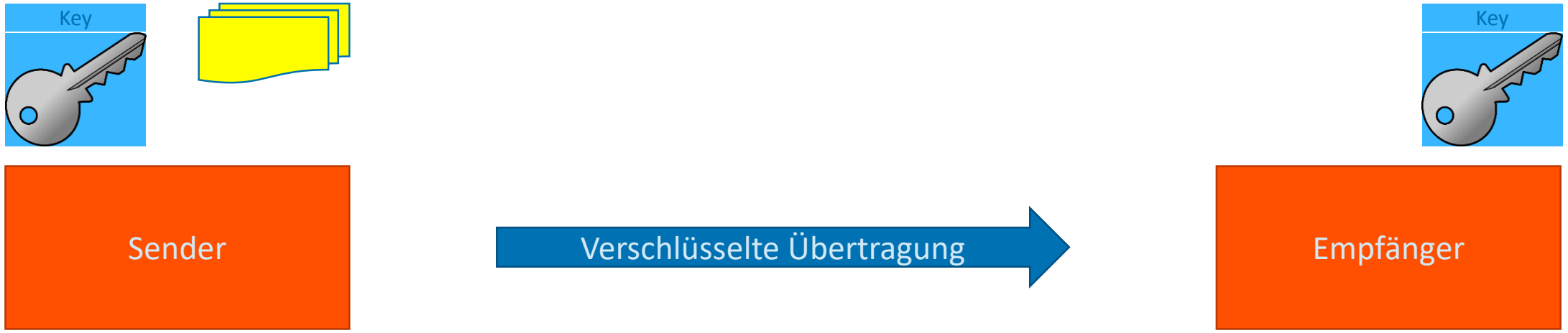
1.2 symmetrische Verschlüsselung

- Lösungsansatz
  - Es wird EIN Schlüssel erzeugt.
  - Der Schlüssel muss dem Sender und Empfänger vorliegen

1 Verschlüsselung

1.2 symmetrische Verschlüsselung

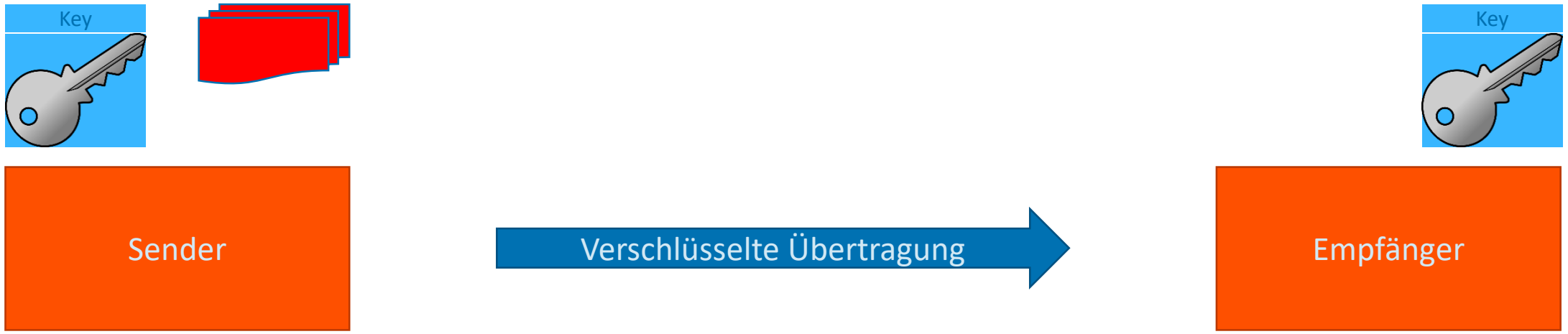
- Lösungsansatz
  - Paket kann nun verschlüsselt werden.



1 Verschlüsselung

1.2 symmetrische Verschlüsselung

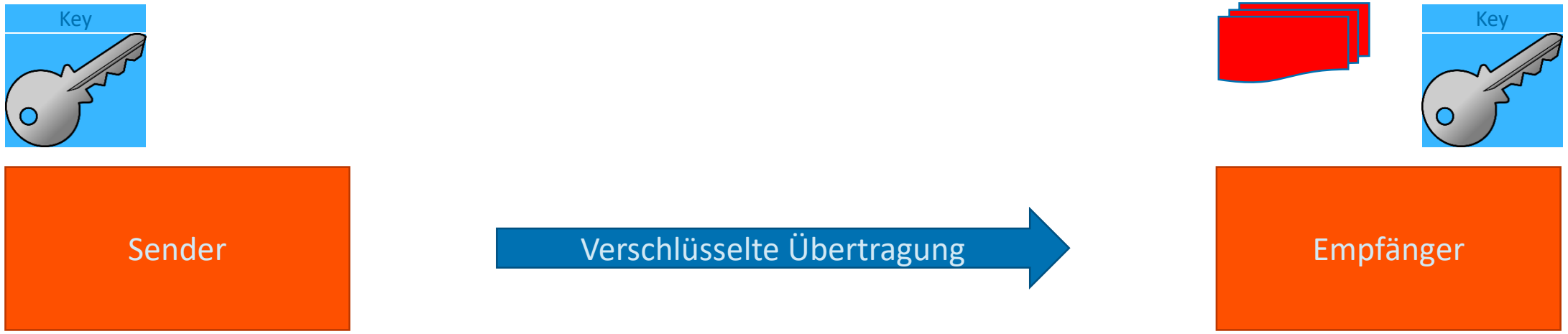
- Lösungsansatz
  - Paket kann nun versendet werden.



