Kryptographie
Ausgewählte Aspekte

Gärtringen, 9. März 2017

Dr. Manfred Gnirss
manfred.gnirss@t-online.de

Vorbemerkungen

- **Vertrauen**
  Menschen (Freunde, Partner, Feinde,...), Infrastruktur, Technik (Betriebssystem, Krpytographische Programme,...)
  - Integrität
- **Paranoia**
  Tatsächliche und vermeindliche Gefahren / Bedrohungen
- **Philosphie**
  Was ist das beste Vorgehen?
- **Erfahrungen**

Standards and Such

- NIST SP800-xx
  - set of crypto standards by (US) National Institute of Standards and Technology
  - e.g. NIST SP800-90A describes new PRNG (aka DRBG) to be used starting 2016
- PKCS
  - Public Key Cryptography Standards
  - originally hosted by RSA company (PKCS #11 now hosted by OASIS)
  - e.g. PKCS #11 defines an API to use cryptographic modules
- FIPS 140-2
  - compliance standard for cryptographic modules
  - US and Canada
  - 4 levels, SW can only be certified according to level 1
- ...

ZEIT ONLINE

Suche

Politik Gesellschaft Wirtschaft Kultur Wissen **Digital** Campus Karriere Entdecken Sport Spiele mehr ZEITmagazin

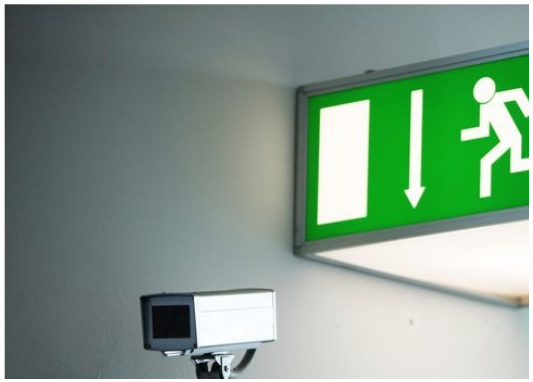
Videoüberwachung

Die NSA schaut durch die Hintertür zu

Überwachungstechnik, die auch am Frankfurter Flughafen verbaut ist, ermöglicht es der NSA, heimlich zuzusehen. D davon – und schwieg.

Von **Christian Bergmann**, **Christian Fuchs** un

27. September 2016, 15:30 Uhr / Aktualisiert am 27. Septemb



SPIEGEL ONLINE DER SPIEGEL SPIEGEL TV

Anmelden

NETZWELT

Schlagzeilen | Wetter | DAX 11.967,31 | TV-Programm | Abo

Nachrichten > Netzwelt > Netzpolitik > Überwachung > BND-Skandal: Netbotz baut offenbar Hintertüren in seine Kameras

Spionage für US-Geheimdienste

BND verschweigt offenbar Hintertür in Überwachungskameras

Der Überwachungskamerahersteller NetBotz hat einem ARD-Bericht zufolge Hintertüren in seine Geräte eingebaut. Dadurch konnten US-Geheimdienste auf die Daten zugreifen - offenbar mit Wissen des BND.

DPA

Video-Überwachungskamera

Neue Enthüllungen: ...

www.heute.de/wikileaks-enthuellungen-zu-cia-hackern-46716262.html

Suchen

IBM (2.2.0) IBM Travel Box Box privat Sales Support Inform... BluePages zATS Team

ZDF | ZDFneo | ZDFinfo | ZDFheute | ZDFsport | ZDFtivi | ZDFmediathek heute.de-Rubriken Suchbegriff

heute

08.03.2017

Alle Kurznachrichten

19:07 Anschlag in Düsseldorf geplant: Anklage gegen mutmaßliche IS-Aktivisten

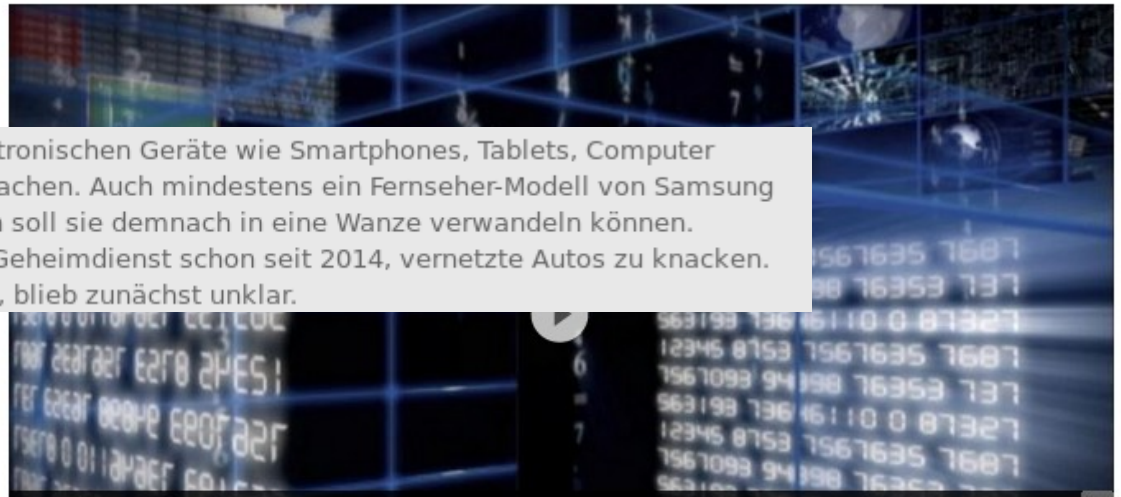
18:43 Gabriel in Polen: Warnung vor Spaltung Europas

18:08 Brand in Waisenhaus: Mindestens 15 Tote

Neue Enthüllungen

Wikileaks: Das Hacker-Arsenal der CIA

Die CIA kann sich in elektronischen Geräte wie Smartphones, Tablets, Computer hacken, um sie zu überwachen. Auch mindestens ein Fernseher-Modell von Samsung mit Kamera und Mikrofon soll sie demnach in eine Wanze verwandeln können. Außerdem versuche der Geheimdienst schon seit 2014, vernetzte Autos zu knacken. Was er dabei erreicht hat, blieb zunächst unklar.



Nach der größten Veröffentlichung von CIA-Dokumenten in der Geschichte, ist die Reichweite der Hacker-Tools sichtbar geworden: Im Grunde könnte jeder Ziel der CIA sein. Der Internet-Knotenpunkt Frankfurt spielt dabei offenbar eine zentrale Rolle. *(08.03.2017)*

Video CIA: Wikileaks-Enthüllung | Video Die Macht von Wikileaks | Doku NSA - Operation Allmacht

Dass US-Geheimdienste zu weitreichender Überwachung fähig sind, ist spätestens seit den NSA-Enthüllungen von Edward Snowden klar. Mit der jüngsten Veröffentlichung von Wikileaks weiß man nun auch mehr über die Hacker-Fähigkeiten der CIA. Ein Überblick über die wichtigsten Enthüllungen.

Weitere Themen

- Ehe für alle im Bundestag
  "Lassen Sie es uns doch einfach machen"
- U-Ausschuss zu Dieselgate
  Merkel: Erst aus Medien vom VW-Skandal erfahren
- Endlager für den Atommüll
  Suche nach dem Punkt auf der weißen Landkarte
- Neue Enthüllungen
  Wikileaks: Das Hacker-Arsenal der CIA
- Wirtschaftliche Folgen
  Brexit: London erwartet weniger Wachstum
- Frontal 21
  Willkür gegen Oppositionelle in Türkei
- Nach Außenminister-Treffen
  Cavusoglu: Freundschaft mit Deutschland gefährdet
- Afghanistan
  Angriff auf Militär-Hospital: Mindestens 30 Tote
- Chef der Polizeigewerkschaft
  Disziplinarverfahren gegen Wendt
- Vor der Parlamentswahl
  Niederlande: Wirtschaft gut, Stimmung mies
- Fischereiverbot in der Ostsee
  Eine Atempause für den Dorsch

“Enthüllungen sind schädlich für die Geheimdienste”

Wie überraschend kommt das?

So richtig überraschend ist das nicht. Schon die von Edward Snowden mitgenommenen Dokumente des Abhördienstes NSA enthüllten ein breites Überwachungssystem. Die Veröffentlichung der über 8.000 CIA-Dateien gibt aber erstmals einen Einblick in die Fähigkeiten des amerikanischen Auslandsgeheimdienstes. Ansonsten: Sicherheitslücken in Software von Smartphones und Computern werden immer wieder bekannt. Auch einige Autos mit Internet-Zugang wurden gehackt - diese Lücken wurden aber geschlossen und die Industrie hat daraus gelernt.

Ist die Verschlüsselung von WhatsApp und Co. geknackt?

Die Entwickler des Krypto-Protokolls, das dahintersteckt, bestreiten das. Vielmehr hacke die CIA die Software der Telefone selbst, um Informationen vor der Verschlüsselung oder nach der Entschlüsselung abzugreifen, betonten die Krypto-Experten von Open Whisper Systems. Sie sehen sich damit eher bestätigt: "Die allgegenwärtige Verschlüsselung treibt Geheimdienste von nicht entdeckbarer Massenüberwachung hin zu teuren, riskanten, gezielten Attacken."

Muss sich der normale User Sorgen machen?

