Designing Education
Connecting People

Schutzbedarfsanalyse im eigenen Arbeitsplatzbereich durchführen

Lernfeld 04

Das erwartet Sie:

- Verteidigungsmöglichkeiten

Die Themen

Kryptographie-Grundlagen

Lernziele

Klassische und Moderne Kryptographie

Hash-Grundlagen

Lernziele

Hashkryptographie

Steganographie

Lernziele

Grundlagen zu der Steganographie

Sonstige Verschlüsselung

Lernziele

Digitale Signatur, Zertifikate, PKI und PGP, SSL/TLS

Kennwortsicherheit

Lernziele

Grundlagen zur Kennwortsicherheit

©Urheber

Kryptographie-Grundlagen

Lernziele

Klassische und moderne Kryptographie

Kryptographie

Definition:

- Schutz der Daten vor Dritten durch Unkenntlichkeit
- Verschlüsselter Text = Ciphertext
- Text/Dateien werden durch einen Algorithmus und Schlüssel verschlüsselt
- Ohne beide Informationen ist keine Entschlüsselung möglich

- Klassische Kryptographie
- Moderne Kryptographie

„Crypto will not be broken, it will be bypassed“

- Adi Shamir -

Verschlüsselung wird nicht gebrochen, sie wird umgangen.

Verschlüsselungsziele

Vertraulichkeit

Nur Empfänger kann Nachricht lesen

Integrität

Empfänger kann feststellen, ob Nachricht bearbeitet worden ist

Authentizität

Absender soll identifizierbar sein

Verbindlichkeit

Urheber soll nicht abstreiten können, dass die Nachricht von ihm ist

Caesar-Verschlüsselung

Stammt vom Feldherren Gaius Julius Caesar (100 v. Chr. – 44 v. Chr.)

Klartext: Hier steht mein geheimer Text.

Schlüssel: 7

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G

Ciphertext: OPLY ZALOA TLPU NLOPTLY ALEA.

Vigenère-Verschlüsselung

Stammt vom Französischen Kryptographen Blaise de Vigenère (1523 – 1596)

Klartext: Wie gut, dass niemand weiß, dass hier mein geheimer Text steht.

Schlüssel: Geheimer Schluessel

W	i	e		g	u	t	,		d	a	s	s		n	i	e	m	a	n	d		w	e	i	ß	,		d	a	s	s
G	e	h		e	i	m			e	r	S	c		h	l	u	e	s	s	e		l	G	e	h			e	i	m	e
C	m	l		k	c	f	,		h	r	k	u		u	t	y	q	s	f	h		h	k	m	ß	,		k	e	a	e

Ciphertext: Cml kcf, hrku utyqsfh hkmß, keae lzwt tpcr ywlpoqlv Bqbk kvlsn.

XOR Verschlüsselung

Verschlüsselungsverfahren auf Basis des exklusiven Oder

Wahrheitstabelle:

A	B	A XOR B
0	0	0
0	1	1
1	0	1
1	1	0

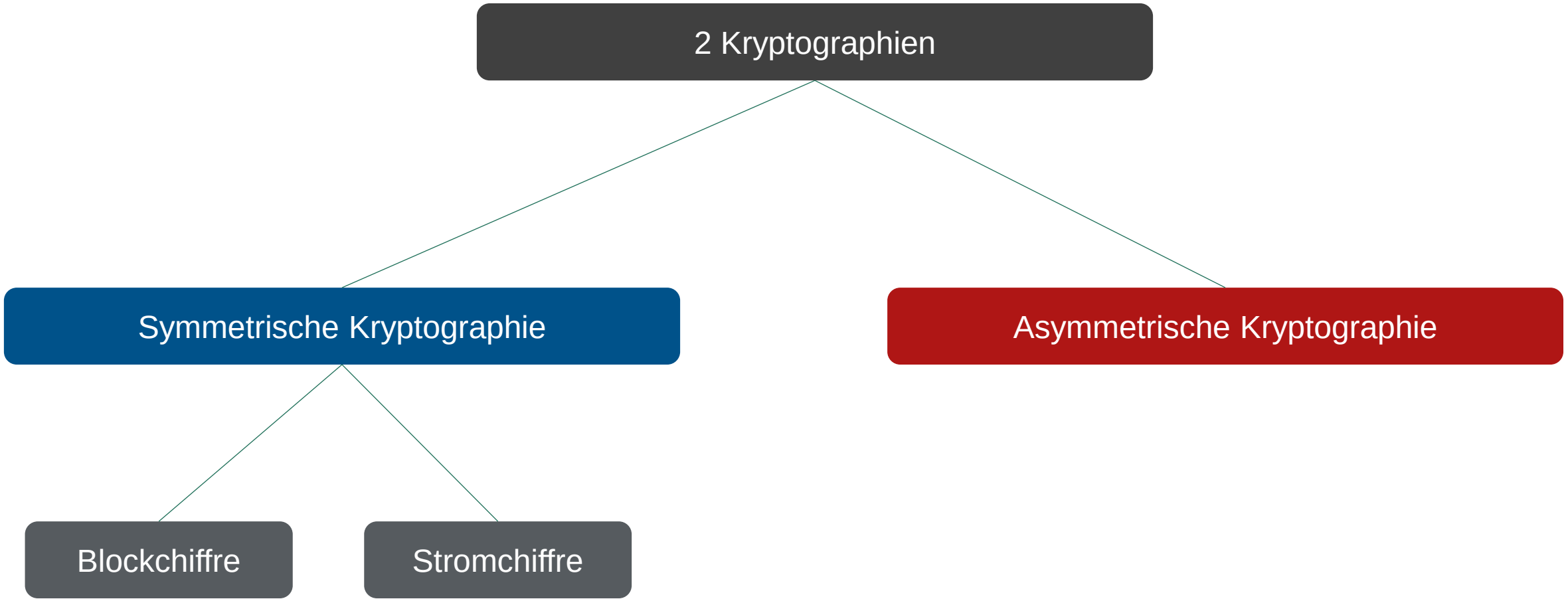
Klartext: 1001 1111 0011 1001 1010 1101 1101 1100 1100 1000 0000 0001 0011 1011 0101

Schlüssel: 1010 1100 1111 1011

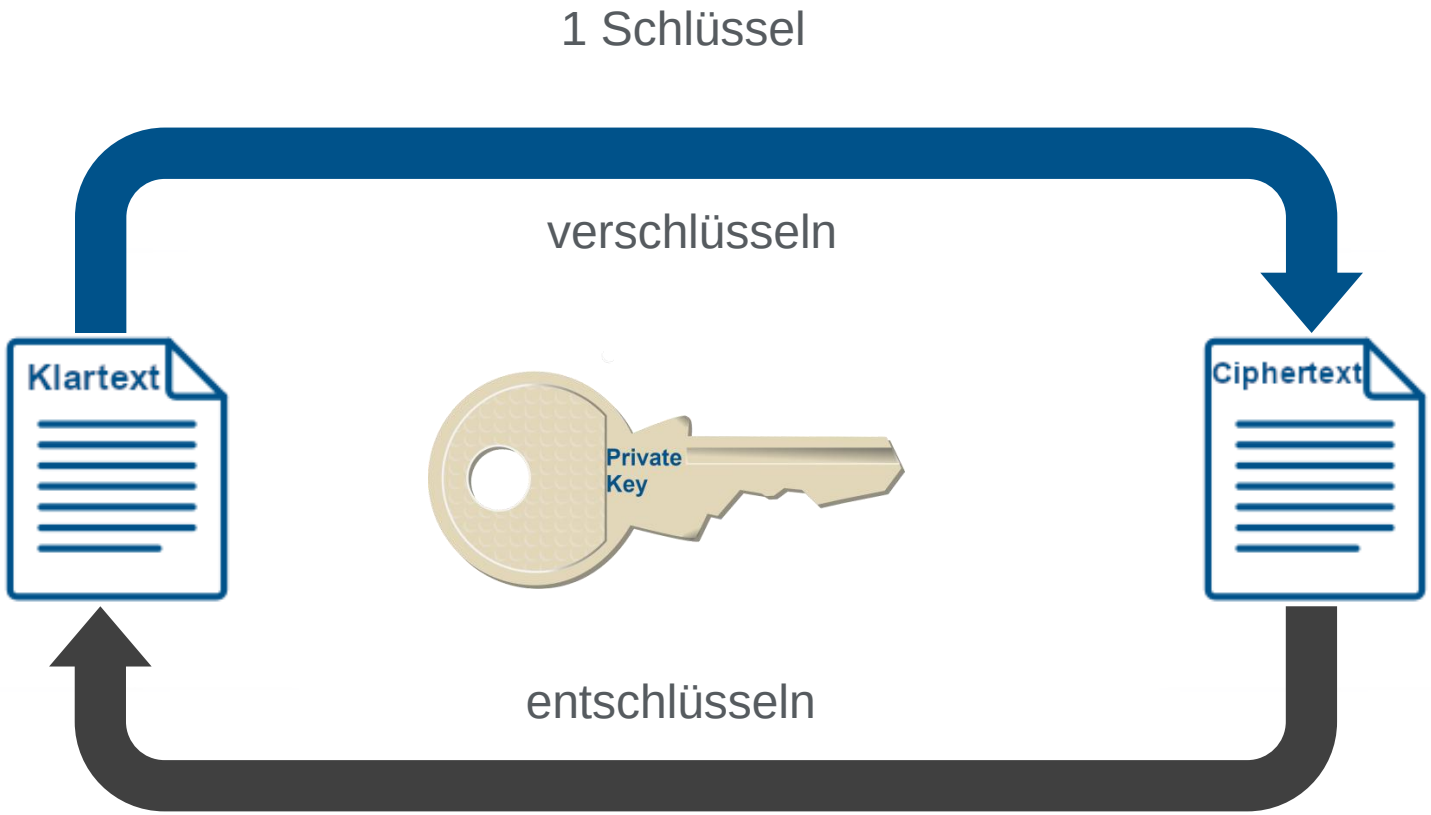
1	0	0	1	1	1	1	1	0	0	1	1	1	0	0	1	1	0	1	0	1	1	0	1	1	1	0	0	1	1	0	0
1	0	1	0	1	1	0	0	1	1	1	1	1	0	1	1	1	0	1	0	1	1	0	0	1	1	1	1	1	0	1	1
0	0	1	1	0	0	1	1	1	1	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	0	1	1	0	1	1	1