1 Verschlüsselung

1.2 symmetrische Verschlüsselung

- Lösungsansatz
  - Paket kann nun entschlüsselt werden.



1 Verschlüsselung

1.2 symmetrische Verschlüsselung

- Beispiele für Verschlüsselungsverfahren
  - Caesar Ciffre
  - Data Encryption Standard (DES)
  - Advanced Encryption Standard (AES)
  - Blowfish
  - . . .

1 Verschlüsselung

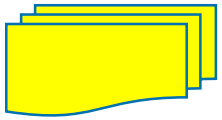
1.2 symmetrische Verschlüsselung

- Vorteile symmetrischer Verschlüsselung
  - relativ schnelle Ver- und Entschlüsselung
  - Für größere Datenmengen geeignet
  - Mit langem Schlüssel ergibt sich eine hohe Sicherheit
- Nachteile symmetrischer Verschlüsselung
  - Jeder, der im Besitz des Schlüssels ist, kann die Nachrichten Ent- und verschlüsseln
  - Es muss ein sicherer Übertragungsweg für den Austausch des Schlüssels gefunden werden

1 Verschlüsselung

1.3 asymmetrische Verschlüsselung

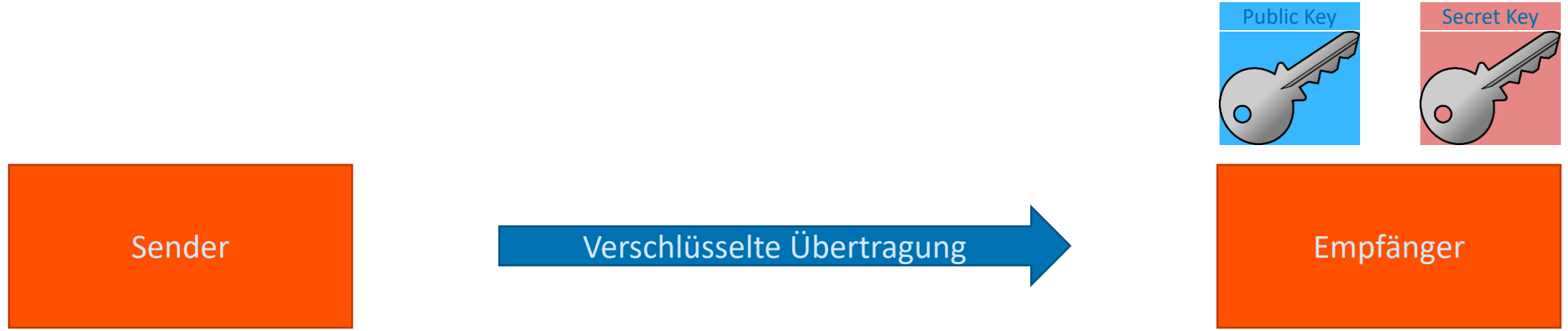
- Ziel
  - Sender sendet eine verschlüsselte Nachricht zum Empfänger.
  - Empfänger erhält eine verschlüsselte Nachricht und kann sie lesen



1 Verschlüsselung

1.3 asymmetrische Verschlüsselung

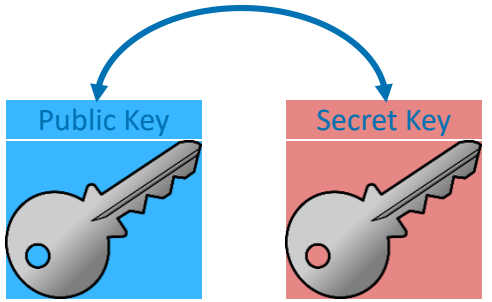
- Lösungsansatz
  - 1. Der Empfänger erstellt ein Schlüsselpaar.
    - Einen öffentlichen Schlüssel (Public Key)
    - und einen geheimen Schlüssel (Secret Key)



1 Verschlüsselung

1.3 asymmetrische Verschlüsselung

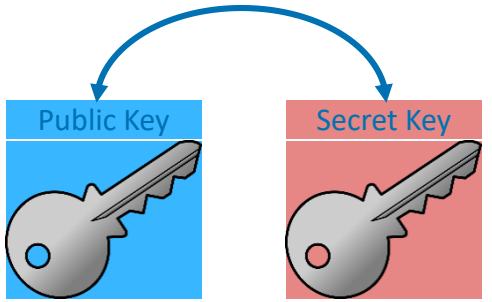
- Lösungsansatz
  - 1. Der Empfänger erstellt ein Schlüsselpaar.
    - Das Paar ist mathematisch verbunden
    - Es wird durch einen Algorithmus erzeugt