Die Software-Schwachstellen sind wertvoll, weil meist ein hoher technischer Aufwand nötig ist, um sie zu finden und unbemerkt zu nutzen. Geheimdienste setzen sie also grundsätzlich nur gezielt und sparsam ein, weil sie mit einer Entdeckung verbrannt wären. Zugleich machen nicht geschlossene Sicherheitslücken die Geräte immer grundsätzlich gefährlich.

"Es gibt keinen Grund anzunehmen, dass diese Schwachstellen nicht auch den Chinesen oder den Russen bekannt sind", sagte Paul Rosenzweig von der IT-Sicherheitsfirma Redbranch Consulting dem Online-Dienst "CNET". Und einer breite Veröffentlichung des CIA-Codes könnte die Geräte zur Beute für Kriminelle machen, noch bevor die Lücken gestopft werden können.

Haben die Enthüllungen langfristige Folgen?

Das Verhältnis zwischen der Tech-Industrie und der US-Regierung könnte sich dadurch noch weiter verschlechtern. Schon die Snowden-Enthüllungen im Sommer 2013 hatten den Fokus auf Verschlüsselung ausgelöst und viele Unternehmen dazu getrieben, Daten in Europa statt in den USA zu speichern.

Jetzt bekommt das Silicon Valley ein besseres Bild davon, wie viele entdeckte Schwachstellen die Geheimdienste für sich behalten, statt sie den Unternehmen zu melden. Die Geheimdienst-Community wird zugleich inmitten ihrer aktuellen Auseinandersetzung mit US-Präsident Donald Trump um die vermuteten Russland-Verbindungen seiner Entourage geschwächt.

Quelle: www.heute.de

Ein paar Gefahren

- Trojaner
- Viren
- Tastaturlogger, Screen-Copies
- Pishing
- Social Engineering
- Passwörter und andere sensitive Informationen ausspionieren
  z.B. auf Festplatte, im Netzwerk, auf Bildschirm, auf Server, in der Cloud (Wolke),...

- Muss ich etwas für einen kurzen Zeitraum schützen?
  z.B. bei Kommunikation/Datenverkehr, während einer Websession, im Online-shop,...
- Oder muss ich langfristig schützen?
  z.B. Dokumente, Archiv (etwa 10 Jahre wg. Aufbewahrungsfrist)
- Problem der Schlüssel- und Passwortverwaltung
  Wiederfinden, ungültig, abgelaufen,...
- Problem der Schlüsselverteilung

Authentifizierung / Identifizierung

Drei Arten zur Prüfung der Identität eines Benutzers:

- Nachweis der Kenntnis einer Information (Wissen)
  z.B. Passwort, PIN, ...
- Verwendung eines Besitztums (Besitz)
  z.B. Schlüssel, Chipkarte, Zertifikat, USB-Stick, TAN, …
- Gegenwart des Benutzers (Biometrie)
  z.B. Fingerabdruck, Iris, Stimme,...

Übertragung der Information

- Challenge-Response-Authentifizierung
- Identifizierungsdaten nur einmal benutzten (TAN)
- Einmalpasswort-Systeme (gebunden an Zeit)

Kombination von Methoden

- 2 Faktor Authentifizierung

Sicherung durch zweiten Kanal

- z.B. mTAN (mobile TAN) per SMS, E-mail, früher Postweg
- z.B. eTAN (TAN Generator)

Danach erst Autorisierung

Informationen schützen

Zugriff beschränken
Mechanismen, die Zugriff kontrolieren (z.B. Schloß)

Verstecken
Steganographie
z.B. Film von Roman Polanski: Der Ghostwriter (geheime Botschaft in Anfangsbuchstaben einer Seite)
z.B. Verstecken in Bildern (bestimmte Pixel verändern)

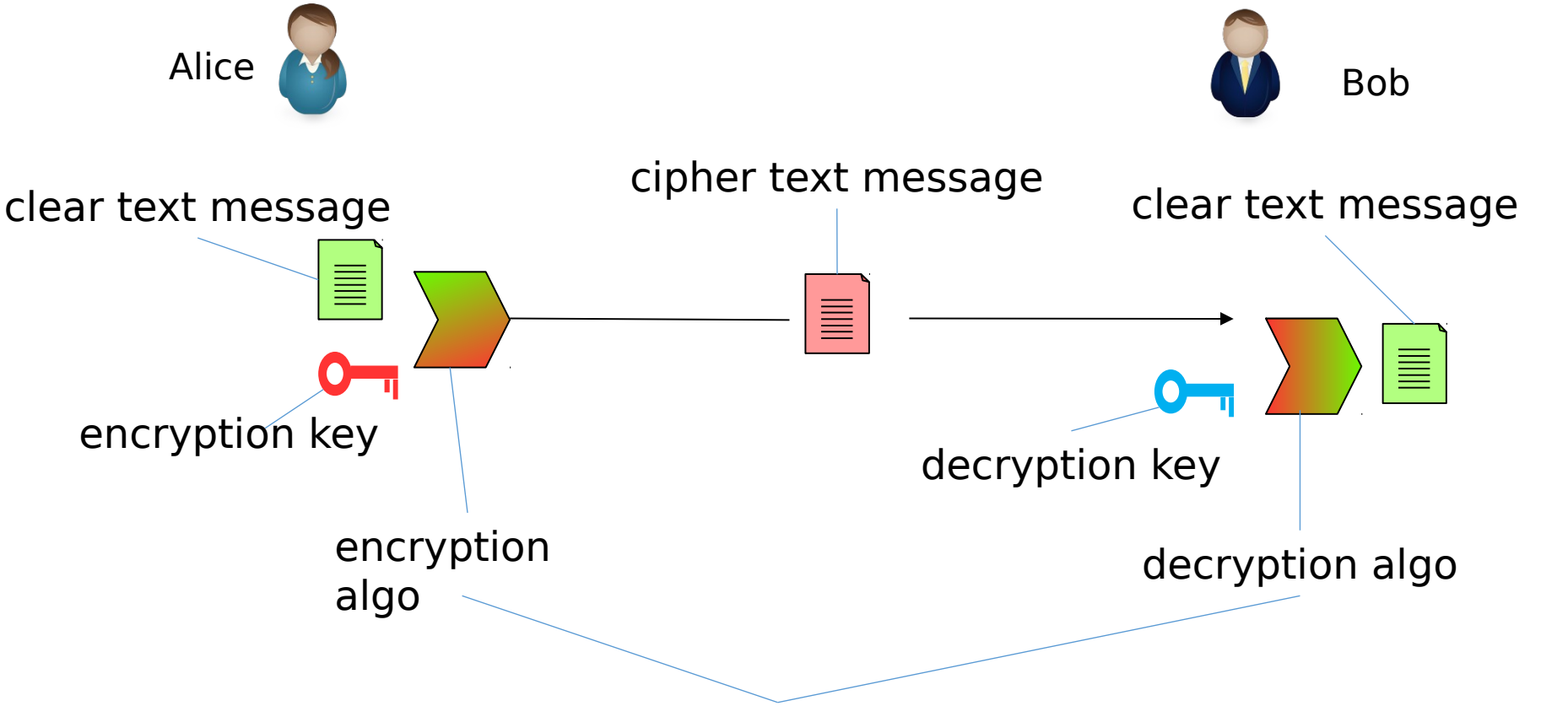
Verschlüsseln
- Trotz vorhandenem Zugriff auf verschlüsselte Information, ist diese nicht verständlich
- Es gibt Situationen, da kann Zugriff nicht verhindert werden
  z.B. bei Datenübertragung im Internet, Speichern von Dateien auf gemeinsamen Medien,...

Nebenbemerkung:
Klar: Wer Zugriff auf physische Infrastruktur (Server, PC, Platten) hat, kann (fast) alles machen. z.B.:
- Daten, Bibliotheken, Programme lesen, verändern, oder löschen,
- Funktionalität ändern,
- Konfiguration des Gerätes ändern, zusätzliches installieren,
- Firmware verändern,
- ...

Wozu Kryptographie?