Ciphertext: 0011 0011 1100 0010 0000 0001 0011 0111 0010 1100 1110 1000 0001 1001

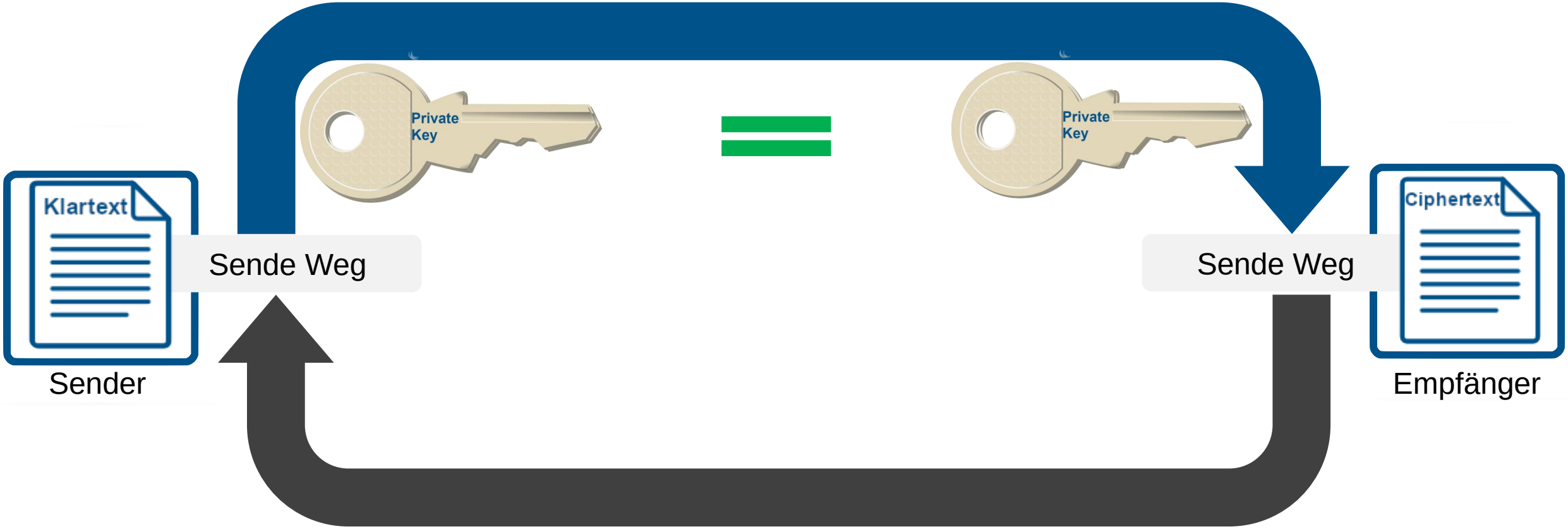
Moderne Kryptographie



Symmetrische Verschlüsselung



Symmetrische Verschlüsselung



Symmetrische Verschlüsselung

Algorithmen:

- DES
- 3DES
- AES
- Twofish/Blowfish
- Serpent
- RC

Vorteile:

- Einfaches Schlüssel-management (nur ein Schlüssel für Ver- und Ent-schlüsselung)
- Hohe Geschwindigkeit für Ver- und Ent-schlüsselung

Nachteile:

- Nur ein Schlüssel (Darf nicht an Unbefugte gelangen)
- Schlüssel muss über sicheren Weg übermittelt werden
- Anzahl der Schlüssel bezogen auf Anzahl der Teilnehmer (wächst quadratisch)

Symmetrische Verschlüsselung

DES – Data Encryption Standard
- Entwickelt 1977
- Schlüssellänge: 64 Bit
- Tatsächliche Verschlüsselung: 56 Bit
- Geknackt
- Anwendung: Geldautomat

3DES – Triple DES
- Entwickelt 1995
- Basierend auf DES
- Schlüssellänge 168 Bit
- EDE (Encrypt-Decrypt-Encrypt)
- Anwendung: TPM, OpenSSL

AES – Advanced Encryption Standard
- Rijndael-Algorithmus
- Schlüssellänge: 128 Bit, 192 Bit, 256 Bit
- AES-256 nicht sicherer als AES-128
- Gilt als sicher
- Anwendung: WLAN, SSH usw.

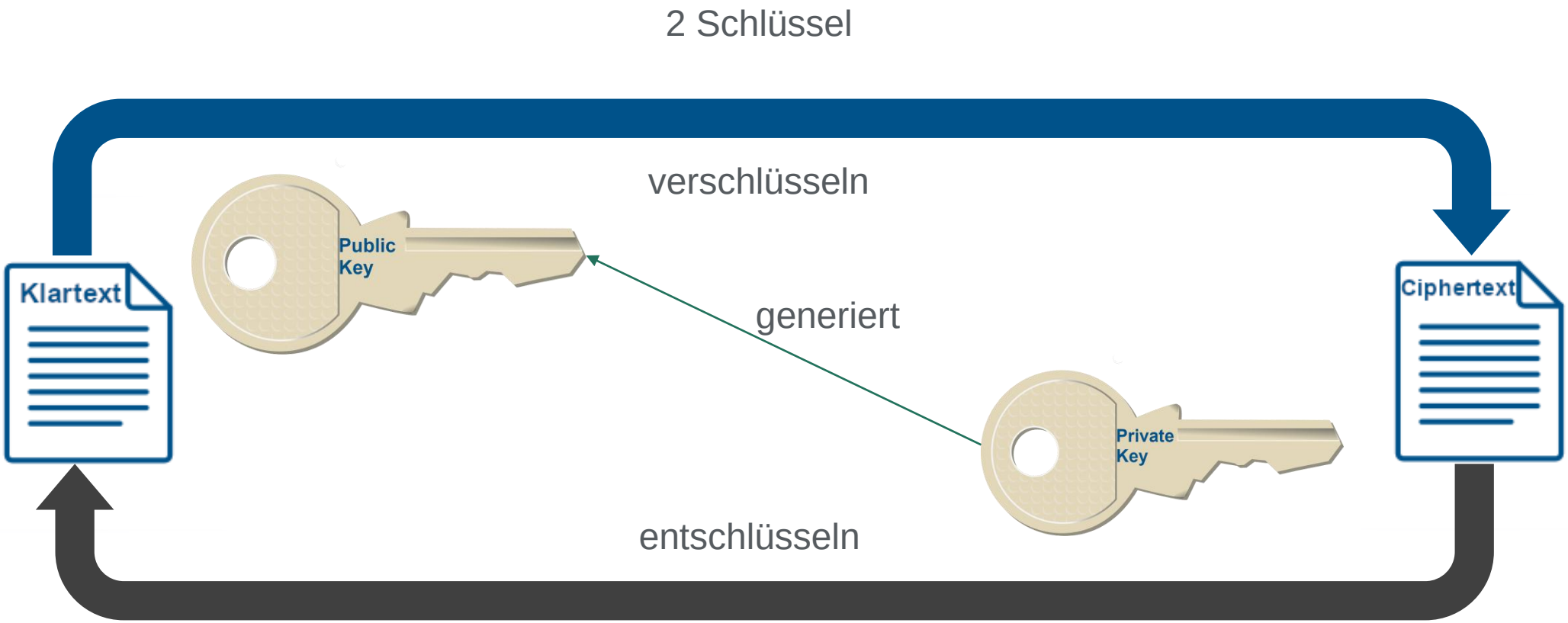
Symmetrische Verschlüsselung

Twofish/Blowfish
- Entwickelt 1998
- Twofish Nachfolger von Blowfish
- Schlüssellänge: 128 Bit,192 Bit, 256 Bit
- Twofish gilt als sicher
- Anwendung: GNU Privacy Guard

