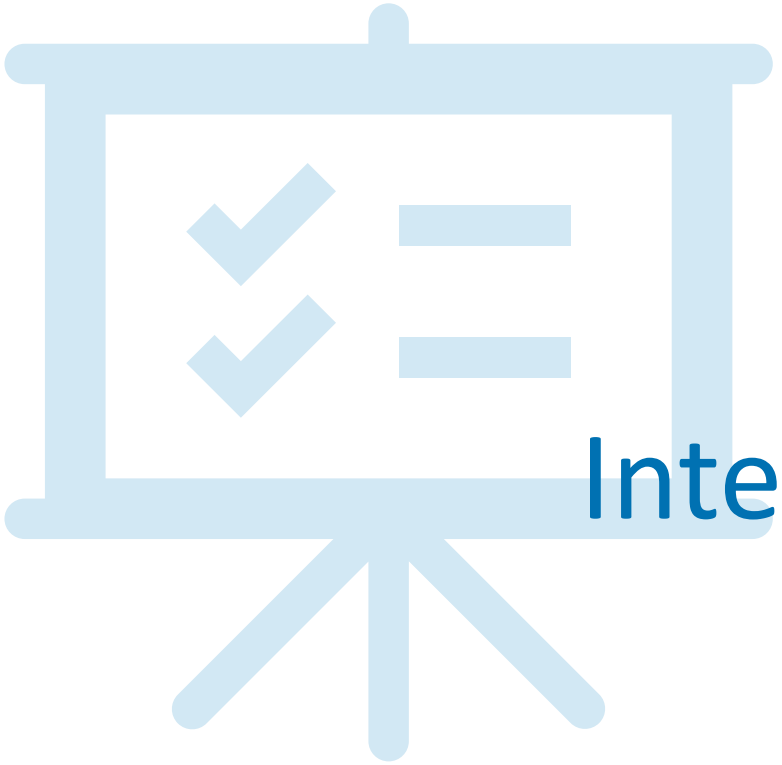

Netzwerke und Internettechnologien 1

Verschlüsselung

Netzwerke und Internettechnologien 1

Lernziele

1. Verschlüsselung Grundlagen

2. Digitale Signatur

3. Verschlüsselungsarten

Grundlagen Verschlüsselung

- Verschlüsselung ist der Vorgang, bei dem ein lesbarer Klartext mittels eines Verschlüsselungsverfahrens in einer „unleserliche“, nicht einfach interpretierbare Zeichenfolge umgewandelt wird.
- Ziele:
  - Die Vertraulichkeit einer Nachricht zu gewährleisten.
  - Die Integrität der Daten zu gewährleisten
  - Authentizität
  - Verbindlichkeit

Grundlagen Verschlüsselung

Unterschied von Steganographie zur Kryptographie

- Steganographie
  - Ist die verborgene Übermittlung oder Speicherung von Daten bzw. Informationen.
  - Ziel ist dabei, die Geheimhaltung und Vertraulichkeit einer Nachricht durch Tarnung zu gewährleisten.
  - Ist ein Versuch, eine sichere und nicht nachweisbare Kommunikation zu erreichen.
  - Ein Dritter soll die Existenz der steganographierten Information nicht erkennen.
- Kryptographie
  - Ist die Wissenschaft der Geheimhaltung von Informationen.
  - Die Daten werden dabei in eine Form überführt, die für Unberechtigte nicht zu lesen/zu verstehen ist.
  - Kryptografie erfordern dabei auch eine Möglichkeit für den Empfänger, die verschlüsselte Botschaft wieder lesbar zu machen.

Grundlagen Verschlüsselung

- Verschlüsselungsverfahren
  - Besteht aus einem Algorithmus zum Verschlüsseln und Entschlüsseln.
  - sowie Verfahren zum Schlüsselaustausch, Prüfung der Authentizität und Integrität.
  - Die bekannten Verschlüsselungsverfahren teilen sich in symmetrische, asymmetrische und hybride Verschlüsselungsverfahren auf.
  - Bei den hybriden Verschlüsselungsverfahren wird ein symmetrisches und asymmetrisches Verschlüsselungsverfahren miteinander kombiniert.