- Ensure data can only be consumed by authorized users
  - encryption & decryption
- Prove integrity of data
  - hashes, digests, digital fingerprints
- Proof of data origin
  - digital signatures, authentication codes

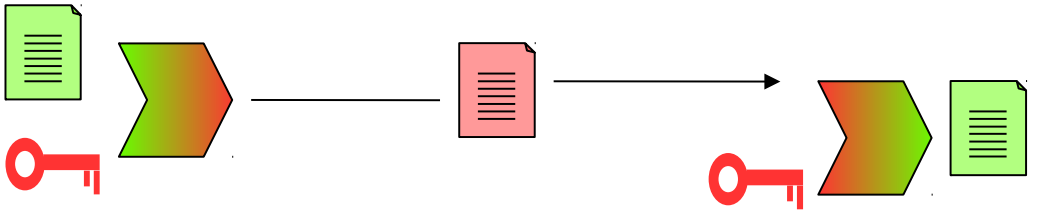
Encryption & Decryption



symmetric ciphers: encryption key == decryption key
asymmetric ciphers: encryption key =/= decryption key

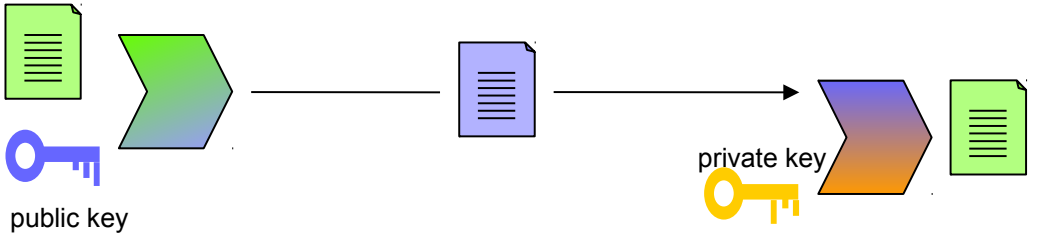
Symmetric & Asymmetric Encryption

Symmetric Encryption



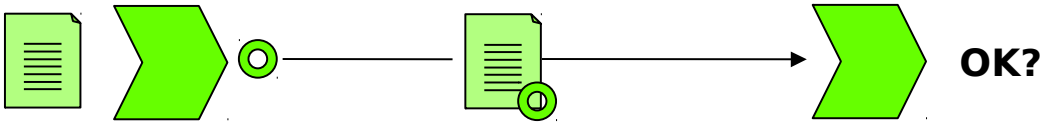
- aka secret key encryption
- fast
- used to encrypt bulk data (messages or files)
- requires secure key distribution
- block ciphers
  - e. g. DES, triple DES, (3DES, TDES, DES-ede), AES, Camelia, towfish, ...
  - parameters
    - key size (typical 56 – 256 bits) determines security (the longer the better)
    - block size = fixed number of bits that can be encrypted (typical 64 or 128 bits)

Asymmetric Encryption



- aka public key encryption
- slow
- used to encrypt keys or hashes
- public keys must be published by *trust worthy* server
- ciphers:
  - e.g. RSA, Diffie-Hellman (DH), Elliptic Curve based Diffie-Hellman (ECDH)
  - key sizes (256 for ECDH - 4096 fro RSA) not comparable to to symmetric encryption

Hashes and Signature

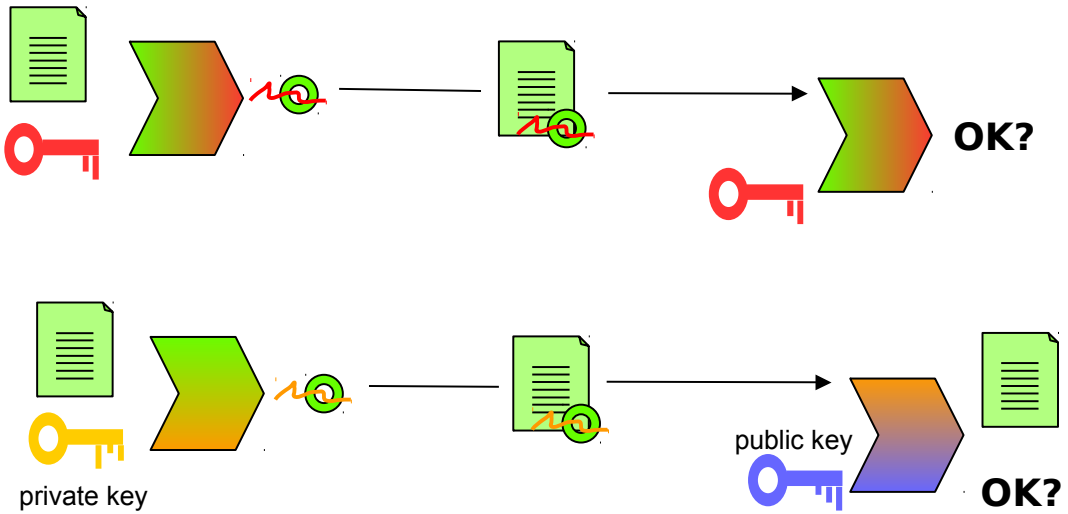


Hashes

- aka digest, digital fingerprints
- fast one-way functions
- used to check integrity of data
- hash algorithms
  - MD5, SHA-1, SHA-2 family (SHA224, SHA 256, SHA384, SHA512) , SHA-3 family
  - hash size 64 - 512

Authentication

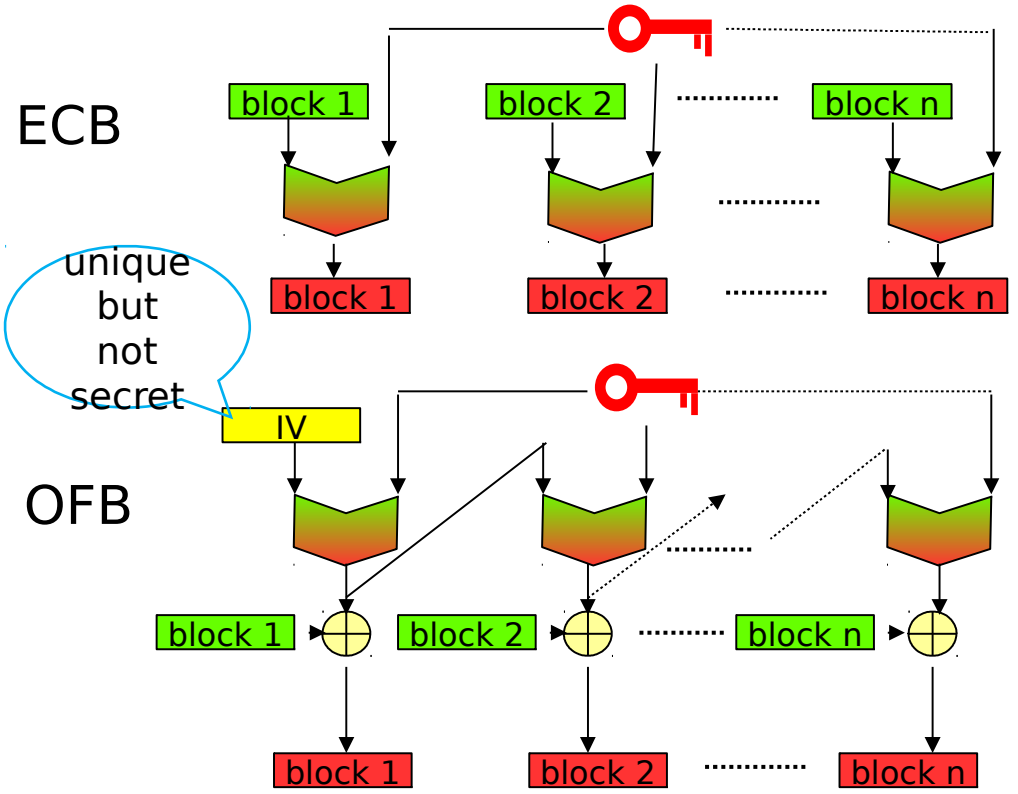
- proof integrity and origin
- symmetric variant
  - aka message authentication code (MAC)
  - e.g. HMAC, CMAC
- asymmetric variant
  - aka signature
  - e.g. RSA, DSA, ECDSA
  - used for certificates

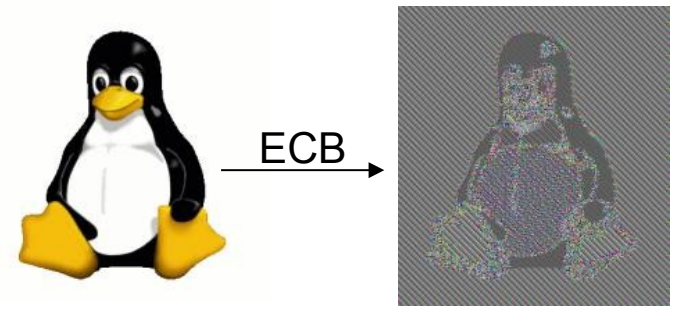


Modes of Operation

Block ciphers only encrypt small blocks of data (64 – 128 bits)

- divide large message into list of blocks
- requires messages that are multiple fo block sizes: padding
- simple block wise encryption is prone to statistical analysis
- simple padding is prone to statistical analysis





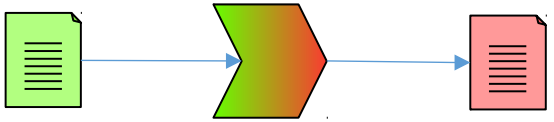
http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation

Goal:

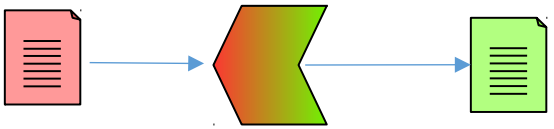
ensure that each instance of the same plain text in enciphered differently

Asymmetric Crypto – Basic Idea

- uses a one way function (with trap door)
- based on mathematics and computational complexity



easy, fast to compute



difficult, computationally infeasible

- examples of one way functions:
  - multiplication $a \cdot b = ?$ is easy, but factorization $n = ? \cdot ??$ is hard
  - exponentiation $a^b = ?$ is easy, but computation of logarithms $\log_a b = ?$ is hard
  - each of the hard problems gets even harder in modular arithmetic (mod n)

- the trap door is additional information that makes solving the hard problems easy (or at least feasible): the private key

