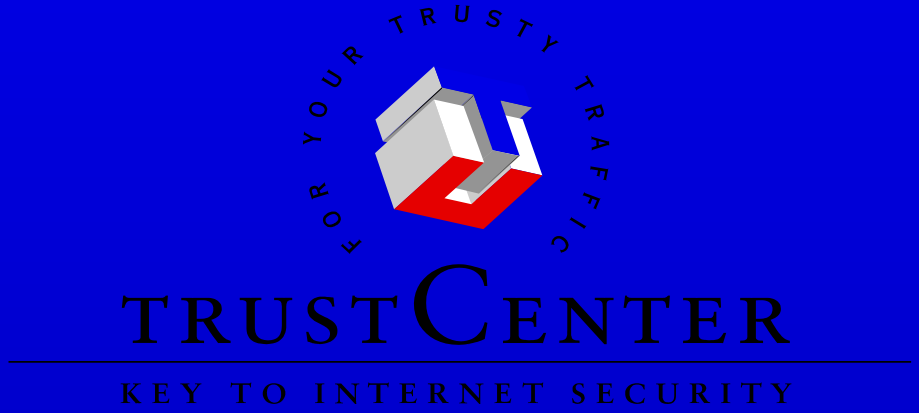
Verschlüsselung und Digitale Signaturen



Verschlüsselungsverfahren:

- Symmetrische Verschlüsselung

- Asymmetrische Verschlüsselung

Symmetrische Verschlüsselung

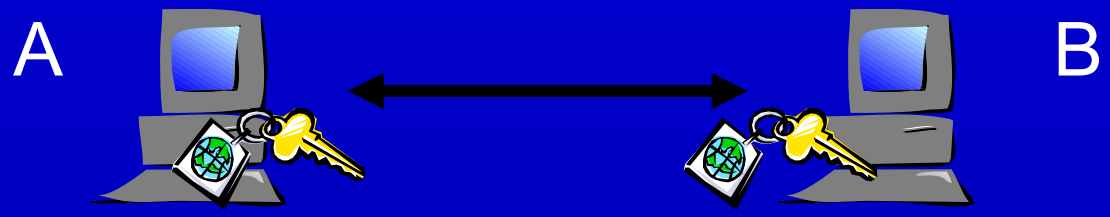
Vorteil:

- **Verschlüsselung ist sehr schnell**

Nachteil:

- **Schlüsselverteilungsproblem: Wie bekomme ich einen symmetrischen Schlüssel über einen unsicheren Kanal?**

Algorithmen: DES, 3DES, IDEA, RC2, RC4



Asymmetrische Verschlüsselung

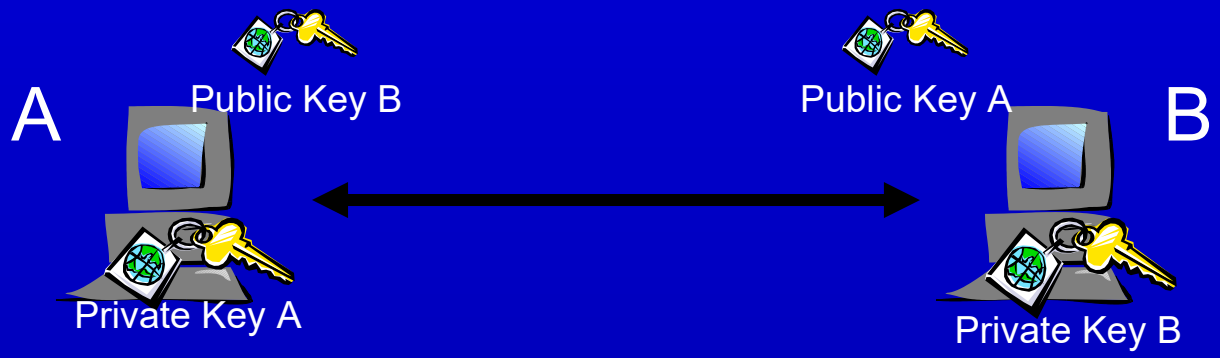
Vorteil:

- **Schlüsselverteilungsproblem ist gelöst, da der Transport der Public Key über unsicheren Kanal unkritisch ist.**
- **Private und Public Key sind komplementär zueinander**