Grundlagen Verschlüsselung

- Verschlüsselungsalgorithmus
  - Ein mathematisches Verfahren zur Umwandlung eines Klartextes in einen Geheimtext.
  - Dem Algorithmus wird der Klartext und ein Schlüssel übergeben.
  - Nur mit dem Schlüssel kann man mit demselben Algorithmus den Geheimtext wieder in den Klartext umwandeln.

Grundlagen Verschlüsselung

- Ein Kriterium für die Sicherheit einer Verschlüsselung ist die Anzahl möglicher Schlüssel und eine möglichst überschaubare Anzahl schwacher Schlüssel.
  - Ein Schlüssel mit einer Länge von 1.024 Bit, also eine Folge von 1.024 Nullen und Einsen, ist sicherer als ein Schlüssel mit nur 64 Bit.
  - Selbst wenn man weiß, wie die Verschlüsselung arbeitet, müsste man alle möglichen Schlüssel durchprobieren, um irgendwann den richtigen Schlüssel zu bekommen.
  - In der Regel gilt, je länger ein Schlüssel ist, desto schwieriger ist es an eine verschlüsselte Information ohne Schlüssel zukommen.

Grundlagen Verschlüsselung

- Eine starke Verschlüsselung ist sicher. Verschlüsselung ist immer ein Spagat zwischen Sicherheit und Komfort.
- Absolute Sicherheit gibt es nicht. Man kann nur den Aufwand erhöhen. Mit Verschlüsselung erkauft man sich also nur Zeit, bis jemand einen Weg findet, an den Klartext der verschlüsselten Daten zu kommen.
  - Im Gegensatz zu oft verlautbarten Mitteilungen sind Geheimdienste, wie die NSA (USA), nicht in der Lage jede Verschlüsselung zu knacken.
  - Unter der Voraussetzung, dass die Schlüssel lang genug sind, das Passwort für den privaten Schlüssel stark genug ist und der private Schlüssel auch geheim ist und bleibt, ist Verschlüsselung sicher.

Verschlüsselungsarten

Symmetrische Verschlüsselung

- Es wird ein Schlüssel zum ver- und entschlüsseln genutzt.
- Der Schlüssel muss zwischen den Kommunikationspartnern ausgetauscht werden.
- Gelangt ein dritter in Besitz des Schlüssels kann er sich als einer der beiden Kommunikationsteilnehmer ausgeben, oder die Informationen lesen.
- Vorteil:
  - Ist auch bei großen Datenmengen schnell und verbraucht wenig Ressourcen.
- Nachteil:
  - Ein sicherer Schlüsselaustausch ist vor der Kommunikation notwendig.