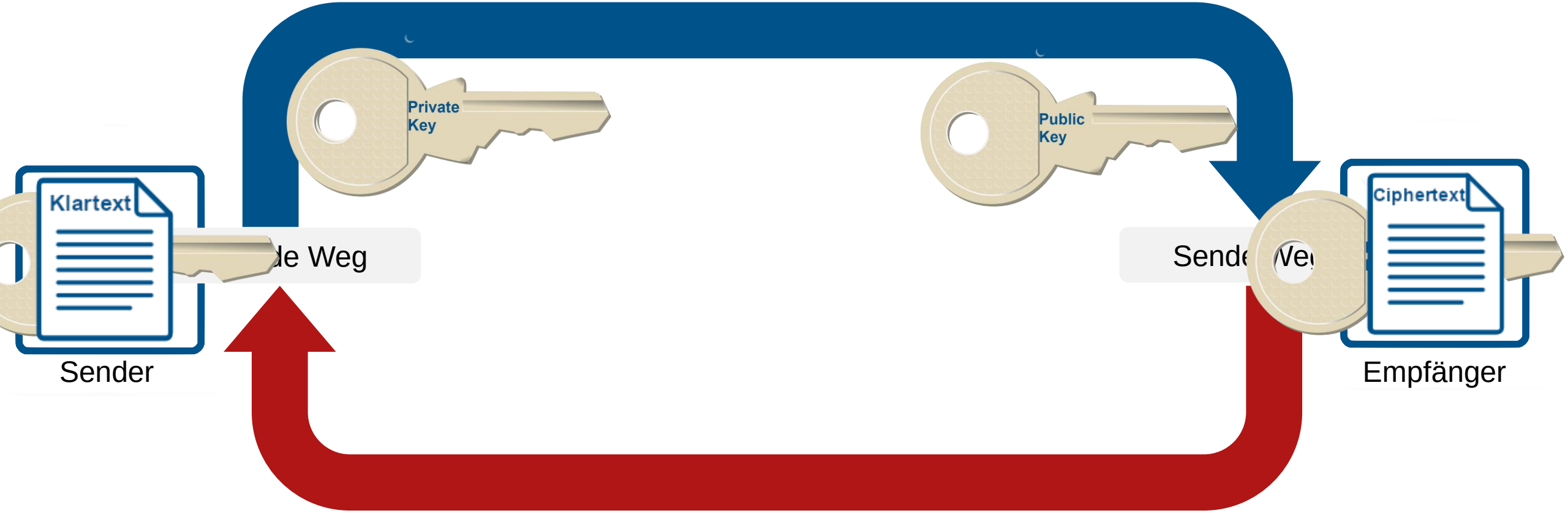
Serpent
- Gilt als sicherster Algorithmus
- Auch der langsamste
- Schlüssellänge: 128 Bit, 192 Bit, 256 Bit
- Gilt als sicher
- Anwendung: Public Domain

RC4
- Schlüssellänge: 128 Bit bis 2.048 Bit
- Stromchiffre
- Basis auf XOR-Algorithmus
- Sehr schnell (ca. 10 x schneller als DES)
- Anwendung: WLAN, SSH1, SSL

Asymmetrische Verschlüsselung



Asymmetrische Kryptographie



Asymmetrische Verschlüsselung

Algorithmen:

- ECC
- DH
- RSA
- Elgamal
- Digitale Signatur

Vorteile:

- Relativ hohe Sicherheit
- Nicht so viele Schlüssel wie bei der symmetrischen Verschlüsselung
- Geringerer Aufwand, Schlüssel geheim zu halten
- Kein Schlüsselverteilungs-problem
- Möglichkeit der Authentifikation durch elektronische Unterschrift

Nachteile:

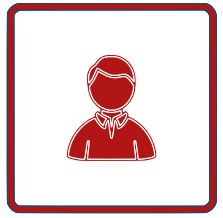
- Algorithmen arbeiten sehr langsam ca. 10.000-mal langsamer)
- Große benötigte Schlüssellänge
- Wenige verschie-dene Algorithmen

ECC – Eliptic Curve Cryptography

- Dient der Generierung des Public-Keys
- Alleinstehend sehr kritisch und unsicher

- Häufige Kombinationen:
- ECDH (Eliptic Curve Diffie-Hellman) – Schlüsselaustausch
- ECDSA (Eliptic Curve Digital Signature Algorithm) - Signaturverfahren

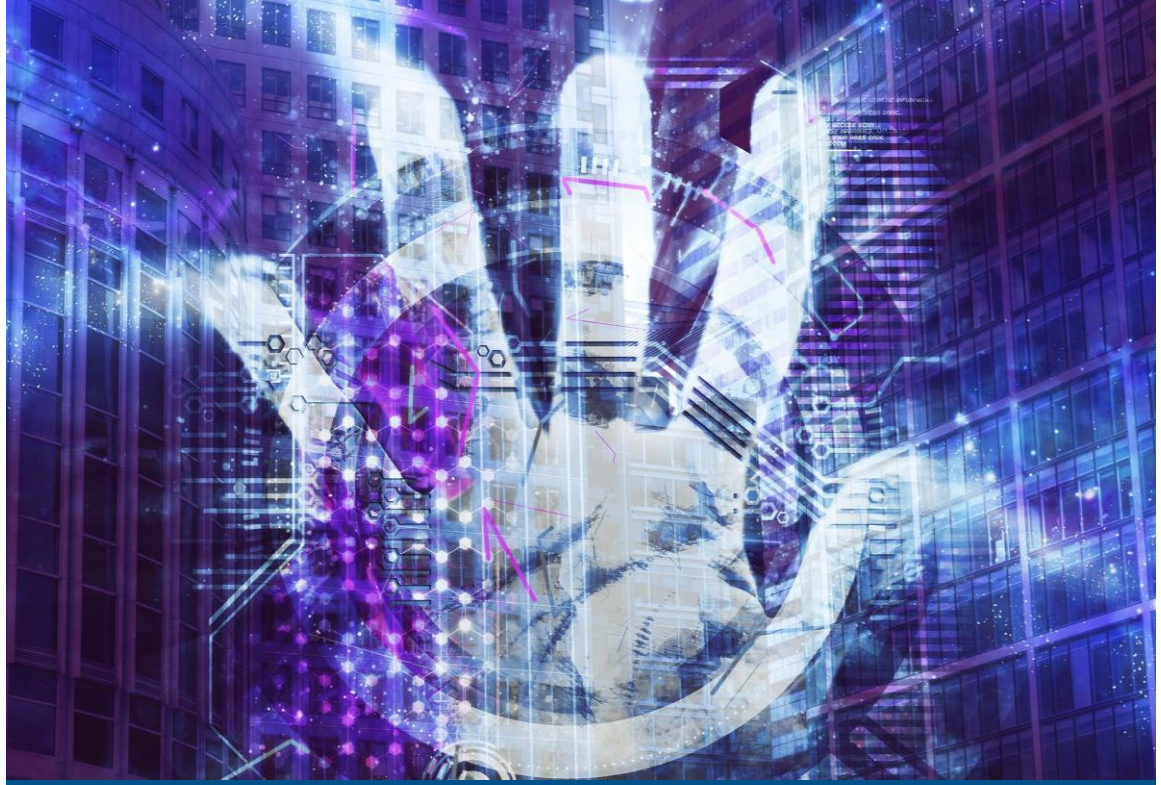
DH – Diffie-Hellman-Merkle

Alice	Susi	Bob
		
Privat	Privat	Privat
+		+
Public	Public	Public
=		=
Mixed		Mixed
	Mixed	
+		+
Privat	Mixed	Privat
=		=
Common Privat	?	Common Privat

RSA

- Ron Rivest, Adi Shamir und Leonard Adleman versuchten DH zu brechen

- Verfahren zeigte keine Schwachstellen –> 1977 RSA veröffentlicht
- Basiert auf großen Primzahlen und Einwegfunktionen mit Schlüssellängen ab 512 Bit
  - Länge 2048 Bit, sogar 4096 Bit
- RSA kann für Schlüsselaustausch und digitale Signaturen verwendet werden



©Urheber

Hash-Grundlagen

Lernziele

Hashkryptographie

Hashkryptographie

- Klartext in Hash-Werte
- Umwandlung in Klartext nicht möglich
- Hash-Werte haben immer die gleiche Länge
- Unterschiedliche Klartexte müssen unterschiedliche Hash-Werte haben, sonst spricht man von Kollision oder Hash-Algorithmus geknackt
- Bei Veränderung von nur 1 Zeichen, muss direkt ein unterschiedlicher Hash-Wert erkennbar sein
- Hash dient einzig der Integrität

MD5

- Message-Digest Algorithm 5
- 1991 von Ronald L. Rivest entwickelt
- 128 Bit lang, bestehend aus 32 Hexadezimal-Zahlen
- Unsicher, auch Kollisionen sind möglich

Klartext

Hier könnte auch deine Nachricht stehen, wenn genug Informationen vorhanden und es gestattet wäre.