Nachteil:

- **Asymmetrische Verschlüsselung ist zeitintensiv**

Algorithmen: RSA, DSA



Hybridverfahren

- Kombination beider Verschlüsselungsverfahren
- Daten werden mit symm. Schlüssel verschlüsselt
- Symm. Schlüssel wird mit Public Key des Empfängers verschlüsselt

Vorteil:

- Schlüsselverteilungsproblem ist gelöst und die Verschlüsselung kann trotzdem sehr schnell durchgeführt werden

Sicherheit der Schlüssellängen

Angriffe auf Systeme mit Brute-Force

Unter dem Begriff „Brute-Force“ versteht man ein Programm, welches mit sehr hoher Geschwindigkeit ein Passwort nach dem anderen ausprobiert. In solche Programme werden auch die „Wortbuchdateien“ herein geladen. Findet er das gesuchte Passwort nicht in der „Wortbuchdatei“, dauert der Suchvorgang erheblich länger. Früher oder später kommt das Programm auf das richtige Passwort.

Binärschlüsselgröße	Schlüsselraumgröße	Zeit zum Durchtesten aller Schlüssel
16 Bit	$65536 \approx 6{,}6 * 10^4$	0,07 Sekunden
32 Bit	$4294967296 \approx 4{,}3 * 10^9$	72 Minuten
64 Bit	$\approx 1{,}8 * 10^{19}$	584942 Jahre
128 Bit	$\approx 3{,}4 * 10^{38}$	$1{,}1 * 10^{25}$ Jahre
256 Bit	$\approx 1{,}2 * 10^{77}$	$3{,}7 * 10^{63}$ Jahre

Digitale Signaturen

– Verschlüsselung sichert die Vertraulichkeit

Aber:

– Wer ist der Absender ?

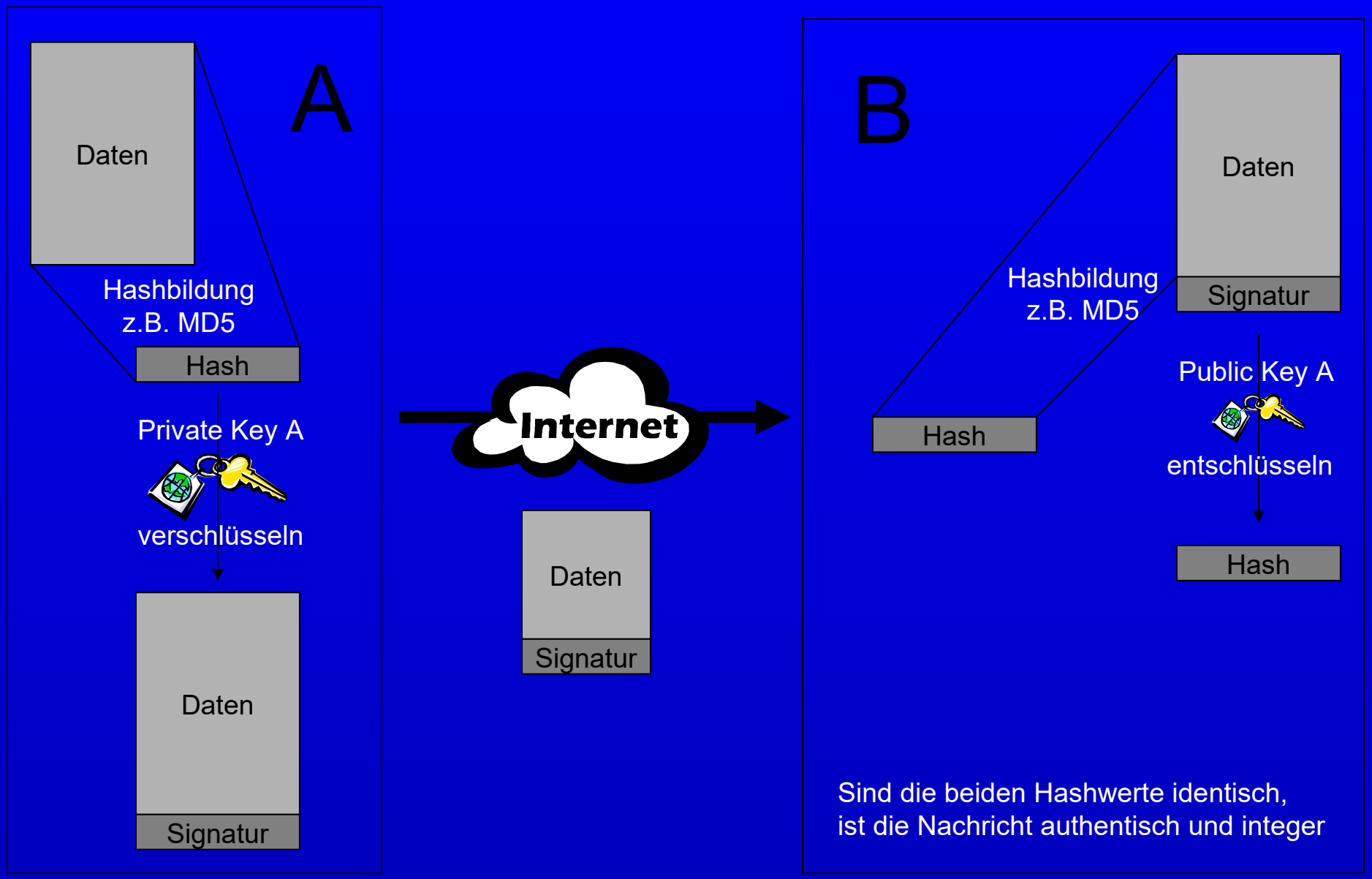
– Wurden die Daten von Dritten verändert ?