Symmetrische Verschlüsselung

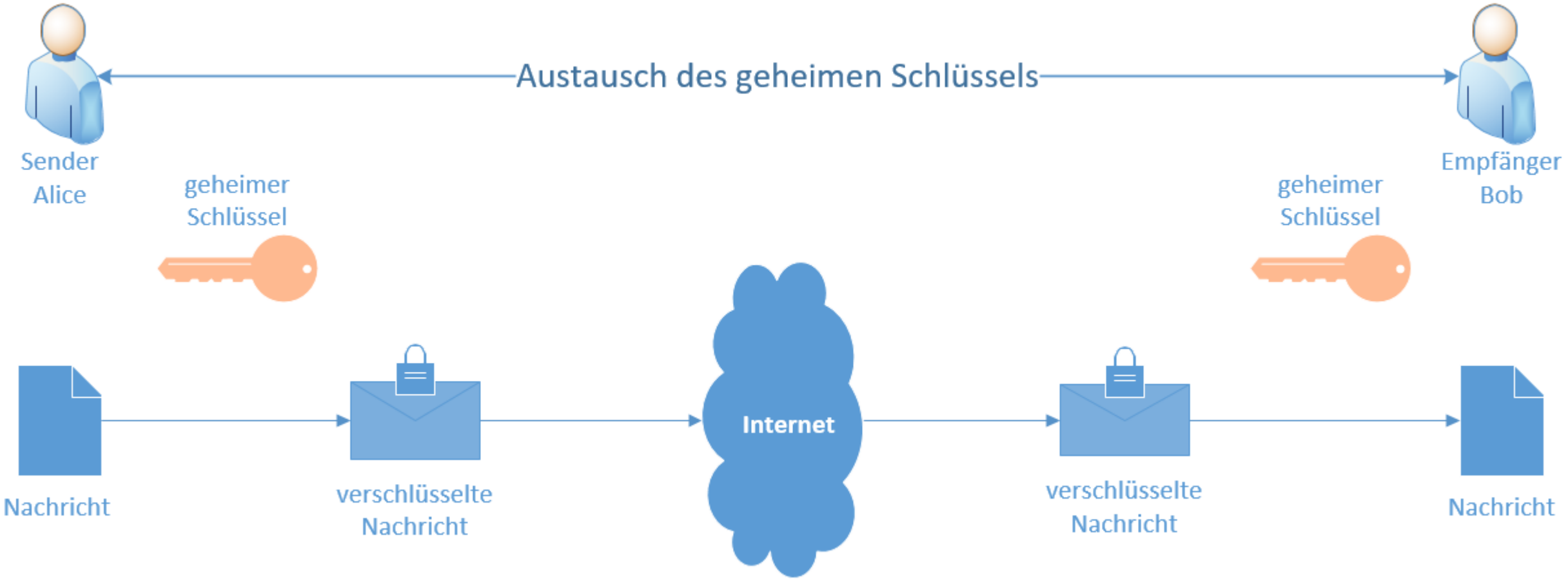

Abbildung 1: symmetrische Verschlüsselung (Eigene Darstellung)

Symmetrische Verschlüsselung

- Beispielhafte Verfahren sind:
  - Caesar Chiffre
  - Data Encryption Standard (DES)
  - Advanced Encryption Standard (AES)
  - Blowfish
  - usw.

Asymmetrische Verschlüsselung

- Jedem Kommunikationsteilnehmer gehört ein Schlüsselpaar, bestehend aus Public-Key und Private Key
  - Nur der Privat-Key muss geheim gehalten werden.
  - Mit dem Public Key kann jeder Nachrichten verschlüsseln, kann frei verteilt werden.
  - Nur mit dem dazugehörigen Private Key können Nachrichten entschlüsselt werden
- Werden auch häufig als Public-Key-Verfahren bezeichnet

Asymmetrische Verschlüsselung

- Vorteil:
  - Schlüsselaustausch über unsichere Netze problemlos möglich.
- Nachteil:
  - Hoher Ressourcenverbrauch und, im Vergleich zu symmetrischen Verfahren, sehr langsam.