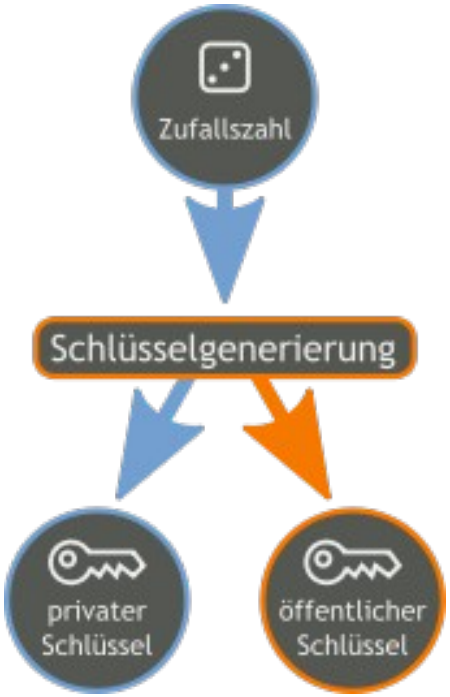
- in some cases modular arithmetic can be accelerated using a method known to Chinese mathematicians since the 3rd century
  - the result is now called Chinese Remainder Theorem (CRT)
  - RSA decryption can be accelerated using CRT methods (and often is)

Asymmetrisches Kryptosystem

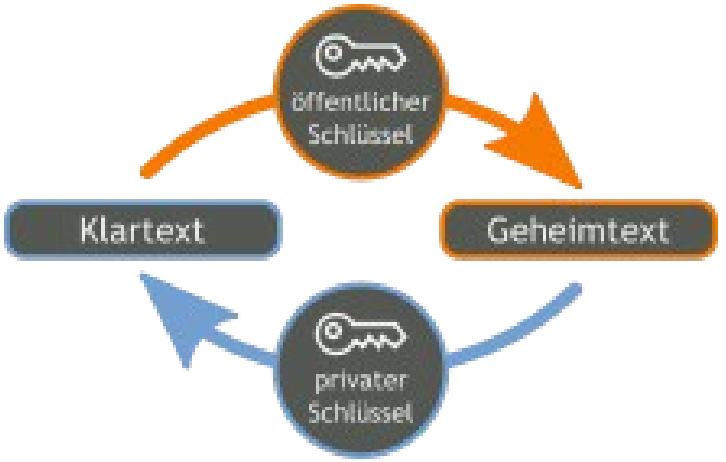
Die theoretische Grundlage für asymmetrische Kryptosysteme sind **Falltürfunktionen**, also Funktionen, die leicht zu berechnen, aber ohne ein Geheimnis (die „Falltür“) **praktisch unmöglich zu invertieren** sind. Der öffentliche Schlüssel ist dann eine Beschreibung der Funktion, der **private Schlüssel** ist die Falltür. **Eine Voraussetzung ist natürlich, dass der private Schlüssel aus dem öffentlichen nicht berechnet werden kann**. Damit das Kryptosystem verwendet werden kann, muss der **öffentliche Schlüssel** dem Kommunikationspartner bekannt sein.

Der entscheidende Vorteil von asymmetrischen Verfahren ist, dass sie das **Schlüsselverteilungsproblem vermindern**. Bei symmetrischen Verfahren muss vor der Verwendung ein Schlüssel über einen sicheren, d. h. abhörsicheren und manipulationsgeschützten Kanal ausgetauscht werden. Da der öffentliche Schlüssel nicht geheim ist, braucht bei asymmetrischen Verfahren der Kanal nicht abhörsicher zu sein; **wichtig ist nur, dass der öffentliche Schlüssel dem Inhaber des dazugehörigen geheimen Schlüssels zweifelsfrei zugeordnet werden kann**. Dazu kann beispielsweise eine vertrauenswürdige Zertifizierungsstelle ein digitales **Zertifikat** ausstellen, welches den öffentlichen Schlüssel dem privaten Schlüssel(inhaber) zuordnet. Als Alternative dazu kann auch ohne zentrale Stelle durch gegenseitiges Zertifizieren von Schlüsseln ein **Vertrauensnetz** (Web of Trust) aufgebaut werden.

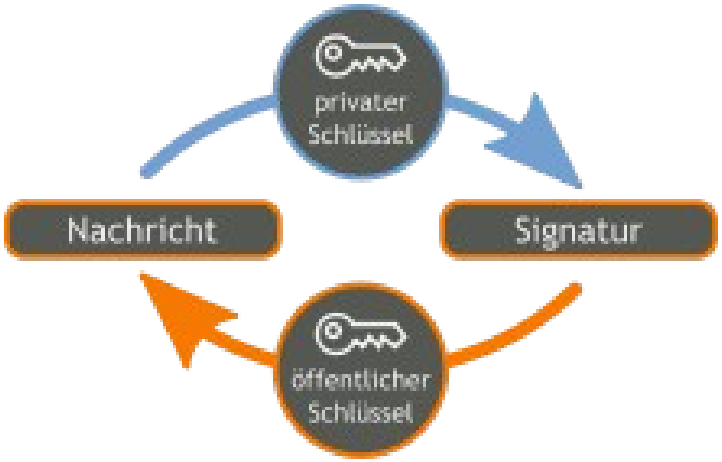
Asymmetrisches Kryptosystem



Erzeugung eines Schlüsselpaars: Blaue Bildelemente sind geheim, orange sind öffentlich.



Verschlüsselung mit öffentlichem Schlüssel und Entschlüsselung mit privatem Schlüssel

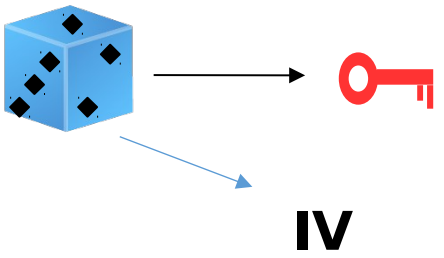


Signieren mit privatem Schlüssel und Verifikation mit öffentlichem Schlüssel

Quelle:
Von Bananenfalter - Eigenes Werk, CC0, https://commons.wikimedia.org/w/index.php?curid=17500027
Von Bananenfalter - Eigenes Werk, CC0, https://commons.wikimedia.org/w/index.php?curid=14688641
Von Bananenfalter - Eigenes Werk, CC0, https://commons.wikimedia.org/w/index.php?curid=17500025

Random Numbers

- Where needed
  - in cryptography: session keys, IVs, nonces, salts
  - in kernel: e.g.: address space randomization
  - simulation & modelling
  - random sampling
  - ...
- Types of random numbers
  - pseudo random numbers (seed + mathematical function)
  - cryptographically secure pseudo random numbers
  - true random numbers



- Cryptographically Secure Pseudo (or Deterministic) Random Number Generator (PRNG, DRNG, DRBG with B=bit)
  - has a secret internal state
  - initially set to „seed“ (from a good secret random source)
  - in each step computes random bits or number while secretly changing its internal state
  - there must be no way to predict the next pseudo random bit given all pseudo random bits output so far
  - must be reseed periodically to maintain „strength“ of pseudo random numbers

Recommended Key and Hash Length

Recommending Org	Criteria	Hash size	symmetric key length	modulus for RSA/DSA/DH	modulus for ECC
ECRYPT II	Level 4 - 2015	160	80	1248	160
2012	Level 5 - 2020	192	96	1776	192
	Level 6 - 2030	224	112	2432	224
	Level 7 - 2040	256	128	3248	256
	Level 8 >2040	512	256	15424	512
NIST	<=2030	224/160*	112	2048	224
2012	>2030	256/160*	128	3072	256
	>>2030	384/224*	192	7680	384
	>>>2030	512/256*	256	15360	512
ANSSI	<=2020	200	100	2048	200
2014	<=2030	256	128	2048	256
	>2030	256	128	3072	256
NSA Suite B	secret	256	128		256
2014	top secret	284	256		384
BSI (for signatures)	2014 - 2015	224/160***		1976/2048**	224
2015	2016 - 2021	256		1976/2048**	250
	>2021	256		1976/2048**	256

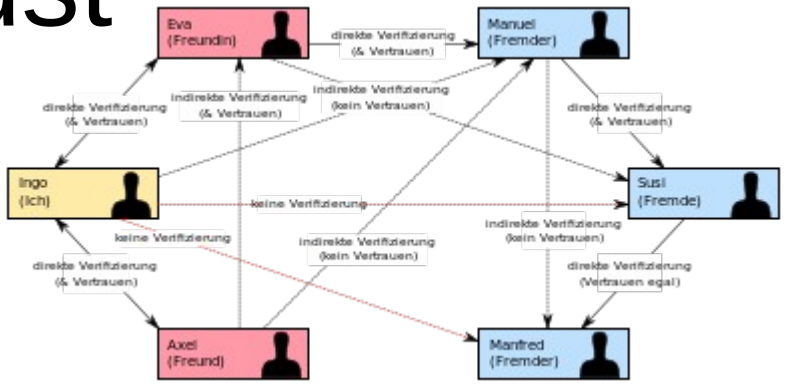
* digital signatures & pure hashes / HMAC, key derivation and PRNG