Lösung:

– Eindeutige Abbildung der Daten auf einen Bitstring (Hashwert)

– Hashwert wird mit privatem Schlüssel des Absenders verschlüsselt und bildet die Signatur

Digitales Signieren und Verifizieren



Kombinationen

– Verschlüsseln (Vertraulichkeit)

– Signieren (Integrität, Authentizität)

– Verschlüsseln und Signieren

Aber:

– Ein Dritter könnte sich für Kommunikationspartner ausgeben und öffentlichen Schlüssel unter falschen Namen publizieren

Zertifikate

„Zertifikat für elektronische Signaturen“ ist eine elektronische Bescheinigung, die elektronische Signaturvalidierungsdaten mit einer natürlichen Person verknüpft und die mindestens den Namen oder das Pseudonym dieser Person bestätigt.“
(VERORDNUNG (EU) Nr. 910/2014 Artikel 3)

– Zertifikate werden von Vertrauensdiensteanbietern (häufig auch Trustcentern bzw. Certficate Authorities (CA)) ausgestellt

Aufgaben eines Trustcenters

- Antragstellung und Registrierung
- Identifizierung
- Zertifikatsausstellung
- Verzeichnis- und Zeitstempeldienst
- Sperrmanagement
- Schlüsselgenerierung

Zertifikate - für wen?

- Personen
- Organisationen
- Webserver
- Software

Zertifikatstypen (Beispiele)

- PGP-Zertifikate
  - Email
  - Dateiverschlüsselung
- X.509-Zertifikate
  - Email (S/MIME)
  - SSL-Verbindungen / „Sicheres Browsen“
  - Dateiverschlüsselung

Was enthält ein Zertifikat

X.509:

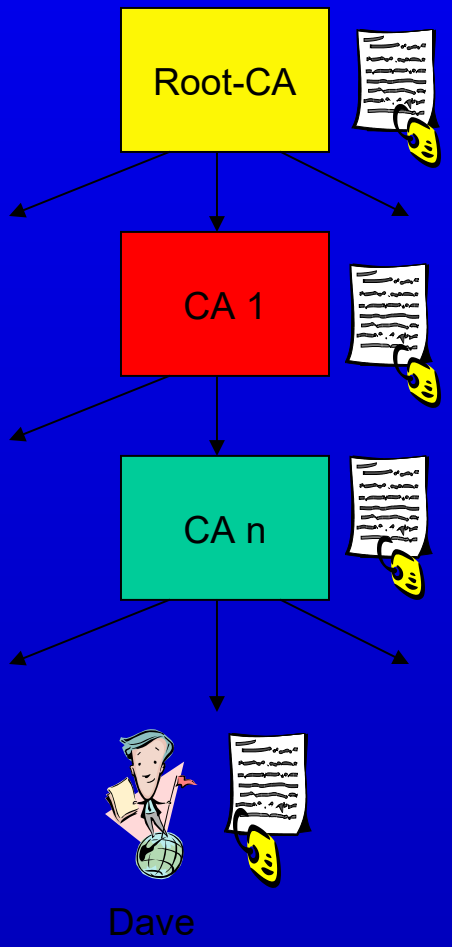
- Angaben zur Person (Name, Firma, Abteilung, Land, Bundesland, Ort, Email, etc.)
- Seriennummer
- Aussteller
- Gültigkeitsdauer
- Öffentlichen Schlüssel
- Signatur eines Trustcenters
- Extensions