Asymmetrische Verschlüsselung

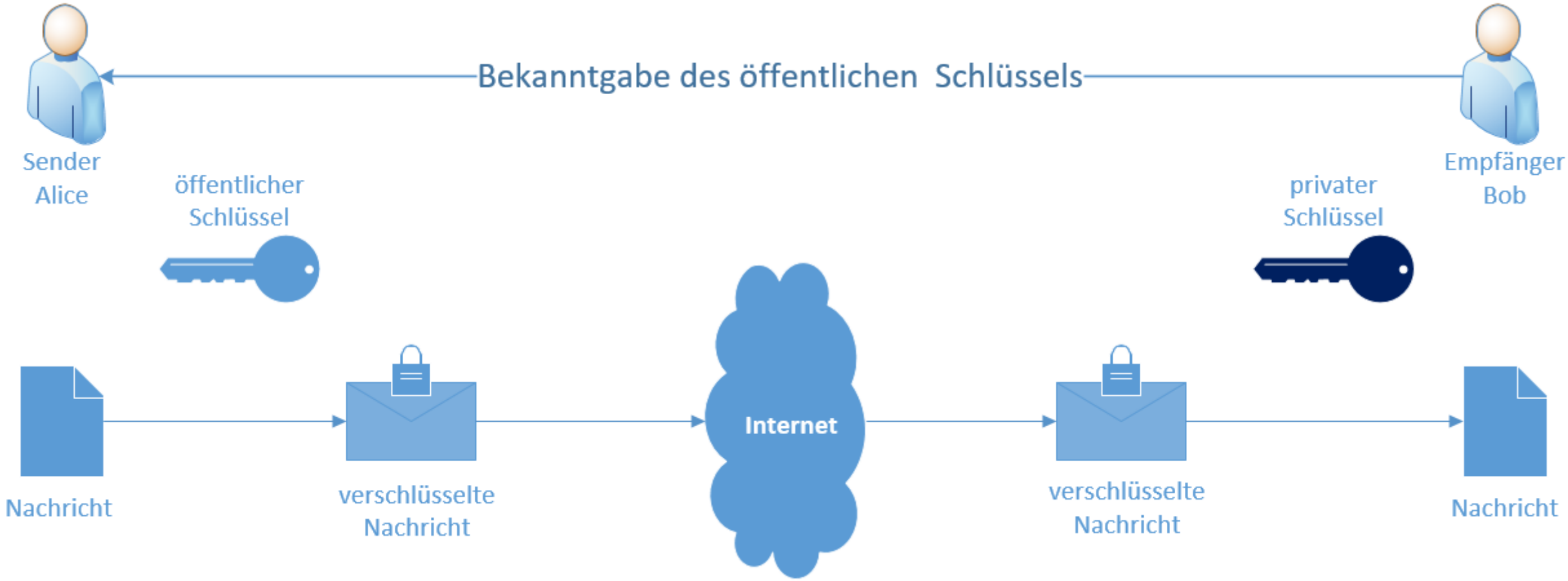

Abbildung 2: asymmetrische Verschlüsselung (Eigene Darstellung)

Asymmetrische Verschlüsselung

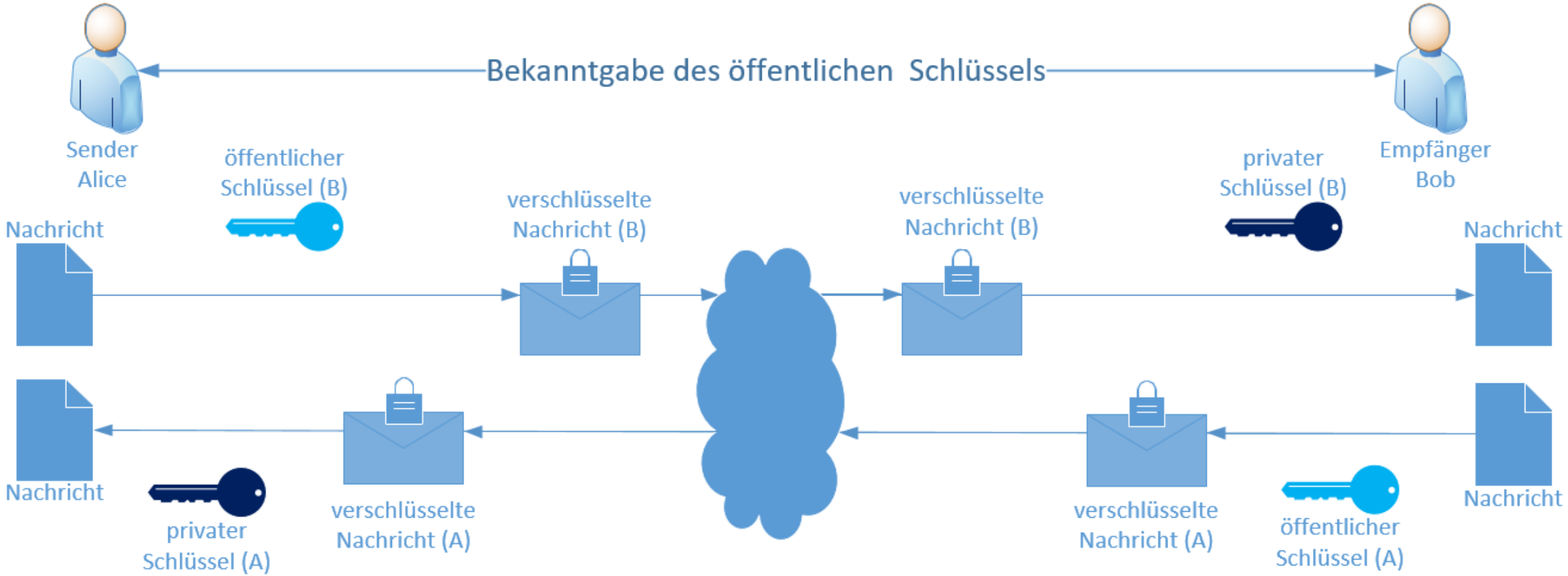

Abbildung 3: symmetrische Verschlüsselung (Eigene Darstellung)