Hashwert

d4b41adb47ba132d2d14dc0e4da9a49b

Klartext

Hier könnte auch deine **n**achricht stehen, wenn genug Informationen vorhanden und es gestattet wäre.

Hashwert

d92a0b6331815415c645cfd2f74ce972

SHA

- Secure Hash Algorithm – SHA0, SHA1, SHA2, SHA3
- Von NIST und NSA 1993 veröffentlicht
- SHA-128 (SHA1), SHA224, SHA-256, SHA-384, SHA-512 (restliche SHA2 oder SHA3)
- Gilt als sicher und ohne Kollisionen

Klartext

Hier könnte auch deine Nachricht stehen, wenn genug Informationen vorhanden und es gestattet wäre.

Hashwert

0928ffd465082fc4c68d39ffb371e9d79056d23771204d22d47092281af07d54

Klartext

Hier könnte auch deine **n**achricht stehen, wenn genug Informationen vorhanden und es gestattet wäre.

Hashwert

b83ab8e8d23c284ce3041cc290712576e32de4d9d8be42d443699c7f2f089516

Whirlpool

- Veröffentlicht 2003
- Abgeleitet von AES
- Dateien bis 2^256 Bit Größe -> Hashwert von 512 Bit
- Bislang keine Schwachstellen entdeckt
- Geringe Anzahl von Anwendungen