PGP V. 5.X

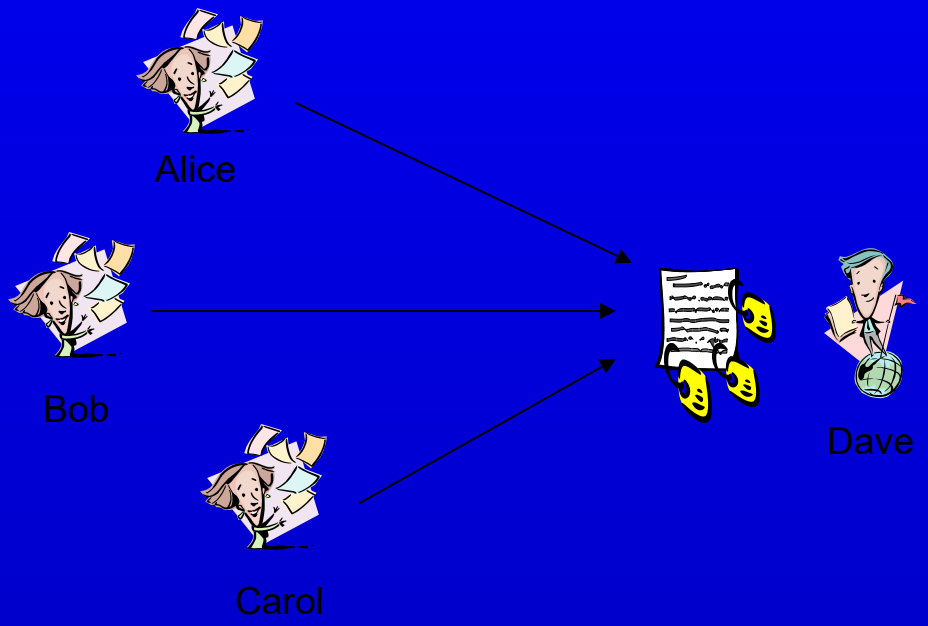
- Angabe zur Person (Name, Email)
- Gültigkeitsdauer (optional)
- Öffentlicher Schlüssel
- Signaturen Dritter