Asymmetrische Verschlüsselung

- Beispielhafte Verfahren sind:
  - RSA
  - Merkle-Hellmann
  - Benaloh

Hybride Verschlüsselung

- Ist die Kombination aus asymmetrischer und symmetrischer Verschlüsselung
- Es wird ein zufälliger symmetrisch Schlüssel erstellt (Session Key)
- Mit diesem Session Key werden die Daten bei der Übertragung symmetrisch verschlüsselt.
- Der Session Key wird vor Übermittlung mit dem öffentlichem Schlüssel des Empfängers asymmetrisch verschlüsselt und an den Empfänger gesendet.
- Damit soll das „Schlüsselverteilungsproblem“ gelöst werden und der Geschwindigkeitsvorteil der symmetrischen Verschlüsselung genutzt werden

Hybride Verschlüsselung

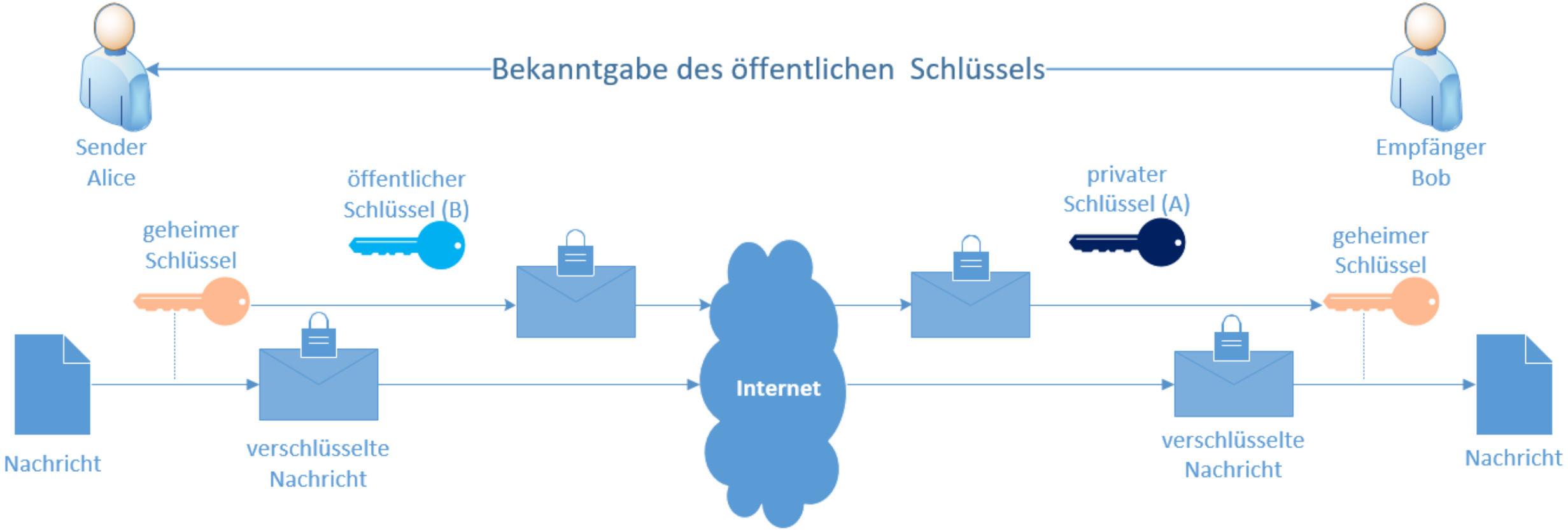

Abbildung 4: hybride Verschlüsselung (Eigene Darstellung)

Hash-Verfahren (Einweg-Verschlüsselung)

- Eine Einweg-Verschlüsselung ist, wie der Name es bereits andeutet, eine Verschlüsselungsform, die nicht wieder rückgängig gemacht werden kann.
- Aus einem beliebigen Datensatz eine Zeichenkette mit fester Länge, als Hashwert oder kryptografische Prüfsumme bezeichnet.
- Die Echtheit einer Nachricht wird überprüft, indem der selbst errechnete Hashwert mit dem übermittelten Hashwert verglichen wird.
- Stimmen beide Ergebnisse überein, wurde die Nachricht während der Übertragung nicht modifiziert.
- Verfahren:
  - MD5 (veraltet unsicher)
  - SHA (Secure Hash Algorithm), z.B. SHA1, SHA2, SHA3
  - RIPEMD-160

Digitale Signatur

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.

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.

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 Identität des Unterzeichners überprüfen.