** factorization based / log based *** non certificates / certificates

source http://www.keylength.com

Web of Trust

Netz des Vertrauens bzw. Web of Trust (WOT) ist in der Kryptologie die Idee, die Echtheit von digitalen Schlüsseln durch ein Netz von gegenseitigen Bestätigungen (Signaturen), kombiniert mit dem individuell zugewiesenen Vertrauen in die Bestätigungen der anderen („Owner Trust“), zu sichern. Es stellt eine **dezentrale Alternative zum hierarchischen PKI-System dar.**



Quelle:
Von https://commons.wikimedia.org/wiki/User:Ogmios - https://upload.wikimedia.org/wikipedia/commons/4/4e/Web_of_Trust.svg, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=30127548

Die Verschlüsselung mit öffentlichen Schlüsseln bietet (gegenüber der symmetrischen Verschlüsselung) den Vorteil, dass der auszutauschende Schlüssel nicht über einen sicheren Kanal übertragen werden muss, sondern öffentlich ist. **Zur Übertragung des Schlüssels kann man sich daher eines Verbunds von Schlüsselservern bedienen, auf die jeder seine öffentlichen Schlüssel hochladen kann und von denen jeder den Schlüssel der Person abrufen kann, mit der er kommunizieren möchte.** Dadurch ergibt sich aber ein anderes Problem: Eine Person könnte einen Schlüssel veröffentlichen, mit welchem sie sich als jemand anderes ausgibt. Es muss also eine Möglichkeit zur Verfügung stehen, **die Authentizität eines Schlüssels zu prüfen.**

Die Lösung für dieses Problem besteht darin, die Echtheit eines öffentlichen Schlüssels von einer **vertrauenswürdigen Instanz** durch ein digitales Zertifikat bestätigen zu lassen. **Bei Public-Key-Infrastrukturen ist dies eine Zertifizierungsstelle; im Web of Trust hingegen übernehmen alle Teilnehmer diese Funktion.**

Zertifikate

X.509 ist ein ITU-T-**Standard für eine Public-Key-Infrastruktur** zum Erstellen digitaler Zertifikate. Der Standard ist auch als ISO/IEC 9594-8 zuletzt im Oktober 2016 aktualisiert worden. Der Standard spezifiziert die folgenden Datentypen: Public-Key-Zertifikat, Attributzertifikat, Certificate Revocation List (CRL) und Attribute Certificate Revocation List (ACRL). In der elektronischen Kommunikation finden X.509-Zertifikate Anwendung bei den TLS-Versionen diverser Übertragungsprotokolle, wie z. B. beim **Abruf von Web-Seiten mit dem HTTPS-Protokoll**, oder zum Unterschreiben und **Verschlüsseln von E-Mails nach dem S/MIME-Standard**.

X.509 setzt ein strikt hierarchisches System von vertrauenswürdigen **Zertifizierungsstellen** (englisch **certificate authority, CA**) voraus, die Zertifikate erteilen können. Dieses Prinzip steht im Gegensatz zum Web-of-Trust-Modell, welches einen Graphen und nicht nur einen Baum darstellt und bei dem jeder ein Zertifikat „unterschreiben“ und damit seine Echtheit beglaubigen kann (siehe z. B. OpenPGP).

Zertifikate . . .

Ein von einer Zertifizierungsstelle ausgestelltes digitales Zertifikat wird im X.509-System immer an einen „Distinguished Name“ oder einen „Alternative Name“ wie eine E-Mail-Adresse oder einen DNS-Eintrag gebunden.

Nahezu alle Webbrowser enthalten eine vorkonfigurierte Liste vertrauenswürdiger Zertifizierungsstellen, deren X.509-Zertifikaten der Browser vertraut. Umgangssprachlich wird häufig von SSL-Zertifikaten gesprochen.

X.509 beinhaltet außerdem einen Standard, mittels dessen Zertifikate seitens der Zertifizierungsstelle wieder ungültig gemacht werden können, wenn deren Sicherheit nicht mehr gegeben ist (z. B. nach dem öffentlichen Bekanntwerden des privaten Schlüssels für das Signieren von E-Mails). Die Zertifizierungsstelle kann hierfür ungültige Zertifikate in Zertifikatsperrlisten (certificate revocation list, kurz CRL) führen. Die automatische Überprüfung, ob ein Zertifikat inzwischen Teil einer Sperrliste ist, ist allerdings nicht in allen Programmen, die X.509-Zertifikate akzeptieren, standardmäßig aktiviert.

Struktur eines X.509-v3-Zertifikats

- Zertifikat
  - Version
  - Seriennummer
  - Algorithmen-ID
  - Aussteller
  - Gültigkeit
    - von
    - bis
  - Zertifikatinhaber
  - Zertifikatinhaber-Schlüsselinformationen
    - Public-Key-Algorithmus
    - Public Key des Zertifikatinhabers
  - Eindeutige ID des Ausstellers (optional)
  - Eindeutige ID des Inhabers (optional)
  - Erweiterungen
    - …
- Zertifikat-Signaturalgorithmus
- Zertifikat-Signatur

Aussteller und Zertifikatinhaber werden jeweils durch eine Reihe von Attributen charakterisiert:

- Gebräuchlicher Name (CN)
- Organisation (O)
- Organisationseinheit (OU)
- Land/Region (C)
- Bundesland/Kanton (ST)
- Ort (L)