Zertifikatshierarchie

X.509 - Certificate chain



PGP - Web of Trust



X509-Zertifikat

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 126636 (0x1eeac)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=DE, ST=Hamburg, L=Hamburg, O=TC TrustCenter for Security in Data Networks GmbH, OU=TC TrustCenter Class 3
CA/Email=certificate@trustcenter.de
 Validity
            Not Before: Nov 18 15:22:37 1998 GMT
            Not After : Nov 18 15:22:37 1999 GMT
        Subject: C=DE, ST=Bremen, L=Bremen, O=, OU=, CN=Stephan Hiller/Email=hiller@trustcenter.de
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:bf:37:be:d2:f8:33:cd:1c:60:b8:a5:bf:51:04:
                    71:8c:b4:29:c4:39:93:24:da:b5:f4:55:34:fc:bf:
                    07:0b:fc:77:bd:fa:86:b9:b5:98:2f:5b:fe:9b:8e:
                    99:b9:65:2b:8a:5e:30:e1:7c:16:8a:28:fe:5a:6c:
                    b2:47:56:83:73:ba:73:86:c2:01:d5:ad:69:25:54:
                    81:b9:45:c7:78:6c:3a:12:2b:f8:43:a8:d1:8a:81:
                    57:d1:92:e3:51:43:f0:22:87:4c:e5:96:23:de:5e:
                    41:5e:c8:82:6d:d7:6e:f9:c1:9d:06:03:34:42:61:
                    bc:5c:39:9a:2f:11:80:a5:0b
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            Netscape Revocation Url:
                https://www.trustcenter.de/cgi-bin/check-rev.cgi/01EEAC?