Digitale Signatur erstellen

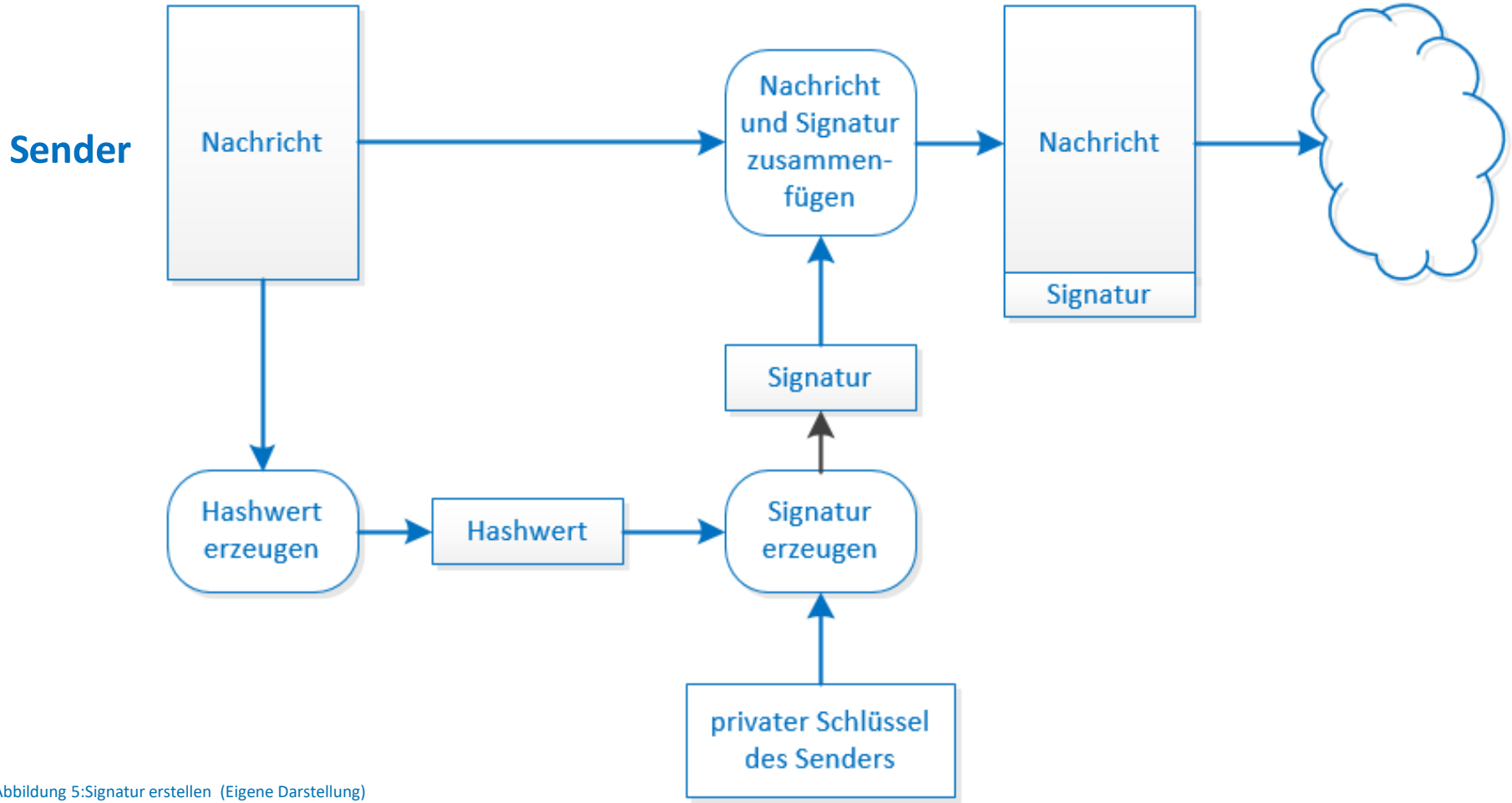

Abbildung 5:Signatur erstellen (Eigene Darstellung)