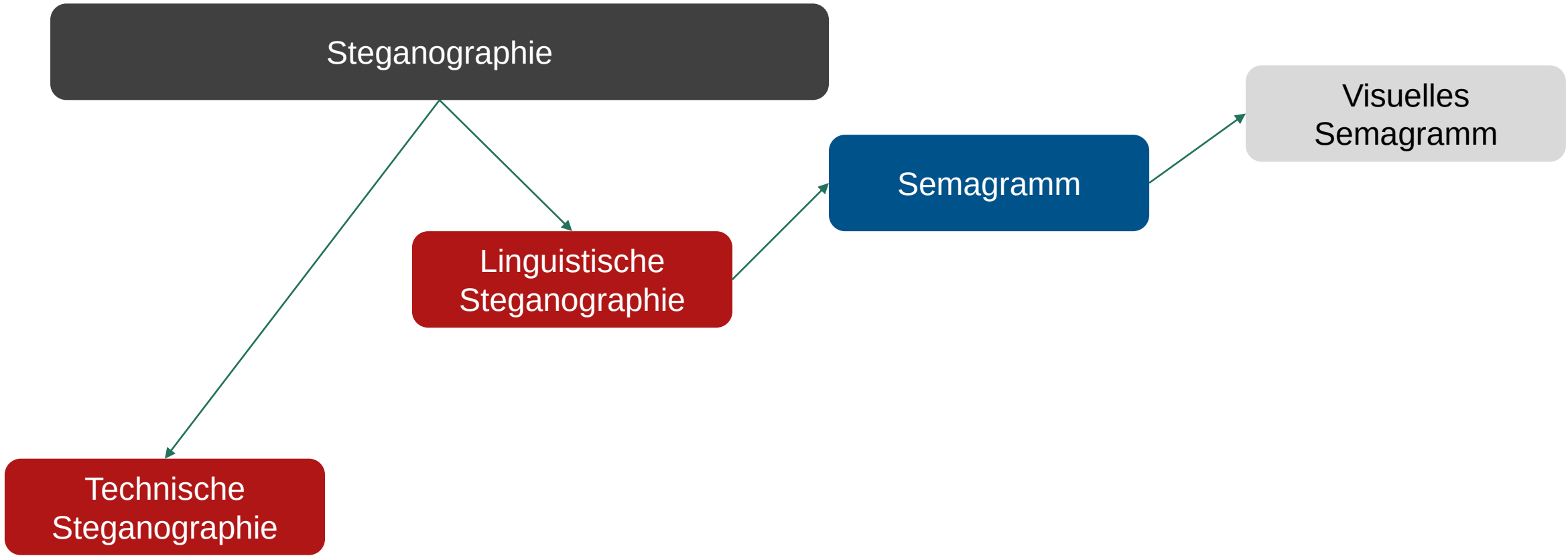
©Urheber

Steganographie

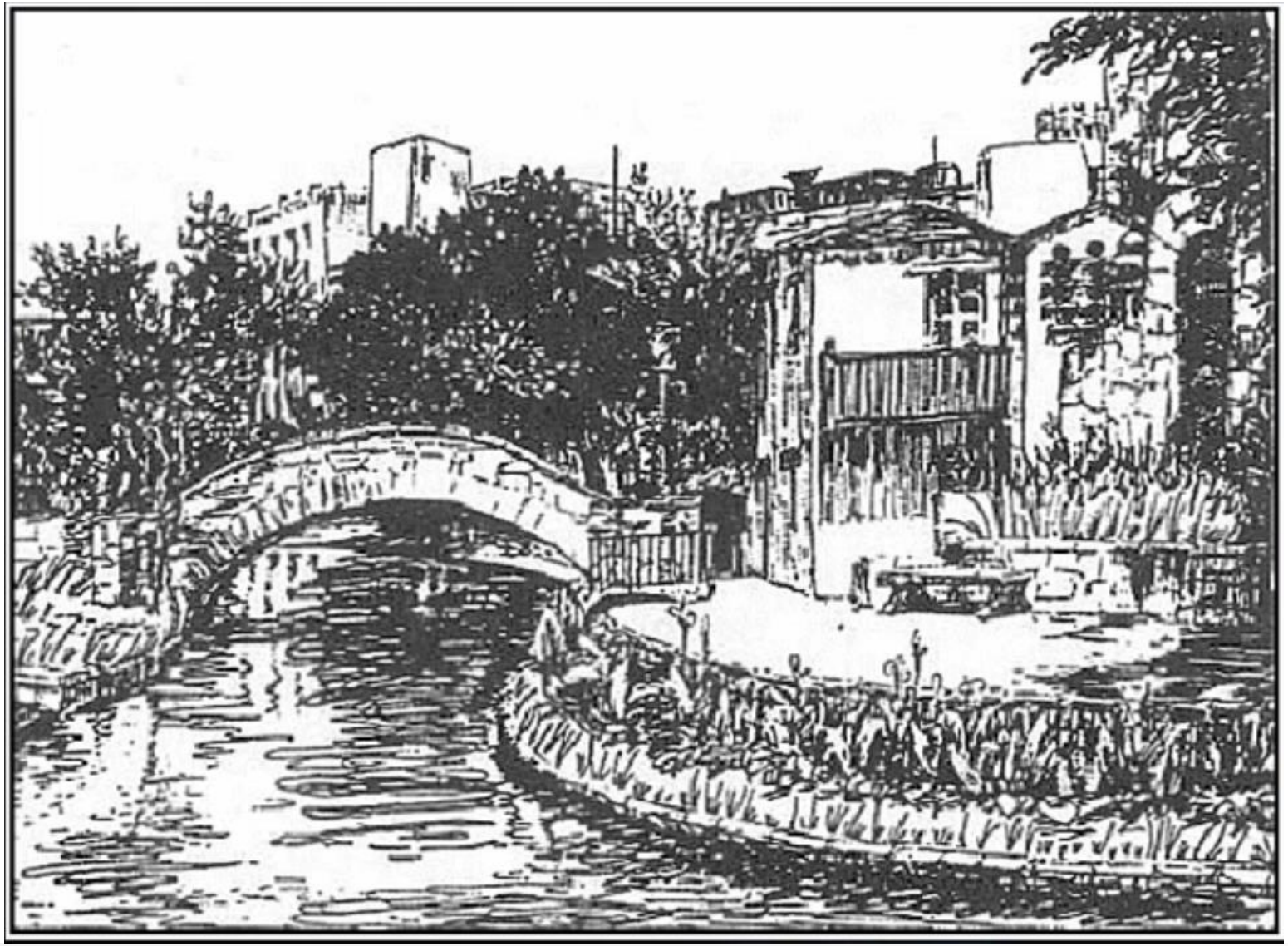
Lernziele

Grundlagen der Steganographie

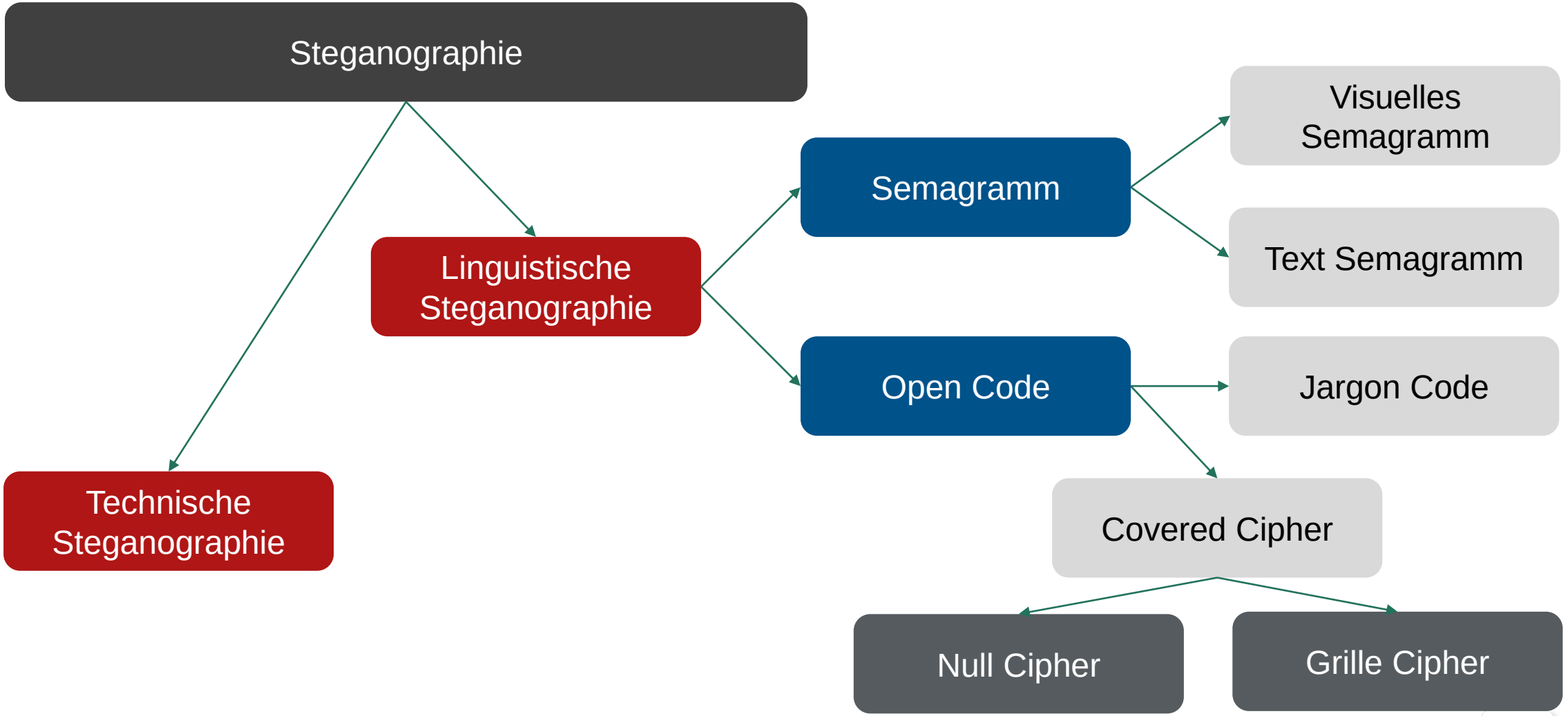
Steganographie-Typen



Visuelles Semagramm



Steganographie-Typen



Null Cipher

Nachricht:

Hallo Alice,

Hast du meine Briefe vermisst? Anders als sonst habe ich dir eine Nachricht per Mail geschickt. Check mal die Mails, ist wichtig. Können wir anschließend darüber reden? Inzwischen ist mir klar geworden, dass ich einen Fehler gemacht habe. Nicht, dass du denkst, ich wäre böse auf dich. Genaugenommen möchte ich mich bei dir entschuldigen.

Liebe Grüße,

Bob

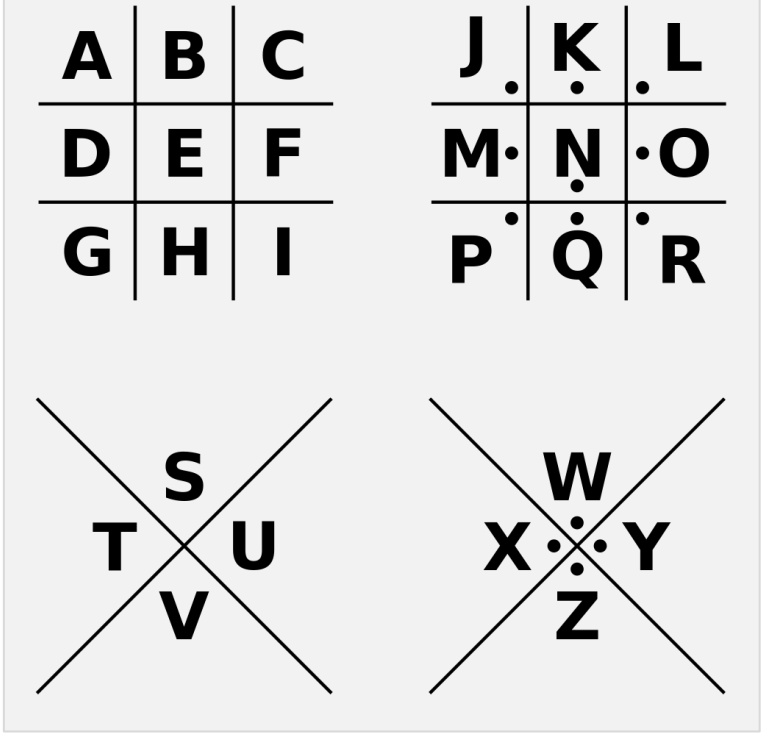
Geheime Nachricht → „hacking“

Gardan-Gitter

Zufallszeichen

Schablone

Zeichensätze



Quelle: Wikipedia – By Stephen Colbourn, CC BY-SA 2.0 <https://creativecommons.org/licenses/by-sa/2.0>, via Wikimedia Commons