            Netscape Renewal Url:
                https://www.trustcenter.de/cgi-bin/Renew.cgi?
            Netscape CA Policy Url:
                http://www.trustcenter.de/guidelines/index.html
            Netscape Comment:
                TC TrustCenter Class 3
            Netscape Cert Type:
                ....
    Signature Algorithm: md5WithRSAEncryption
        7d:80:98:2d:56:35:b5:d7:d9:c2:a6:a8:db:d5:80:2d:f7:89:
        55:99:2d:34:04:7a:fb:c1:ec:30:64:0e:2f:43:a5:45:e0:70:
        81:15:a0:5a:f0:c6:a3:cd:c1:d2:9b:87:fb:46:a3:a1:2d:8b:
        ba:d7:12:25:1f:53:30:13:03:75:9d:97:59:b7:31:3b:fb:29:
        77:d5:08:46:80:d0:1d:7b:c5:be:81:5c:ba:b1:d9:86:44:09:
        d9:73:fe:59:3f:df:c7:24:bf:45:84:48:f2:08:0e:00:d9:87:
        1f:ef:60:6e:c1:62:f4:1c:00:08:e3:43:b9:98:f5:2d:da:0a:
        ff:3e
```

CRL (Certificate Revocation List)

- Sperrliste mit kompromittierten Zertifikaten
- Enthält Seriennummer des Zertifikates mit Signatur der CA
- Wird in regelmäßigen Intervallen veröffentlicht

Aber:

- Ist nicht immer aktuell

Online-Abfrage über OCSP oder LDAP

- Zertifikatsstatus ist immer aktuell

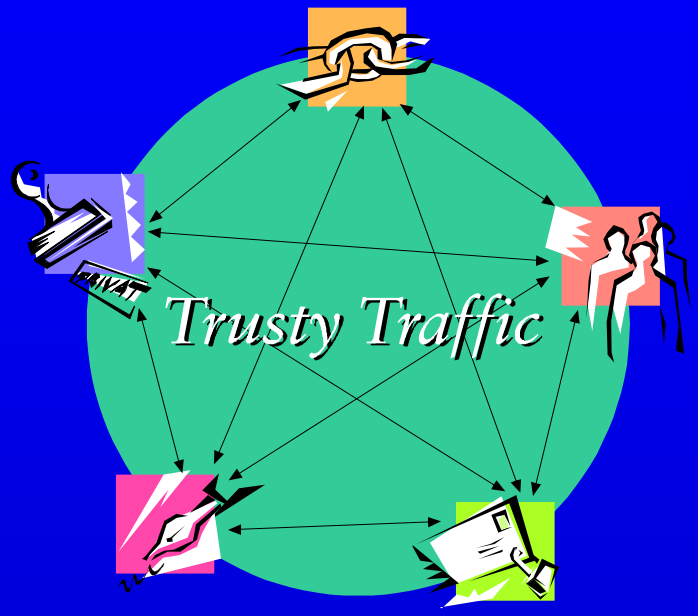
Aber:

- Erfordert große Bandbreite beim OCSP-Responder bzw. LDAP-Server der CA

Anwendungen

- Telearbeit