Digitale Signatur überprüfen

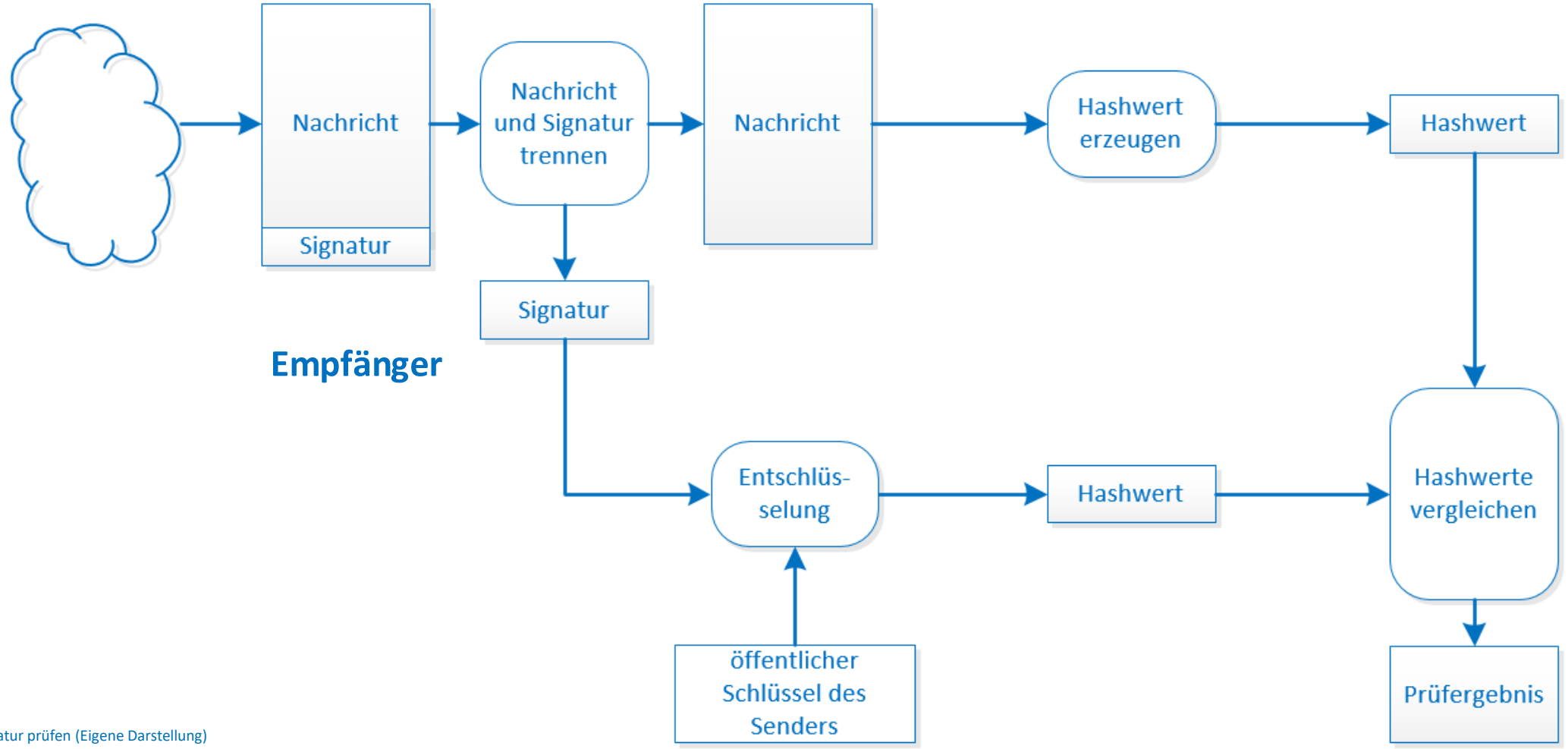

Abbildung 6: Signatur prüfen (Eigene Darstellung)

Quellen

Buchquelle

NAT - Network Address Translation (2021). Online verfügbar unter https://www.elektronik-kompendium.de/sites/net/0812111.htm, zuletzt aktualisiert am 30.04.2021, zuletzt geprüft am 30.04.2021.

Kersken, Sascha (2017): IT-Handbuch für Fachinformatiker. Der Ausbildungsbegleiter. 8. Auflage, revidierte Ausgabe. Bonn: Rheinwerk Verlag; Rheinwerk Computing.

Schreiner, Rüdiger (2014): Computernetzwerke. Von den Grundlagen zur Funktion und Anwendung. 5., erw. Aufl. München: Hanser.

Abbildungen

VIELEN DANK!