1 Verschlüsselung

1.3 asymmetrische Verschlüsselung

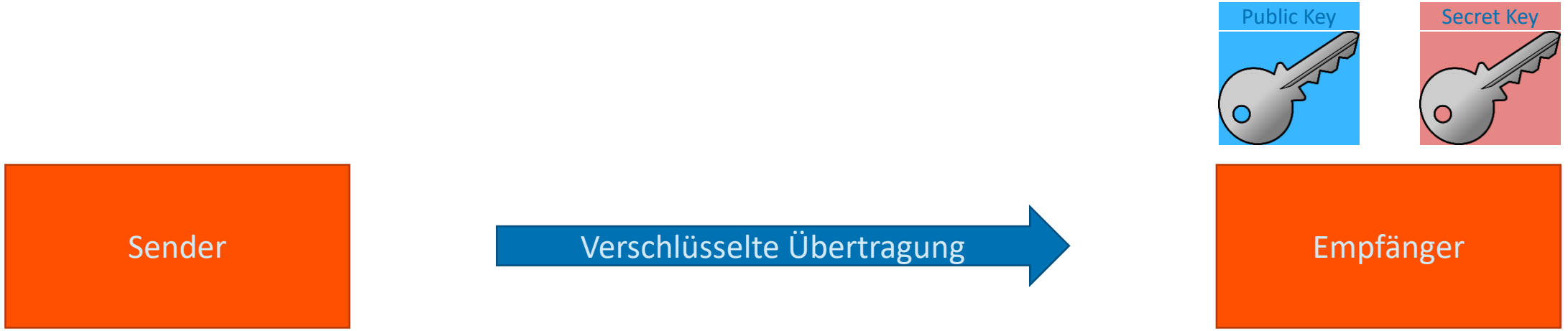
- Lösungsansatz
  - Aufgabe Public Key
    - Er **ver**schlüsselt die Nachricht des Senders
  - Aufgabe Secret Key
    - Er **ent**schlüsselt die verschlüsselte Nachricht des Senders



1 Verschlüsselung

1.3 asymmetrische Verschlüsselung

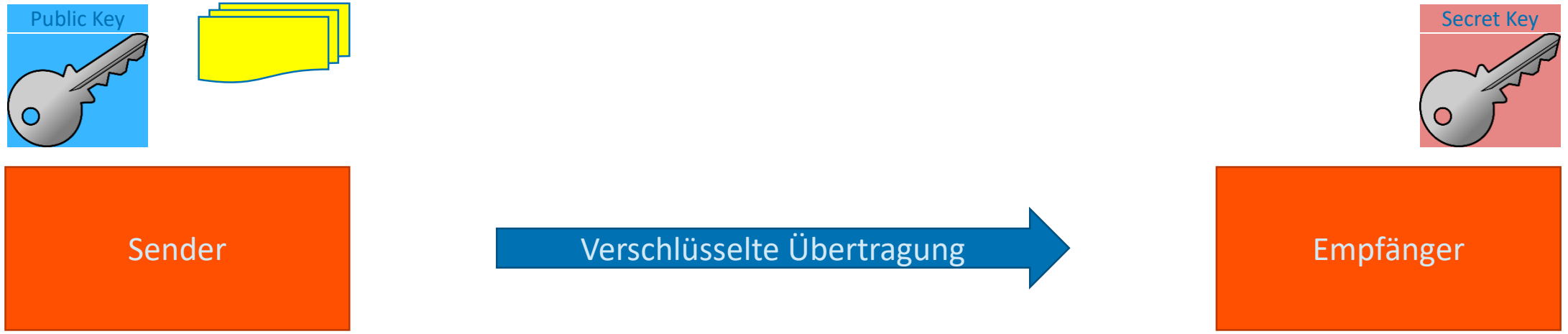
- Lösungsansatz
  - 2. Der Empfänger übermittelt dem Sender seinen Public Key



1 Verschlüsselung

1.3 asymmetrische Verschlüsselung

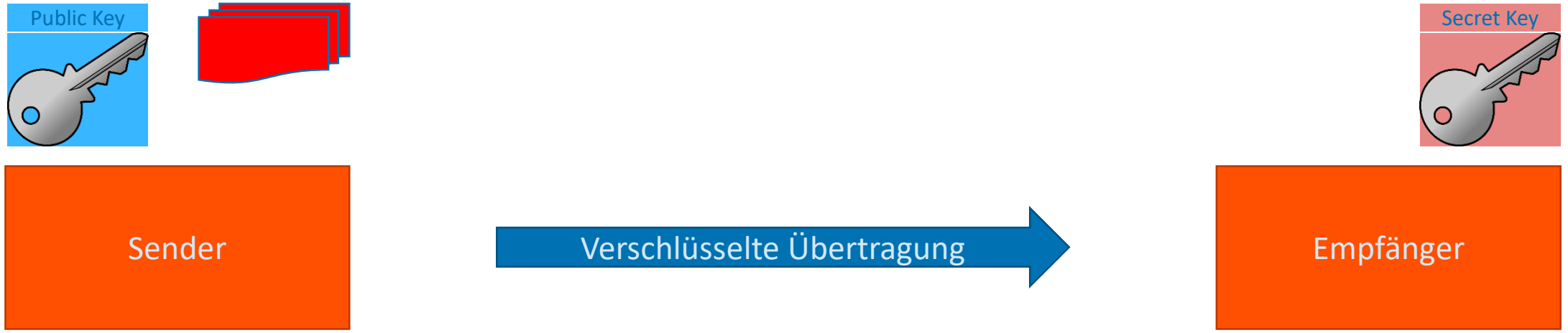
- Lösungsansatz
  - 2. Der Sender verschlüsselt die Nachricht mit dem Public Key des Empfänger