Beispiel eines Zertifikates

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=AT, ST=Steiermark, L=Graz, O=TrustMe Ltd, OU=Certificate Authority, CN=CA/Email=ca@trustme.dom
        Validity
            Not Before: Oct 29 17:39:10 2000 GMT
            Not After : Oct 29 17:39:10 2001 GMT
        Subject: C=AT, ST=Vienna, L=Vienna, O=Home, OU=Web Lab, CN=anywhere.com/Email=xyz@anywhere.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:c4:40:4c:6e:14:1b:61:36:84:24:b2:61:c0:b5:
                    d7:e4:7a:a5:4b:94:ef:d9:5e:43:7f:c1:64:80:fd:
                    9f:50:41:6b:70:73:80:48:90:f3:58:bf:f0:4c:b9:
                    90:32:81:59:18:16:3f:19:f4:5f:11:68:36:85:f6:
                    1c:a9:af:fa:a9:a8:7b:44:85:79:b5:f1:20:d3:25:
                    7d:1c:de:68:15:0c:b6:bc:59:46:0a:d8:99:4e:07:
                    50:0a:5d:83:61:d4:db:c9:7d:c3:2e:eb:0a:8f:62:
                    8f:7e:00:e1:37:67:3f:36:d5:04:38:44:44:77:e9:
                    f0:b4:95:f5:f9:34:9f:f8:43
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Alternative Name:
                email:xyz@anywhere.com
            Netscape Comment:
                mod_ssl generated test server certificate
            Netscape Cert Type:
                SSL Server
    Signature Algorithm: md5WithRSAEncryption
        12:ed:f7:b3:5e:a0:93:3f:a0:1d:60:cb:47:19:7d:15:59:9b:
        3b:2c:a8:a3:6a:03:43:d0:85:d3:86:86:2f:e3:aa:79:39:e7:
        82:20:ed:f4:11:85:a3:41:5e:5c:8d:36:a2:71:b6:6a:08:f9:
        cc:1e:da:c4:78:05:75:8f:9b:10:f0:15:f0:9e:67:a0:4e:a1:
        4d:3f:16:4c:9b:19:56:6a:f2:af:89:54:52:4a:06:34:42:0d:
        d5:40:25:6b:b0:c0:a2:03:18:cd:d1:07:20:b6:e5:c5:1e:21:
        44:e7:c5:09:d2:d5:94:9d:6c:13:07:2f:3b:7c:4c:64:90:bf:
        ff:8e
```

Kerckhoffs' Prinzip oder Kerckhoffs' Maxime

1883 formulierte Auguste Kerckhoffs den Grundsatz der modernen Kryptographie:
Die Sicherheit eines Verschlüsselungsverfahrens beruht auf der Geheimhaltung des Schlüssels, anstatt auf der Geheimhaltung des Verschlüsselungsalgorithmus.