Sonstige Verschlüsselung

Lernziele

Digitale Signatur

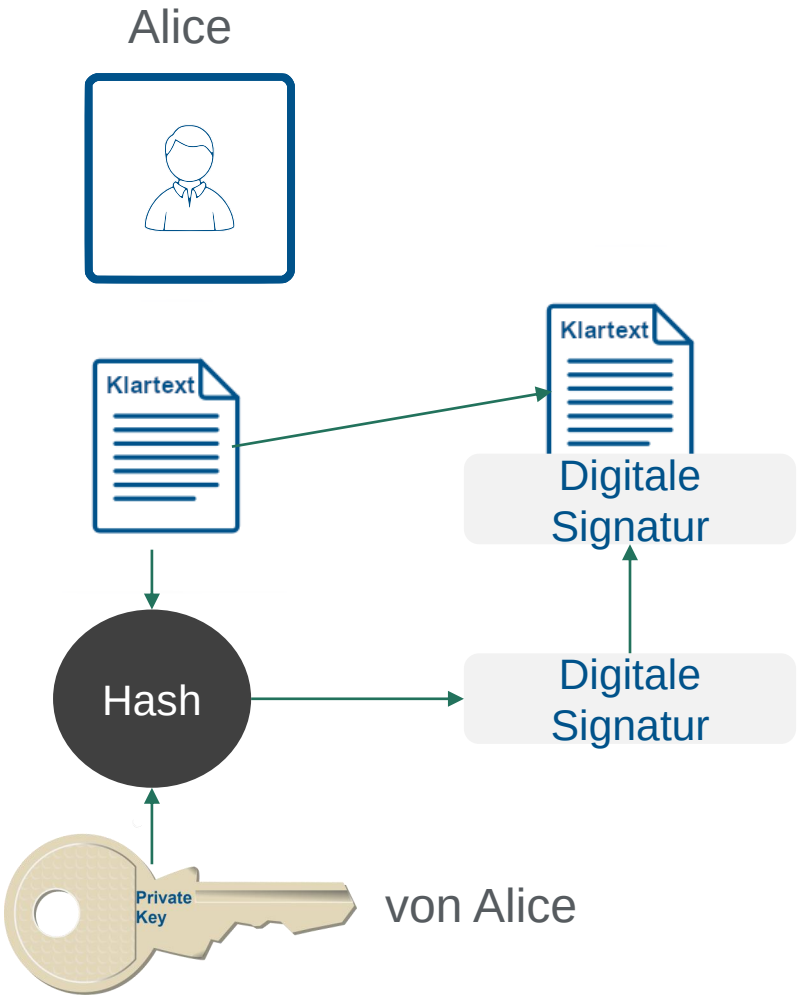
Zertifikate

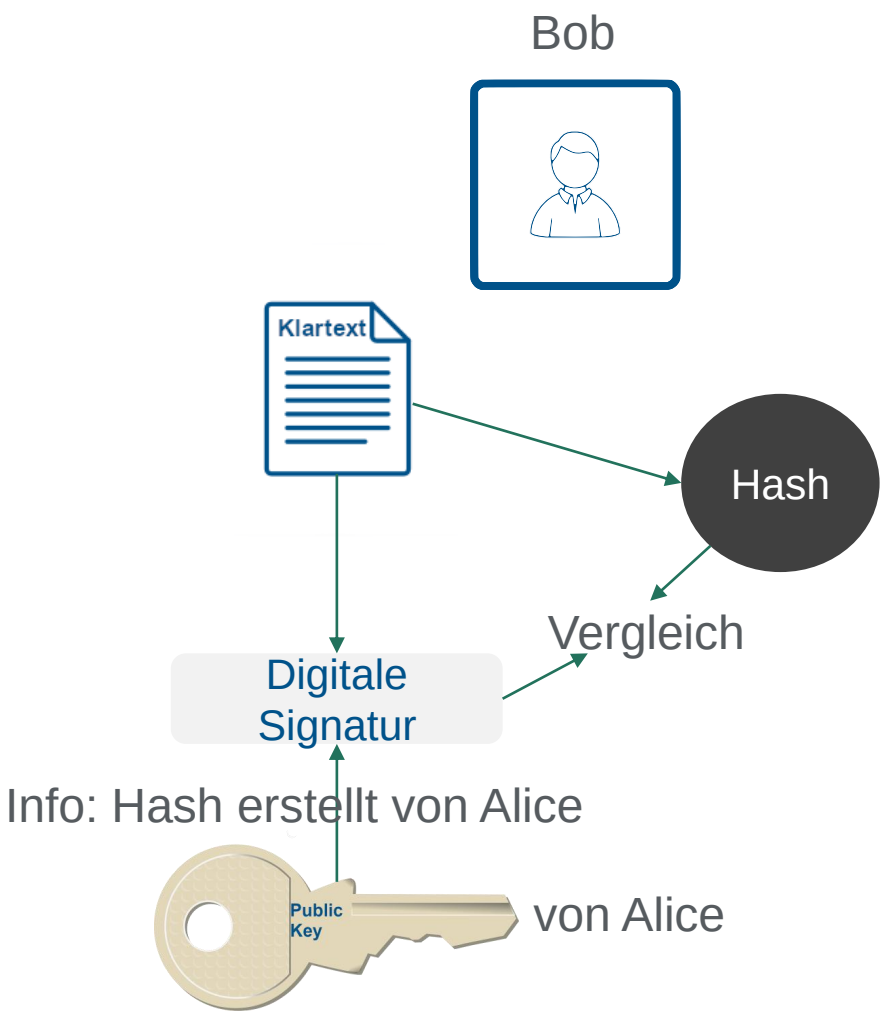
PKI und PGP

SSL und TLS

Digitale Signatur

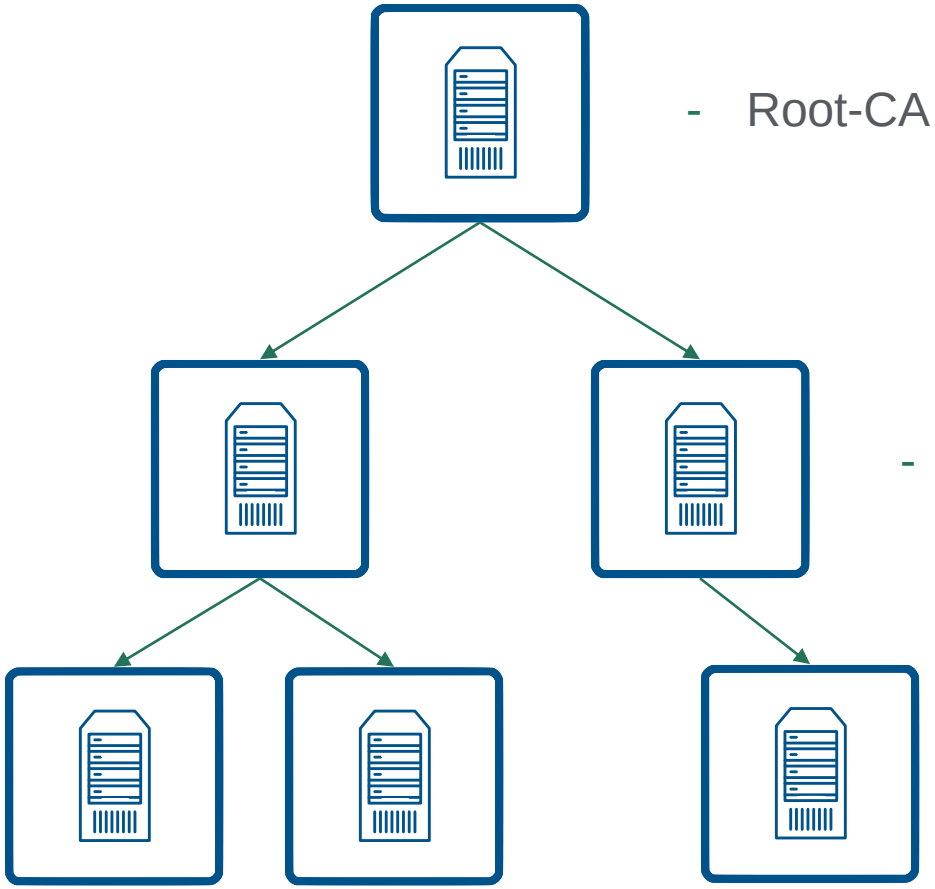
- Auf Basis von SHA





PKI

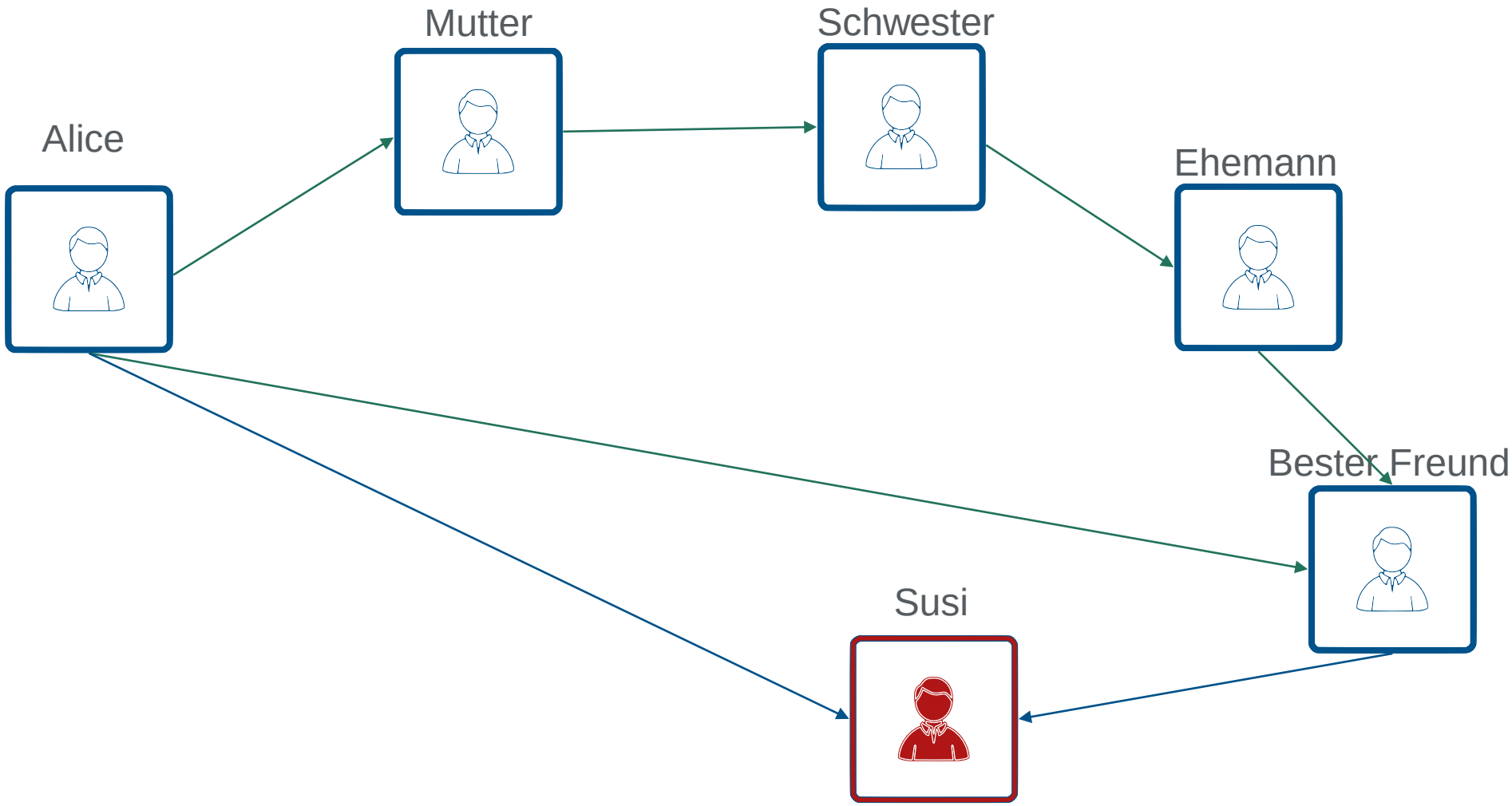
- Public Key Infrastructure



- Root-CA
- Intermediate CA
- CA (Firmeninterne-CA)