1 Verschlüsselung

1.3 asymmetrische Verschlüsselung

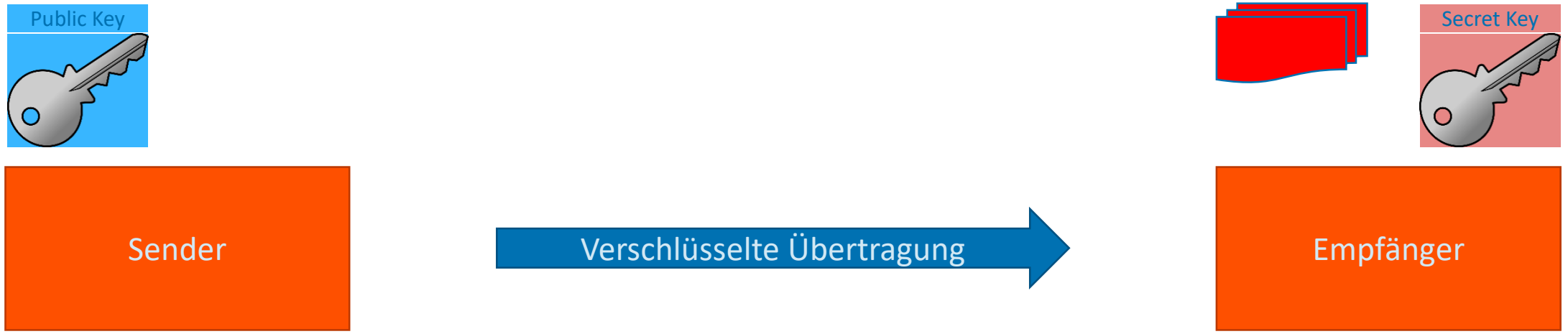
- Lösungsansatz
  - 2. Der Sender versendet die Nachricht zum Empfänger



1 Verschlüsselung

1.3 asymmetrische Verschlüsselung

- Lösungsansatz
  - 2. Der Empfänger entschlüsselt die Nachricht mit seinem Secret Key



1 Verschlüsselung

1.3 asymmetrische Verschlüsselung

- Beispiele für Verschlüsselungsverfahren
  - RSA
  - Merkle-Hellmann
  - Benaloh
  - . . .

1 Verschlüsselung

1.3 asymmetrische Verschlüsselung

- Vorteile asymmetrischer Verschlüsselung
  - Für kleinere Datenmengen geeignet
- Nachteile asymmetrischer Verschlüsselung
  - Benötigt mehr Rechenleistung als bei symmetrischer Verschlüsselung (bis zu 1000 x mehr)n

1 Verschlüsselung

1.4 weitere Verschlüsselungen

- Hybride Verschlüsselung
  - Vereint die Vorteile der symmetrischen und asymmetrischen Verschlüsselung
  - Der gemeinsame Schlüssel wird asymmetrisch übertragen, der Rest anschließend symmetrisch

1 Verschlüsselung

1.5 Verschlüsselungsprotokolle und ihre Anwendung

- Hierbei handelt es sich um Netzwerkprotokolle, die eine verschlüsselte Datenübertragung in einem Netz garantieren.
- Dies dient zur Sicherstellung der Vertraulichkeit und Integrität in Bezug auf die übertragenen Daten, stellt zugleich jedoch auch eine gesetzliche Pflicht im Zusammenhang mit der Übermittlung personenbezogener Daten dar.
- In der Regel bestehen Verschlüsselungsprotokolle aus einem sogenannten Schlüsselaustauschprotokoll in Verbindung mit einem symmetrischen Verschlüsselungsverfahren

1 Verschlüsselung

1.5 Verschlüsselungsprotokolle und ihre Anwendung

Die wichtigsten Standards von Verschlüsselungsprotokollen:

- Transport Layer Security (TLS, früher Secure Sockets Layer, SSL)
- WPA3 und WPA2
- Secure Shell (SSH)
- IPsec

1 Verschlüsselung

1.5 Verschlüsselungsprotokolle und ihre Anwendung

Schlüsselaustauschprotokoll

- Bei diesem Protokoll wird entweder ein geheimer Schlüssel an zwei oder mehr Kommunikationspartner übermittelt oder während der Durchführung des Protokolls ein geheimer Schlüssel nach festgelegter Verfahrensweise erzeugt.