Dem Kerckhoffs'schen Prinzip wird oft die sogenannte Security through obscurity gegenübergestellt: Sicherheit durch Geheimhaltung des Verschlüsselungsalgorithmus selbst, möglicherweise zusätzlich zur Geheimhaltung des bzw. der verwendeten Schlüssel.

Das Kerckhoffs'sche Prinzip ist der zweite der sechs Grundsätze zur Konstruktion eines sicheren Verschlüsselungsverfahrens, die Kerckhoffs 1883 in La cryptographie militaire einführt.

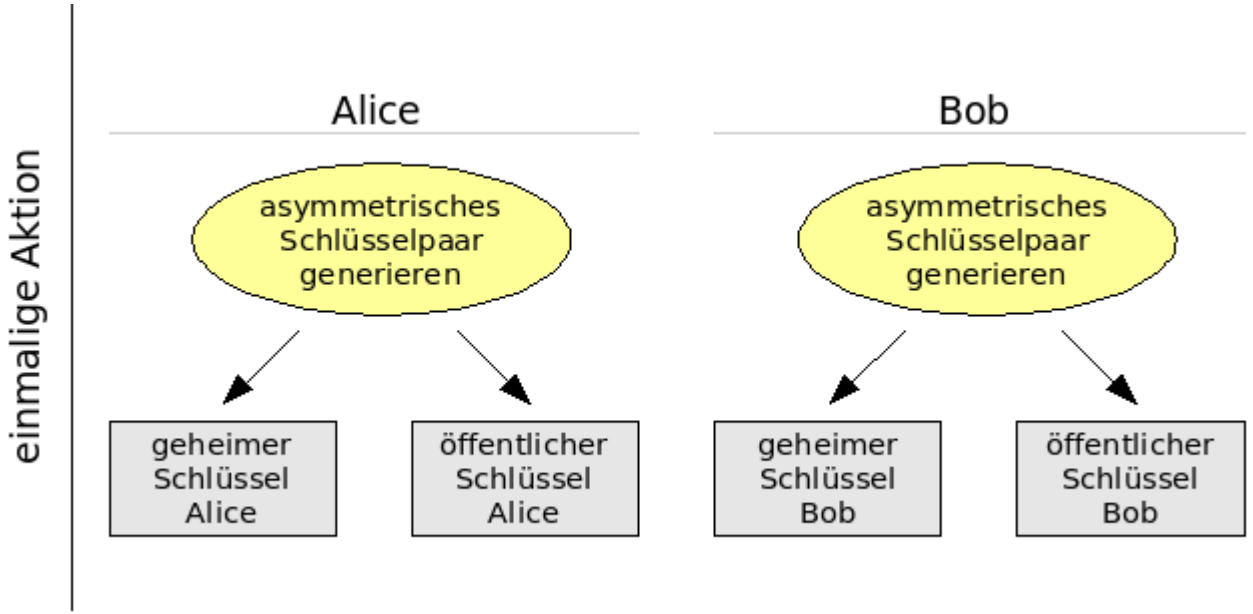
1. Das System muss im Wesentlichen (…) unentzifferbar sein.
2. Das System darf keine Geheimhaltung erfordern (…).
3. Es muss leicht übermittelbar sein und man muss sich die Schlüssel ohne schriftliche Aufzeichnung merken können (…).
4. Das System sollte mit telegraphischer Kommunikation kompatibel sein.
5. Das System muss transportabel sein und die Bedienung darf nicht mehr als eine Person erfordern.
- Das System muss einfach anwendbar sein (…).

Und nun?

Wir kombinieren und setzen alles zusammen . . .

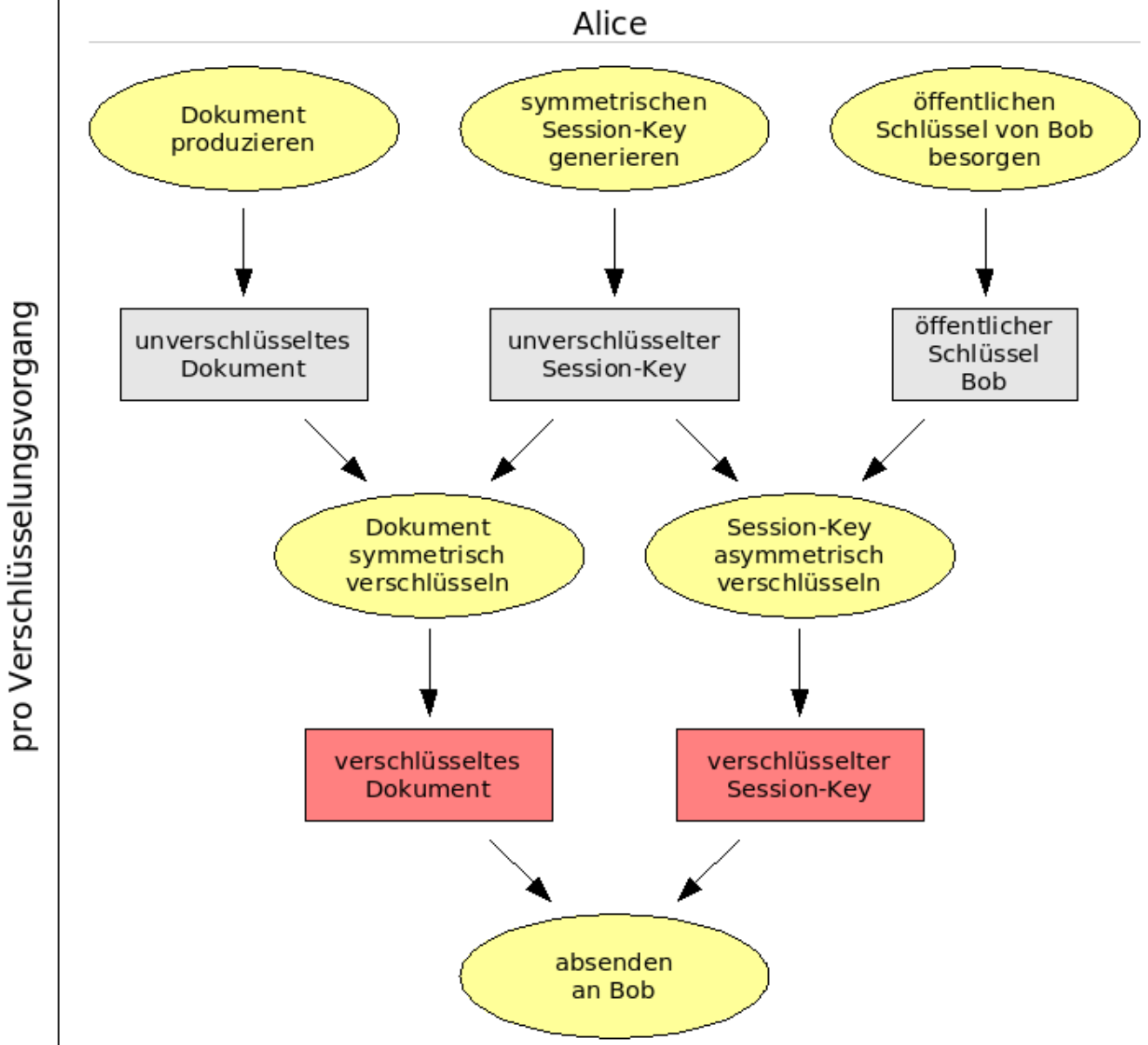
Hybrides Verschlüsselungsverfahren
SSL / TLS

Hybride Verschlüsselung



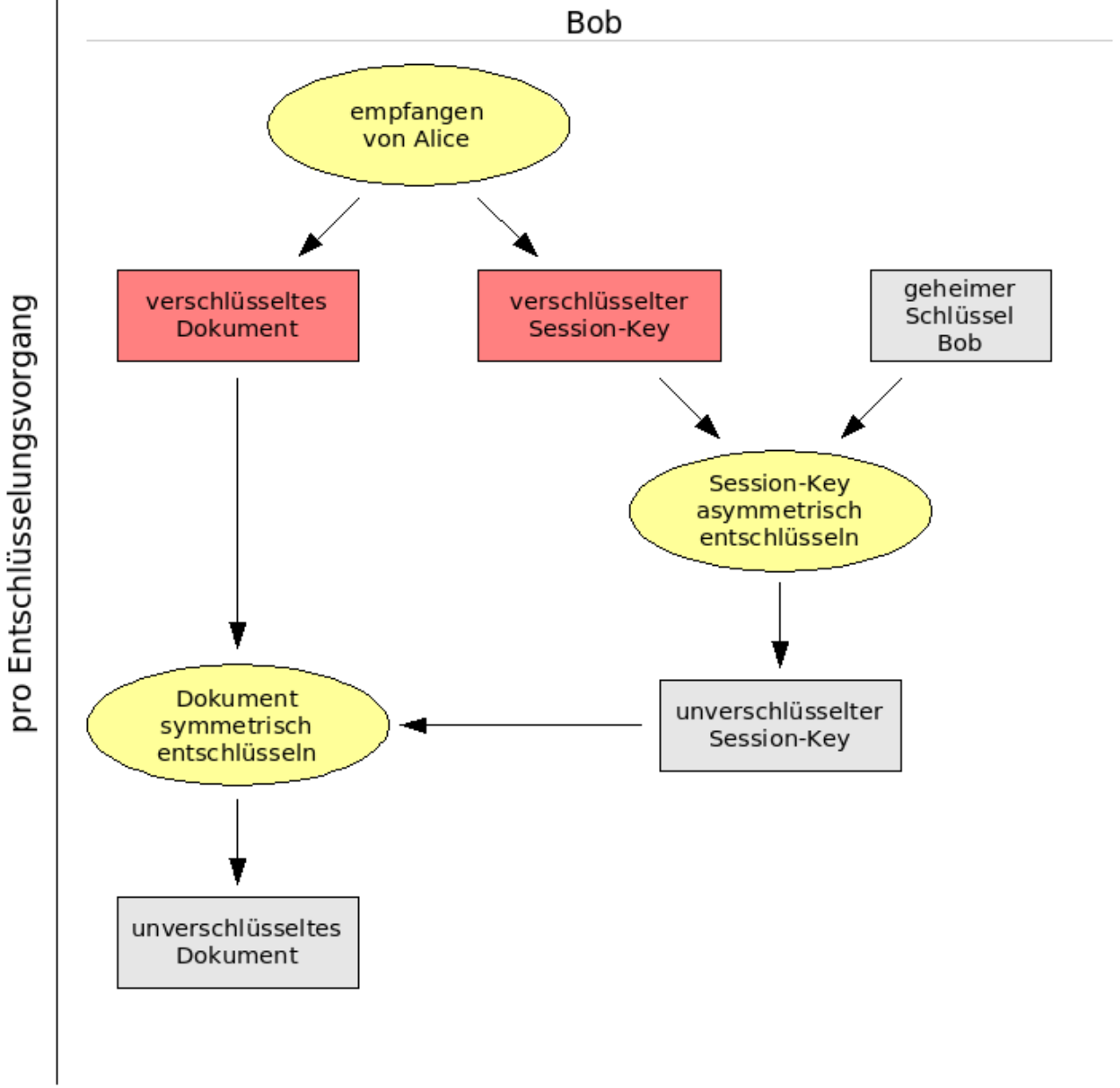
Quelle:
Von Crypto-man - selbst in OpenOffice 2.0.4 erstellt, extra für die Wikipedia, Gemeinfrei, https://commons.wikimedia.org/w/index.php?curid=20556007

Hybride Verschlüsselung



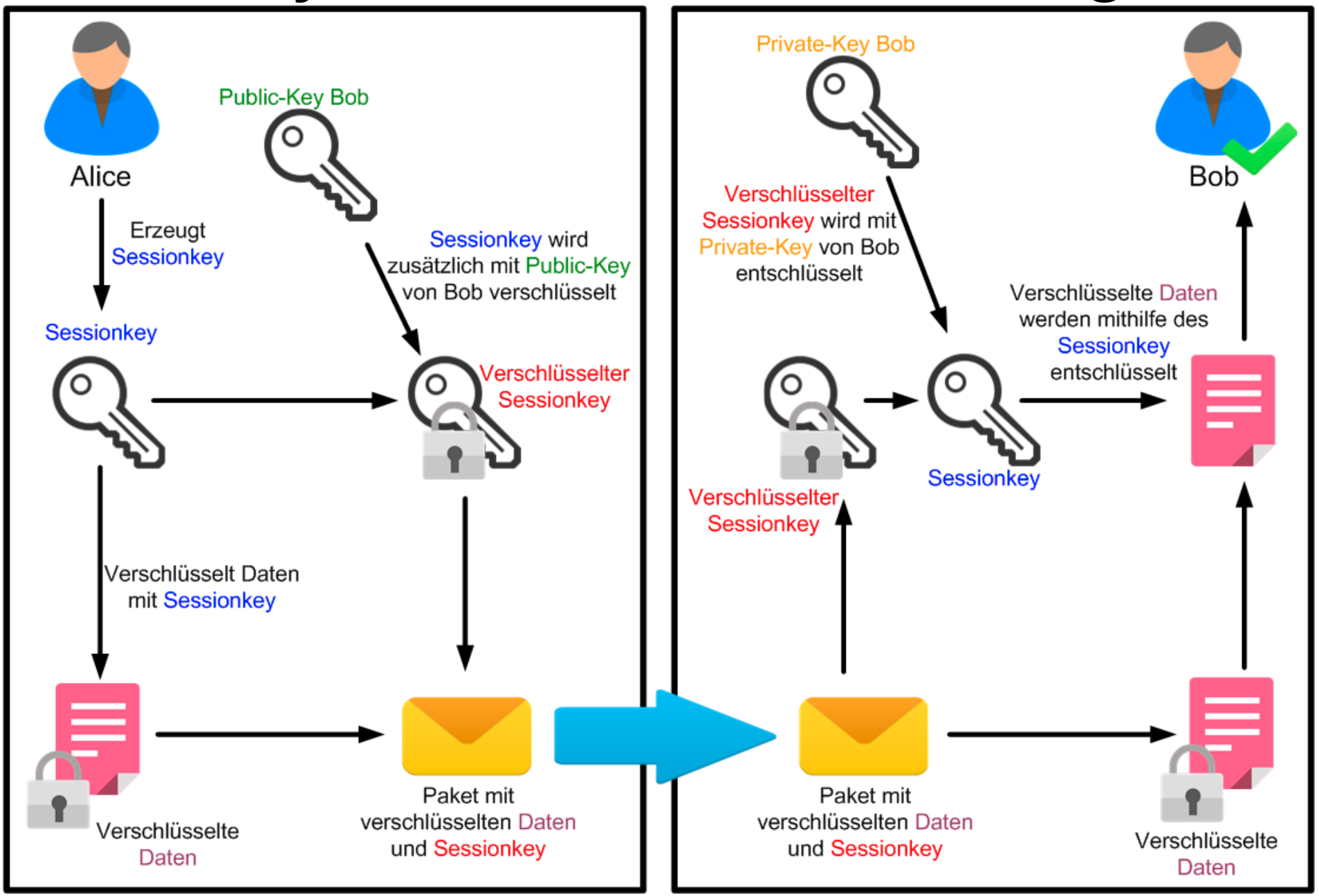
Quelle:
Von Crypto-man - selbst in OpenOffice 2.0.4 erstellt, extra für die Wikipedia, Bild-frei, https://de.wikipedia.org/w/index.php?curid=4975924

Hybride Verschlüsselung



Quelle:
Von Crypto-man - selbst in OpenOffice 2.0.4 erstellt, extra für die Wikipedia, Bild-frei, https://de.wikipedia.org/w/index.php?curid=4975925

Hybride Verschlüsselung



SSL / TLS

TLS im TCP/IP-Protokollstapel

Anwendung	HTTPS	IMAPS	POP3S	SMTPS	...
Transport	**TLS**				
	TCP				
Internet	IP(IPv4, IPv6)				
Netzzugang	Ethernet	Token Bus	Token Ring	FDDI	...