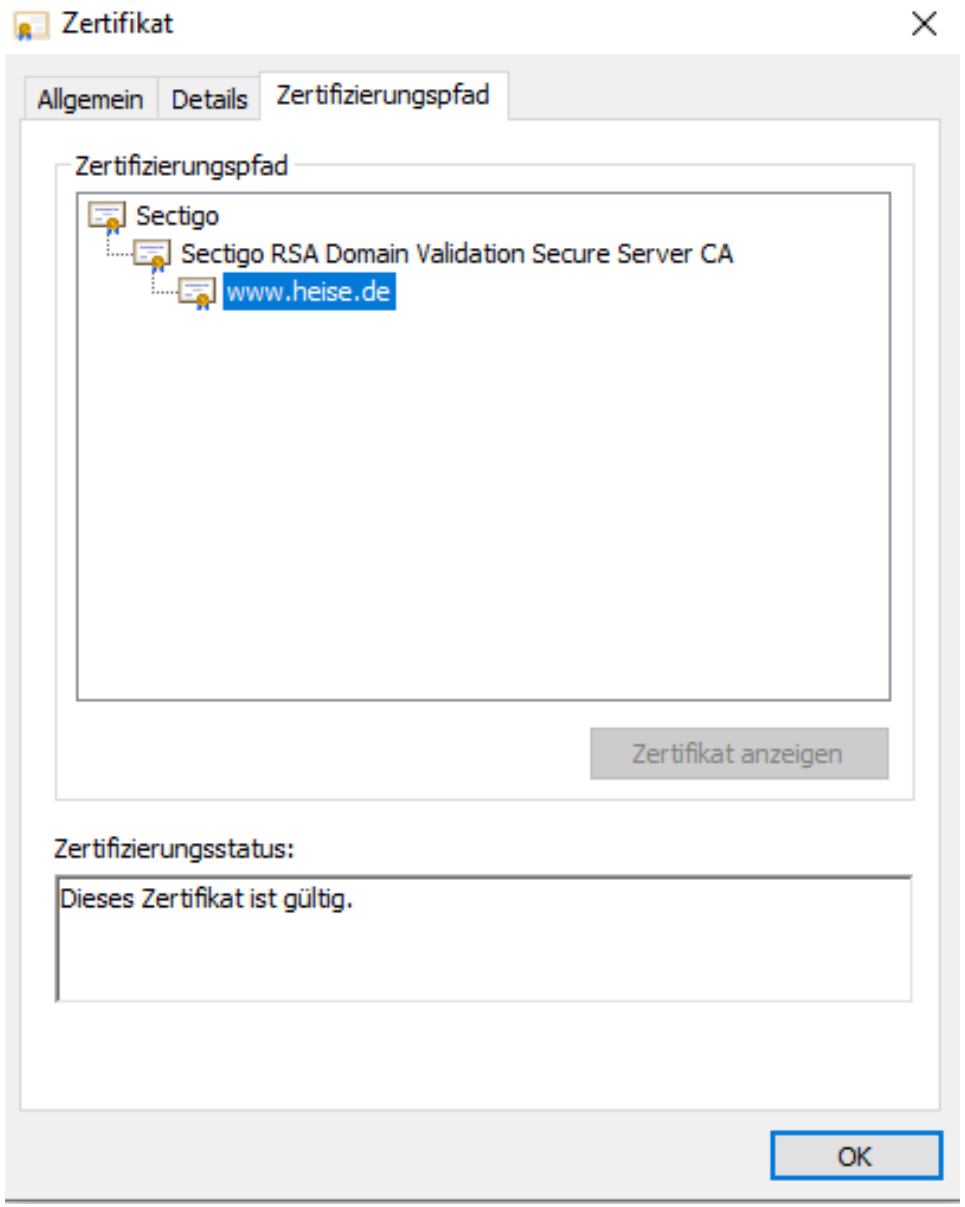
PGP – Pretty Good Privacy

- Web of Trust



Zertifikate

Zertifikate



Zertifikate

www.heise.de	Sectigo RSA Domain Validation Secure Server CA	USERTrust RSA Certification Authority

Inhabername

Allgemeiner Name www.heise.de

Ausstellername

Land GB

Bundesland/Provinz Greater Manchester

Ort Salford

Organisation Sectigo Limited

Allgemeiner Name Sectigo RSA Domain Validation Secure Server CA

Gültigkeit

Beginn 12.3.2020, 01:00:00 (Mitteleuropäische Normalzeit)

Ende 11.6.2022, 01:59:59 (Mitteleuropäische Normalzeit)

Alternative Inhaberbezeichnungen

DNS-Name www.heise.de

DNS-Name heise.de

Öffentlicher Schlüssel - Informationen

Algorithmus RSA

Schlüssellänge 2048

Exponent 65537

Modulus CE:9C:3F:4F:32:5E:01:34:B1:4E:9B:98:BD:B2:F2:4F:34:9A:53:2C:94:4D:A3:5B:30:B0:3D:32:1B:A5:16:10:E0:6F:51:6C:17:2A:8A:DB:A8:47:D6:EB:28:8A:AD:D8:43:6A:9E:F0:6E:A2:B3:63:6F:7C:F0:1F:3E:CB:CE:F9:F9:B1:CE:25:6B:64:C4:FD:3F:66:DD:FA:32:AE:17:02:D2:87:8E:24:5E:78:48:76:67:9E:AB:1F:71:C4:8D:F2:9F:EE:2C:E3:14:47:E4:B1:48:03:40:08:C4:FF:D7:0B:3B:83:AD:EF:8B:9B:2F:90:58:41:52:DD:F3:10:32:CE:1D:4D:FE:8F:EF:47:45:8B:76:05:25:1D:A4:48:D7:C5:D1:4F:39:7C:14:FB:67:35:7D:75:2D:23:CC:40:D8:B9:89:63:4B:0A:3D:5E:87:CF:B3:74:A5:6D:35:47:00:1B:AE:74:D8:DD:EF:45:28:E9:05:41:FC:A8:59:E2:35:7B:FB:B1:89:82:B2:5E:07:63:7C:11:76:4D:CE:FE:8C:16:9C:E3:B3:B9:51:E8:30:F3:62:C4:1D:56:3E:55:10:6A:63:22:C0:9B:79:5F:73:60:2C:19:20:6A:65:A2:46:66:9B:59:30:10:1A:8E:19:22:9D:79:35:51:8E:86:88:99

Verschiedenes

Seriennummer 00:A0:19:44:86:08:54:6F:F9:02:71:18:45:DB:AD:8A:BC

Signaturalgorithmus SHA-256 with RSA Encryption

Version 3

Speichern PEM (Zertifikat) PEM (Zertifikatskette)

Zertifikate

Fingerabdrücke

SHA-256 A1:A0:CE:42:B5:DA:24:E6:21:0F:B4:B2:76:14:BC:FD:A3:6E:47:56:29:6C:6A:9C:D9:31:05:F1:C7:6E:D3:60

SHA-1 17:67:3D:20:C9:2A:D9:44:6F:DB:6C:5E:ED:41:71:6A:71:A6:CF:37

Basiseinschränkungen

Zertifizierungsstelle Nein

Schlüsselverwendung

Verwendungen Digital Signature, Key Encipherment

Erweitere Schlüsselverwendung

Verwendungen Server Authentication, Client Authentication

ID für verwendeten Schlüssel des Zertifikatinhabers (Subject Key ID)

Schlüssel-ID B5:D4:C3:99:A8:9E:A7:AF:98:A6:AB:22:78:84:72:3F:7B:D5:CF:A2

ID für verwendeten Schlüssel der Zertifizierungsstelle (Authority Key ID)

Schlüssel-ID 8D:8C:5E:C4:54:AD:8A:E1:77:E9:9B:F9:9B:05:E1:B8:01:8D:61:E1

Zertifizierungsstelleninformationen - Authority Info (AIA)

Ort http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt

Methode CA Issuers

Ort http://ocsp.sectigo.com

Methode Online Certificate Status Protocol (OCSP)

Zertifikatsregeln

Regel Statement Identifier (1.3.6.1.4.1)

Wert 1.3.6.1.4.1.6449.1.2.2.7

Qualifizierer Practices Statement (1.3.6.1.5.5.7.2.1)

Wert https://sectigo.com/CPS

Regel Certificate Type (2.23.140.1.2.1)