Die drei bekanntesten lauten:

- Merkles Puzzle
- Diffie-Hellmann-Schlüsseltausch
- Needham-Schroeder-Protokoll

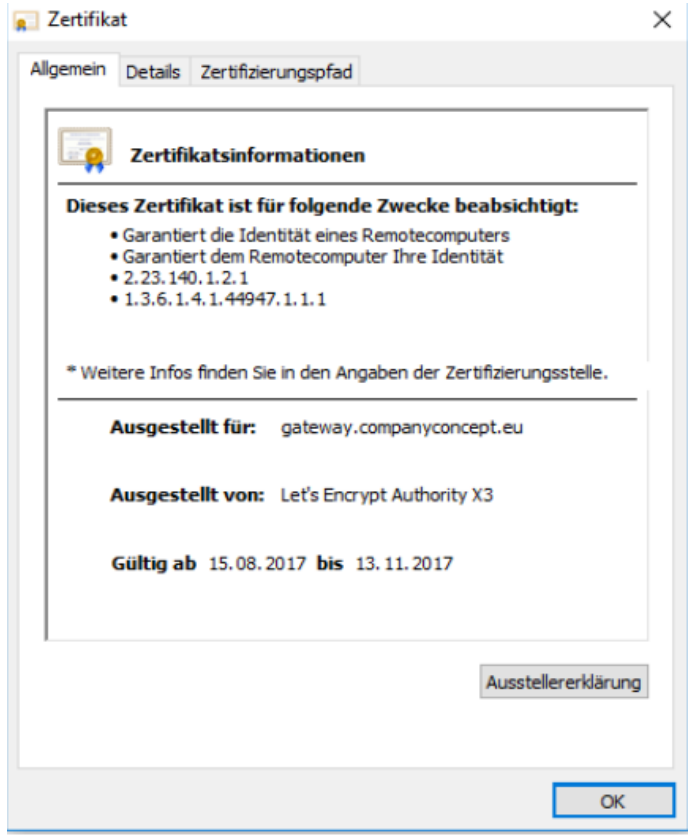
2 Signaturen

2.1 Digitales Zertifikat

2 Signaturen

2.1 Digitales Zertifikat

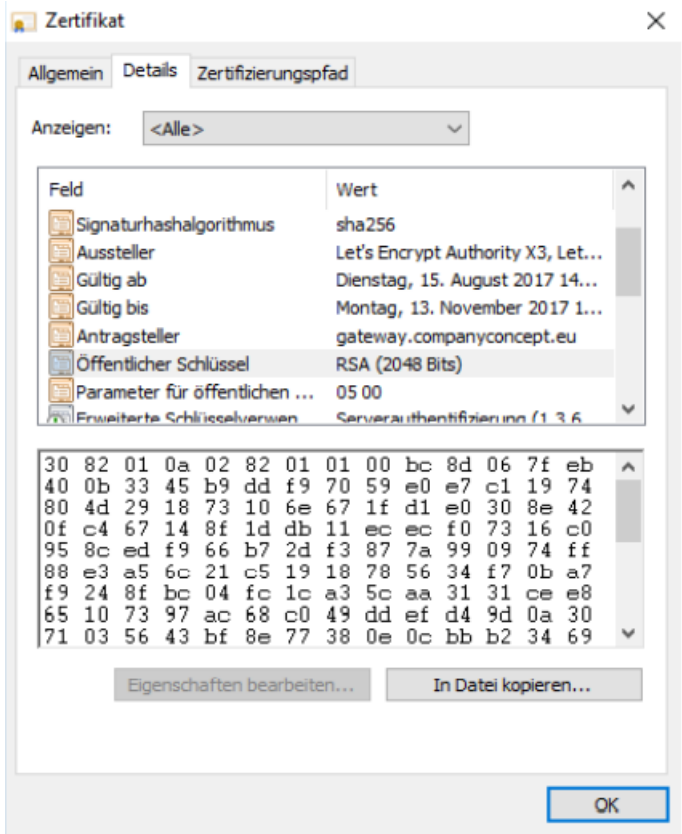
- Ein Datensatz der bestimmte Eigenschaften einer Person bestätigen und dessen Authentizität und Integrität durch kryptografische Verfahren prüft
- Enthält alle zur Prüfung notwendigen Daten
- Die Ausstellung erfolgt durch eine offizielle Zertifizierungsstelle (Certification Authority [CA])
- Verbreiteter Standard ist x.509, diese Zertifikate bestätigen die Identität des Inhaber und weitere Eigenschaften des öffentlichen Schlüssels