- Online-Shopping
- Elektronische Bankgeschäfte
- E-Mail
- Intranet Anwendungen
- Online-Reisebuchung
- Verbindliche Verträge
- Online-Behördengänge
- Sicheres „Surfen“

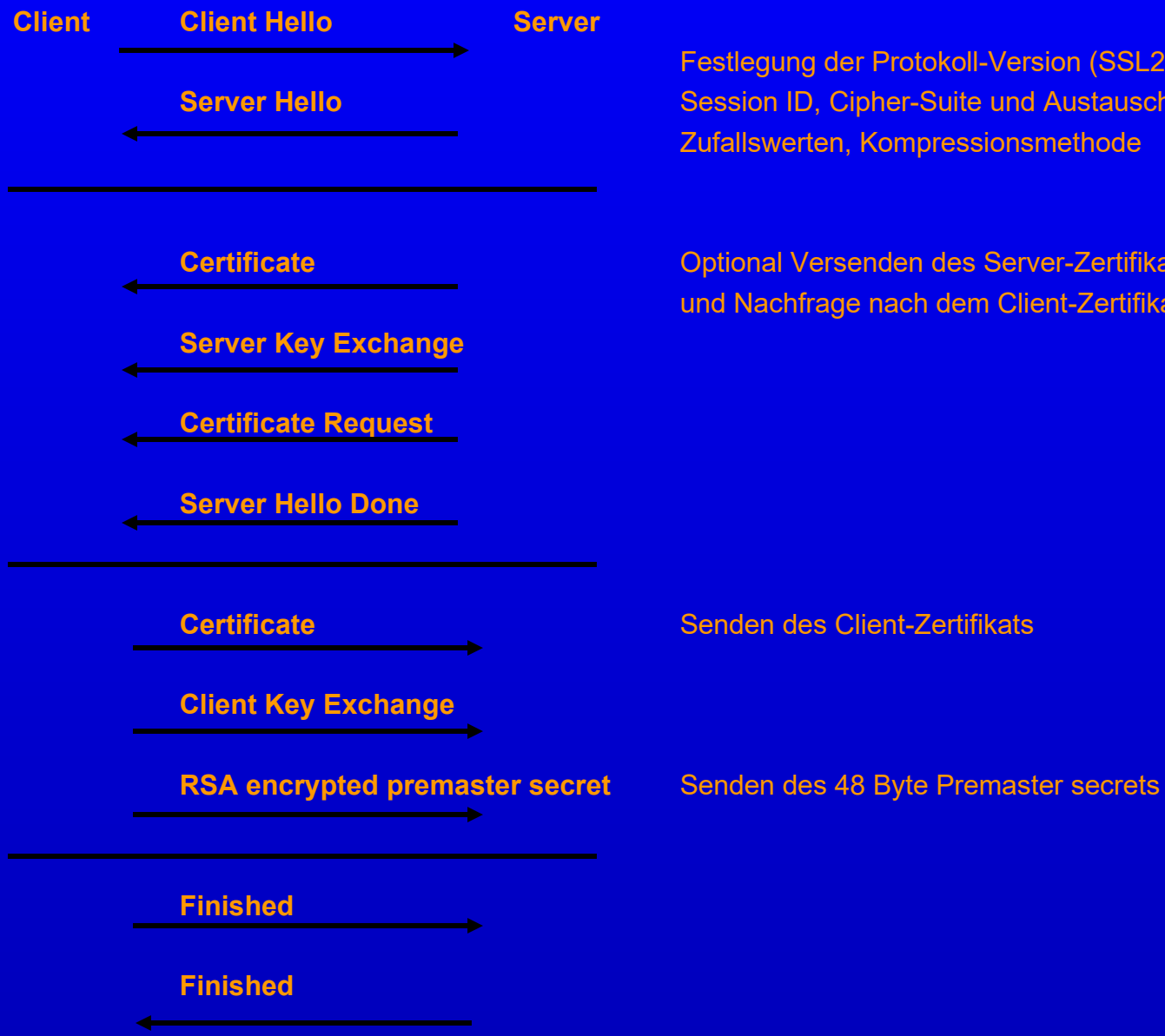
etc.



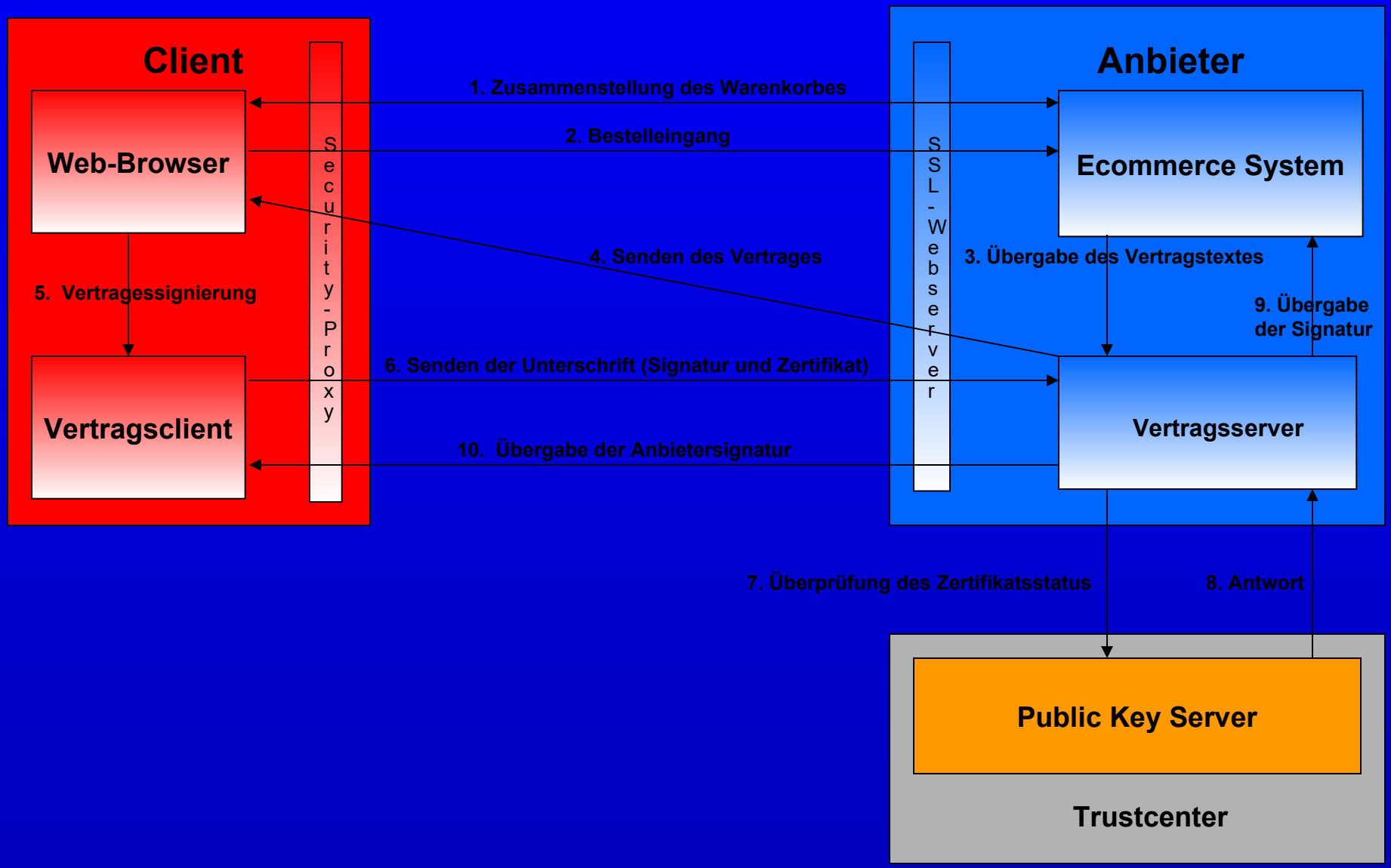
SSL-Protokoll

- Entwicklung von Netscape (1994)
- Bietet die Möglichkeit der End-zu-End-Verschlüsselung, Authentifizierung und Integritätsüberprüfung
- Basiert auf X.509-Zertifikaten
- Unabhängig von Protokollen der Applikationsschicht (HTTP, Telnet, FTP)

SSL-Handshake



Vertragsanwendung



Gesetzliche Grundlagen

- EU-Verordnung Nr. 910/2014 und Vertrauensdienstegesetz (VDG) v. 18.7.2017
- VDG regelt Genehmigung von Zertifizierungsstellen, Inhalt, Vergabe und Sperrung von Zertifikaten, Zeitstempeldienste etc.
- VDG schafft die Rahmenbedingungen für die rechts-verbindliche digitale Signatur
- VDG regelt die Anforderungen für den Betrieb einer Zertifizierungsinstanz / Trustcenter

Vertrauensdienstegesetz: Anforderungen an das Trustcenter

- Zuverlässige Mitarbeiter
- Begrenzte Anzahl von Mitarbeitern darf zertifizieren
- Bauliche Maßnahmen
- Vier-Augen Prinzip
- Lückenlose und manipulationsfreie Protokollierung
- Signaturschlüssel sind nicht kopierbar
- Hohe Verfügbarkeit von Public Key Servern

Vielen Dank für Ihre Aufmerksamkeit