Wert Domain Validation

SSL und TLS

No.	Time	Source	Destination	Protocol	Length	Info
169	52.357530103	2003:e9:7715:d930:2…	2a02:2e0:3fe:1001:7…	TLSv1.2	603	Client Hello
171	52.374714163	2a02:2e0:3fe:1001:7…	2003:e9:7715:d930:2…	TLSv1.2	3696	Server Hello, Certificate, Server Key Exchange, Server Hello Done
173	52.377969850	2003:e9:7715:d930:2…	2a02:2e0:3fe:1001:7…	TLSv1.2	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
175	52.394309180	2a02:2e0:3fe:1001:7…	2003:e9:7715:d930:2…	TLSv1.2	137	Change Cipher Spec, Encrypted Handshake Message

```
    Handshake Type: Client Hello (1)
    Length: 508
    Version: TLS 1.2 (0x0303)
  ▸ Random: 2a190ec63f9bfa09f83910847a55018f2286f585a945a790…
    Session ID Length: 32
    Session ID: 849dab71b04b454e467f8f138de2e372941a0f943d8229b9…
    Cipher Suites Length: 28
  ▾ Cipher Suites (14 suites)
      Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
      Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
      Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
      Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
      Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
      Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
      Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)
      Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
      Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
      Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
      Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
      Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
      Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
      Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
```

```
00b0  cc a8 c0 2c c0 30 c0 13  c0 14 00 2f 00 35 00 0a   ···,·0·· ···/·5··
00c0  01 00 01 97 00 00 00 11  00 0f 00 00 0c 77 77 77   ········ ·····www
00d0  2e 68 65 69 73 65 2e 64  65 00 17 00 00 ff 01 00   .heise.d e·······
00e0  01 00 00 0a 00 0e 00 0c  00 1d 00 17 00 18 00 19   ········ ········
```

SSL und TLS

No.	Time	Source	Destination	Protocol	Length	Info
169	52.357530103	2003:e9:7715:d930:2…	2a02:2e0:3fe:1001:7…	TLSv1.2	603	Client Hello
171	52.374714163	2a02:2e0:3fe:1001:7…	2003:e9:7715:d930:2…	TLSv1.2	3696	Server Hello, Certificate, Server Key Exchange, Server Hello Done
173	52.377969850	2003:e9:7715:d930:2…	2a02:2e0:3fe:1001:7…	TLSv1.2	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
175	52.394309180	2a02:2e0:3fe:1001:7…	2003:e9:7715:d930:2…	TLSv1.2	137	Change Cipher Spec, Encrypted Handshake Message

```
▾ Handshake Protocol: Server Hello
    Handshake Type: Server Hello (2)
    Length: 96
    Version: TLS 1.2 (0x0303)
  ▸ Random: 8801db10387f2512a9308d90c8fb661b89c18ac81d1962e2…
    Session ID Length: 32
    Session ID: d1fd2b8e94f08ea298249e0bdf98178b627f9f8e98a46de1…
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
    Compression Method: null (0)
    Extensions Length: 24
  ▸ Extension: renegotiation_info (len=1)
  ▸ Extension: application_layer_protocol_negotiation (len=5)
  ▸ Extension: ec_point_formats (len=2)
  ▸ Extension: extended_master_secret (len=0)
▾ TLSv1.2 Record Layer: Handshake Protocol: Certificate
```

SSL und TLS


TLSv1.2 Record Layer: Handshake Protocol: Certificate
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 3153
Handshake Protocol: Certificate
Handshake Type: Certificate (11)
Length: 3149
Certificates Length: 3146
Certificates (3146 bytes)
TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 333
Handshake Protocol: Server Key Exchange
Handshake Type: Server Key Exchange (12)
Length: 329
EC Diffie-Hellman Server Params
Curve Type: named_curve (0x03)
Named Curve: secp256r1 (0x0017)
Pubkey Length: 65
Pubkey: 04efe45607edcf9a17086ceb84e4c6aac41899dac6d9bd16…
Signature Algorithm: rsa_pkcs1_sha256 (0x0401)
Signature Length: 256
Signature: 482d76ceecadc606328825ab9f5d6316816c7ea9db858f4a…

SSL und TLS

No.	Time	Source	Destination	Protocol	Length	Info
169	52.357530103	2003:e9:7715:d930:2…	2a02:2e0:3fe:1001:7…	TLSv1.2	603	Client Hello
171	52.374714163	2a02:2e0:3fe:1001:7…	2003:e9:7715:d930:2…	TLSv1.2	3696	Server Hello, Certificate, Server Key Exchange, Server Hello Done
173	52.377969850	2003:e9:7715:d930:2…	2a02:2e0:3fe:1001:7…	TLSv1.2	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
175	52.394309180	2a02:2e0:3fe:1001:7…	2003:e9:7715:d930:2…	TLSv1.2	137	Change Cipher Spec, Encrypted Handshake Message

```
▸ Ethernet II, Src: PcsCompu_94:14:70 (08:00:27:94:14:70), Dst:          3d:b0:1a (  :  :  :3d:b0:1a)
▸ Internet Protocol Version 6, Src: 2003:e9:7715:d930:2   :    :    :    , Dst: 2a02:2e0:3fe:1001:7777:772e:2:85
▸ Transmission Control Protocol, Src Port: 50650, Dst Port: 443, Seq: 518, Ack: 3611, Len: 126
▾ Transport Layer Security
  ▾ TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 70
    ▾ Handshake Protocol: Client Key Exchange
        Handshake Type: Client Key Exchange (16)
        Length: 66
      ▾ EC Diffie-Hellman Client Params
          Pubkey Length: 65
          Pubkey: 0463d3324289e0d102844ee29a79be655a115ffe4fc9b1c1…
  ▾ TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
      Content Type: Change Cipher Spec (20)
      Version: TLS 1.2 (0x0303)
      Length: 1
      Change Cipher Spec Message
  ▾ TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 40
      Handshake Protocol: Encrypted Handshake Message
```

©Urheber

Kennwortsicherheit

Lernziele

Grundlagen zur Kennwortsicherheit

Triple-A

Authentification
Authentifikation

Wer bin ich und bin ich das (Name und Kennwort)

Authorisation
Autorisierung

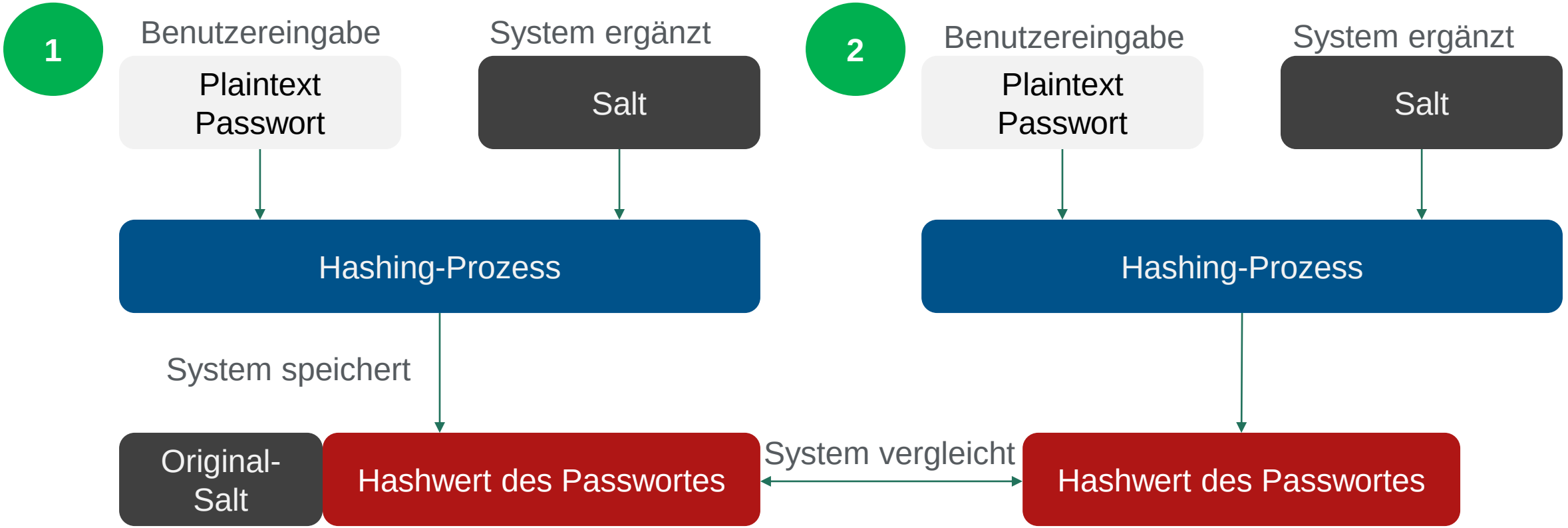
Was darf gemacht werden (Berechtigung)

Accounting
Zurechnung

Wann wurde etwas gemacht (Logs)

Kennwörter

- Speicherung niemals in Klartext



Faktoren

Was ich weiß!

Passwort, Pin, Captcha, Sicherheitsfragen

Was ich habe!

OWP (Authentifikation), Smartcard, Token

Was ich bin!

Finger-Scan, Iris-Scan, Venen-Scan

Was ich tue!

Handschrift, Unterschrift, Gangart

Kennwortrichtlinien

- Zeichenlänge
- Komplexität
- Kennwortlebensdauer
- Fehlversuche
- Sperrdauer
- Gespeicherte Kennwörter
- Multi-Faktor-Kennwörter
- SSO