2 Signaturen

2.1 Digitales Zertifikat

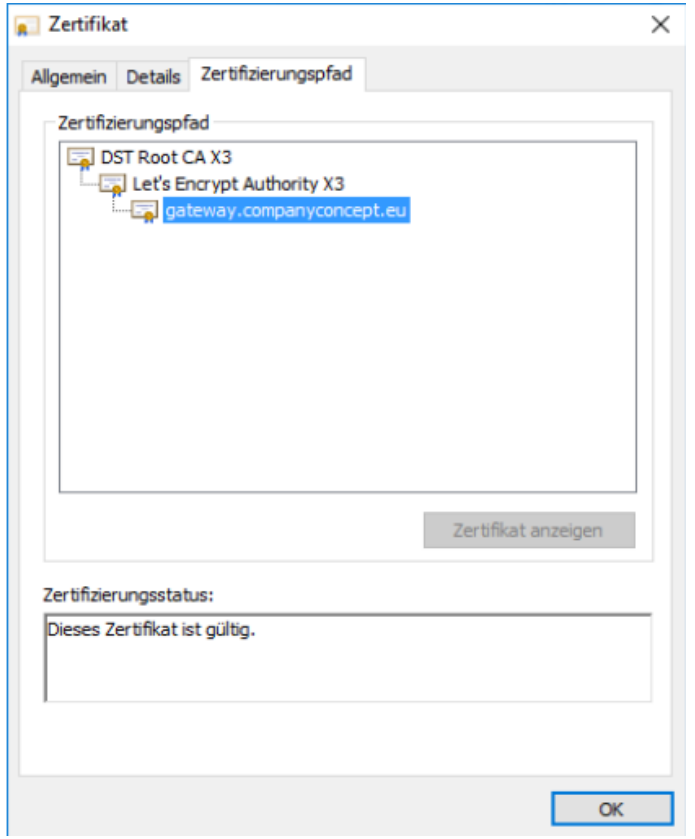
- Können genutzt werden um öffentliche Schlüssel bereit zu stellen
- Haben eine zeitlich befristete Gültigkeitsdauer
- Angaben zur zulässigen Anwendungs- und Geltungsbereich



2 Signaturen

2.1 Digitales Zertifikat

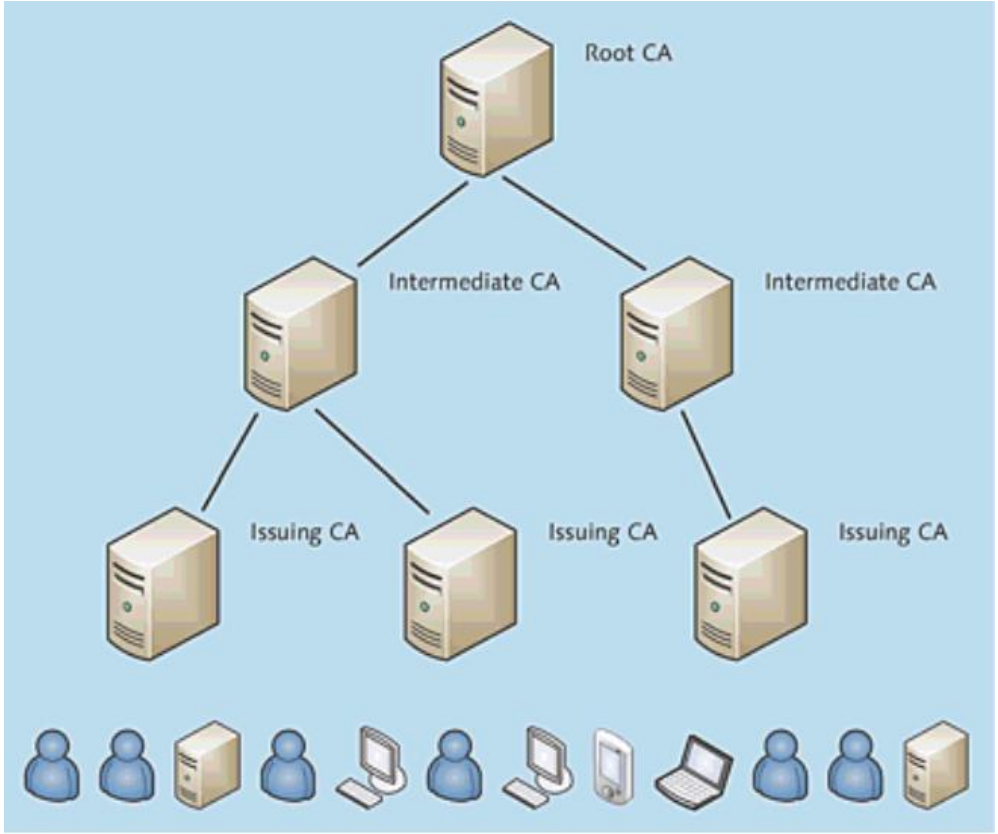
- beinhaltet Informationen über die einzelnen Zertifizierungsinstanzen



2 Signaturen

2.1 Digitales Zertifikat

- Root-CA
  - stellt nur Zertifikate für die untergeordneten CA‘s aus
  - Lange Gültigkeitsdauer der Zertifikate (10 – 20 Jahre)
  - Erstellt das Stammzert. Der gesamten PKI extremer Schutzbedarf
- Intermediate CA
  - Analog Root CA
  - Geringerer Schutzbedarf
- Issuing CA
  - Stellt die tatsächlichen Zert. Für die Clients aus
  - Gültigkeitsdauer ca. 5 Jahre



2 Signaturen

2.2 Digitale Signatur

- Die digitale Signatur ist ein asymmetrisches Verschlüsselungssystem, bei dem mit einem privaten Signaturschlüssel der Hashwert einer Nachricht, die Signatur, berechnet wird.
- Die Signatur ermöglicht es, mittels des dazugehörigen öffentlichen Signaturschlüssels, die Nachricht auf Authentizität und Integrität zu prüfen.
- Der Signaturschlüssel muss eindeutig einer Person zugeordnet sein.

2 Signaturen

2.2 Digitale Signatur

- Rechtliche Folgen
  - Wird die Signatur an eine Nachricht oder ein Dokument angehängt, dann gilt das als unterschrieben.
  - Für digitale Nachrichten und Dokumente werden digitale Signaturen verwendet, um ihre Echtheit glaubhaft und prüfbar zu machen.
  - Die Echtheit der Signatur kann elektronisch geprüft werden.

2 Signaturen

2.2 Digitale Signatur

- Anforderungen
  - Sollte auf einem elektronischen Zertifikat beruhen, damit die Echtheit überprüfbar ist.
  - Die digitale Signatur darf nicht auf andere Dokumente übertragbar sein.
  - Soll den Nachweis erbringen, dass das Dokument seit der Unterzeichnung nicht verändert wurde.
  - Die digitale Signatur soll die Überprüfung der Identität des Unterzeichners überprüfen.

2 Signaturen

2.2 Digitale Signatur

- Digitale Signatur erstellen

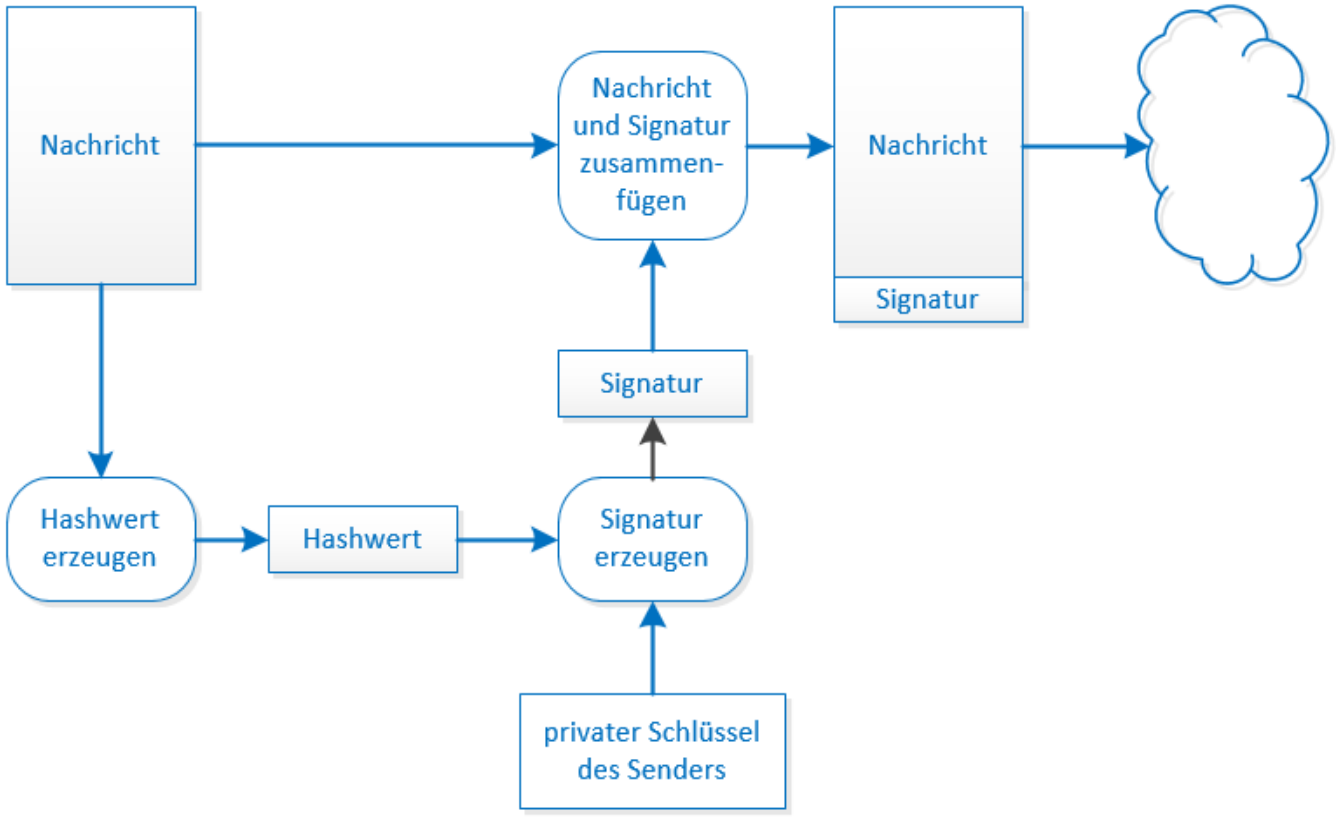


Abbildung 5:Signatur erstellen (Eigene Darstellung)

2 Signaturen

2.2 Digitale Signatur

- Digitale Signatur überprüfen

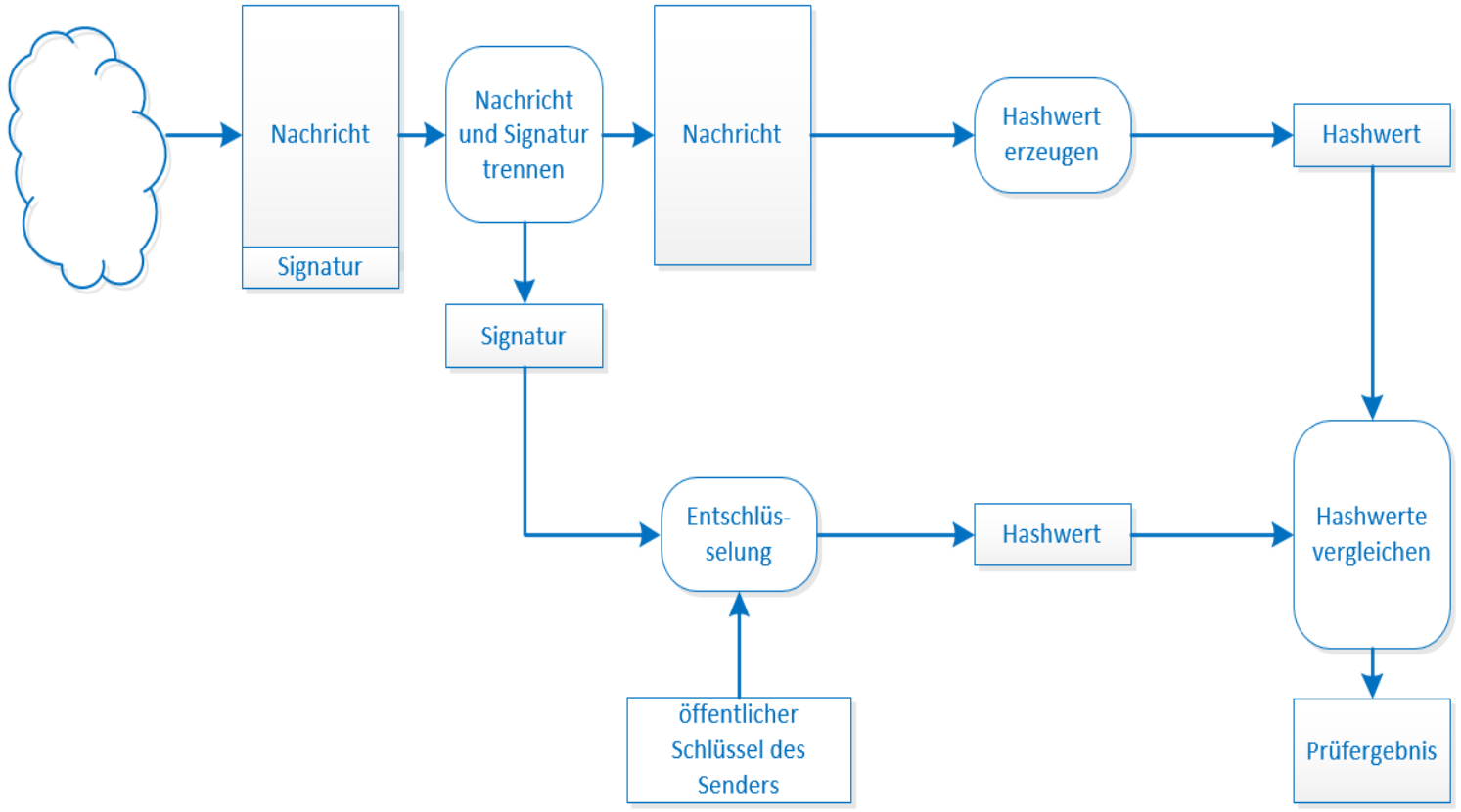


Abbildung 5:Signatur prüfen (Eigene Darstellung)

2 Signaturen

2.3 Public Key Infrastructure (PKI)

- Mittels PKI können digitale Zertifikate erzeugt, verteilt aber auch geprüft werden
- Es soll sichergestellt werden, dass ein öffentlicher Schlüssel tatsächlich vom Absender des Schlüssels stammt (und eben nicht ein Dritter vorgibt, der rechtmäßige Absender zu sein)
- Bestandteile einer PKI
  - Digitale Zertifikate
  - Zertifizierungsstelle
  - Zertifizierungssperrliste
  - Verzeichnisdienst
  - Weitere Dokumente und Informationen
  - (https://www.security-insider.de | www.pki.bayern.de)

VIELEN DANK!

Quellen

- Grafiken:
- https://storyset.com