Transport Layer Security (TLS, deutsch Transportschichtsicherheit), weitläufiger bekannt unter der Vorgängerbezeichnung Secure Sockets Layer (SSL), ist ein hybrides Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet.

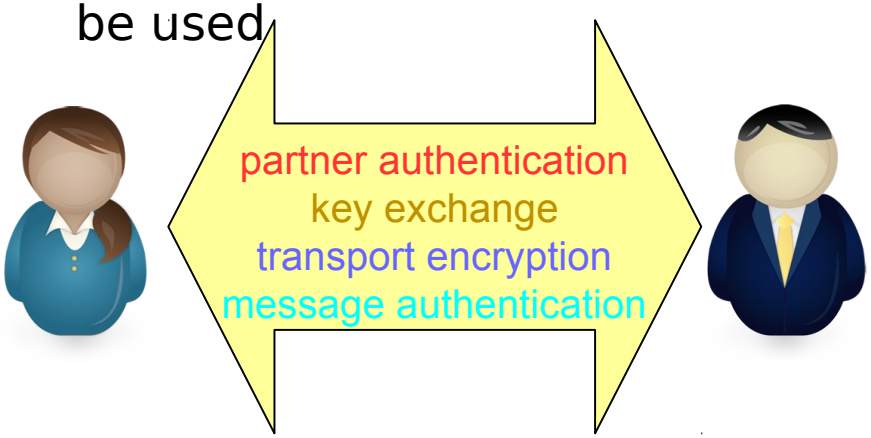
TLS-Verschlüsselung wird heute vor allem mit HTTPS eingesetzt. Die meisten Webserver unterstützen TLS 1.0, viele auch SSLv2 und SSLv3 mit einer Vielzahl von Verschlüsselungsmethoden, fast alle Browser und Server setzen jedoch bevorzugt TLS mit RSA- und AES- oder Camellia-Verschlüsselung ein.

TLS ist ohne eine zertifikatsbasierte Authentifizierung anfällig für Man-in-the-Middle-Angriffe: Ist der Man-in-the-Middle vor der Übergabe des Schlüssels aktiv, kann er beiden Seiten seine Schlüssel vorgaukeln und so den gesamten Datenverkehr im Klartext aufzeichnen und unbemerkt manipulieren. Wegen der mangelnden Vertrauenswürdigkeit einiger Zertifizierungsstellen wird seit Anfang 2010 die Sicherheit von TLS grundsätzlich angezweifelt. Durch die Deaktivierung fragwürdiger Zertifizierungsstellen im eigenen Browser lässt sich dieses Risiko jedoch weitgehend beseitigen.

SSL/TLS Cipher Suites

TLS (former versions were called SSL)

- protocol for secure communication
- e.g. used in https
- starts with negotiating the encryption and authentication methods to be used



name of a cipher suite:

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256

Partner (Key) Authentication

- RSA based certificates

Key Exchange

- Diffie-Hellman ephemeral (to agree on AES key), ephemeral means DH key are recomputed often

Transport Encryption

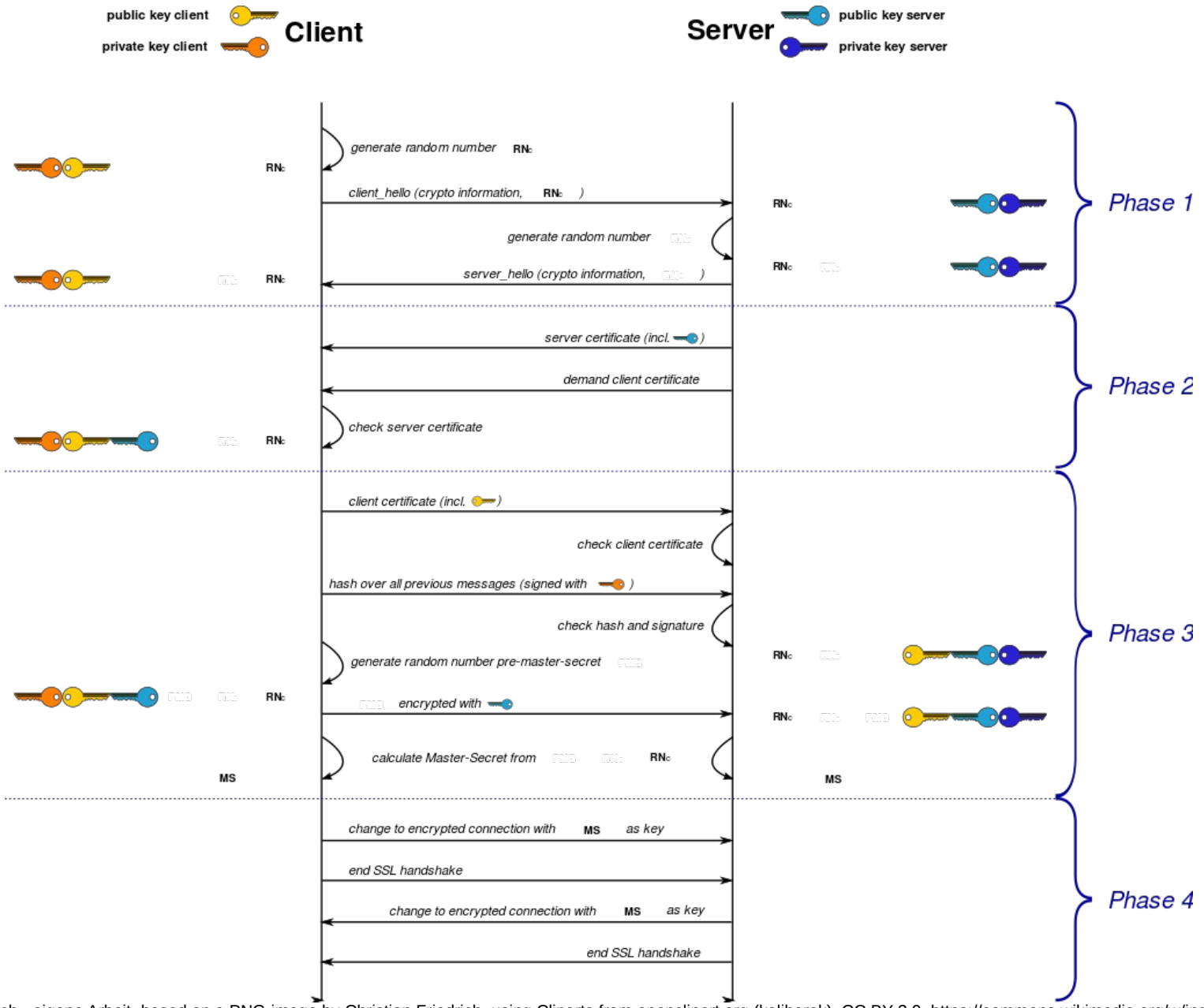
- AES with 128 bit key and cipher block chaining

Message Authentication

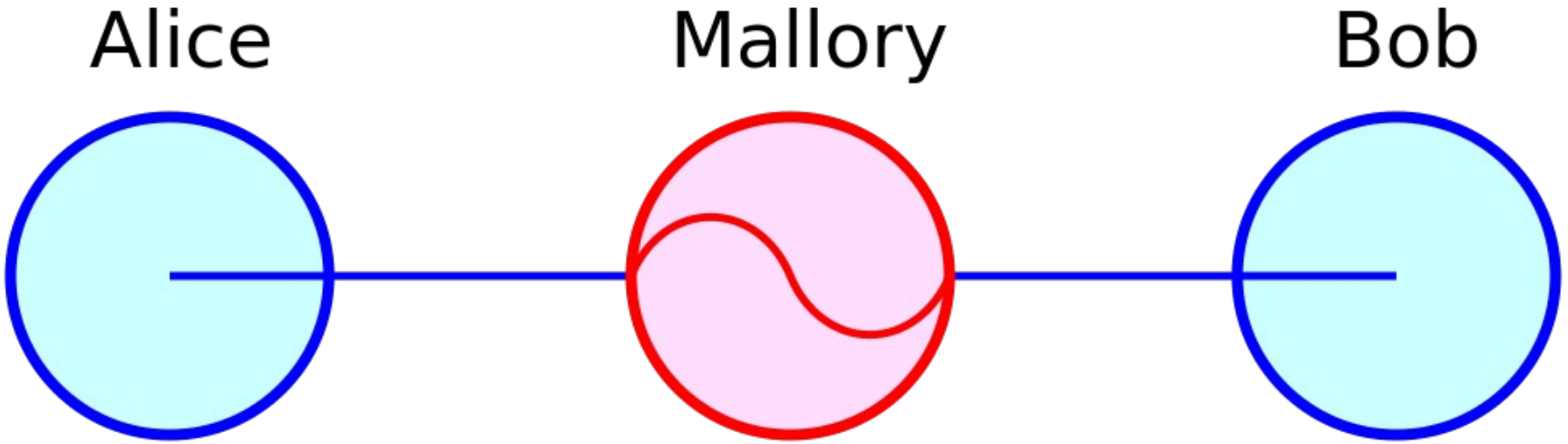
- HMAC using SHA-256 (hash size 256 bits)

The details are spread across many RFCs.

TLS Handshake Protocol

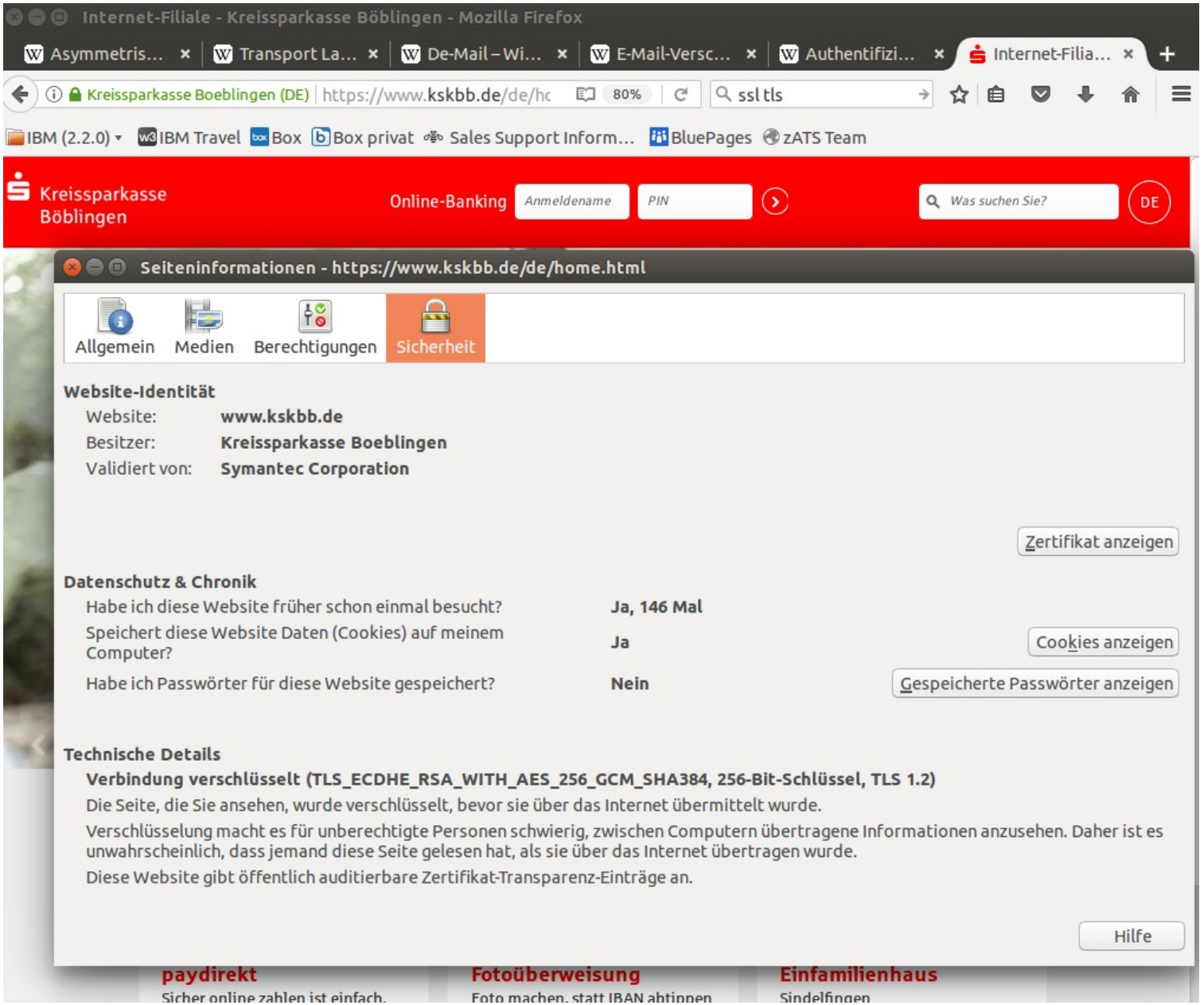


Man-in-the-Middle-Angriff

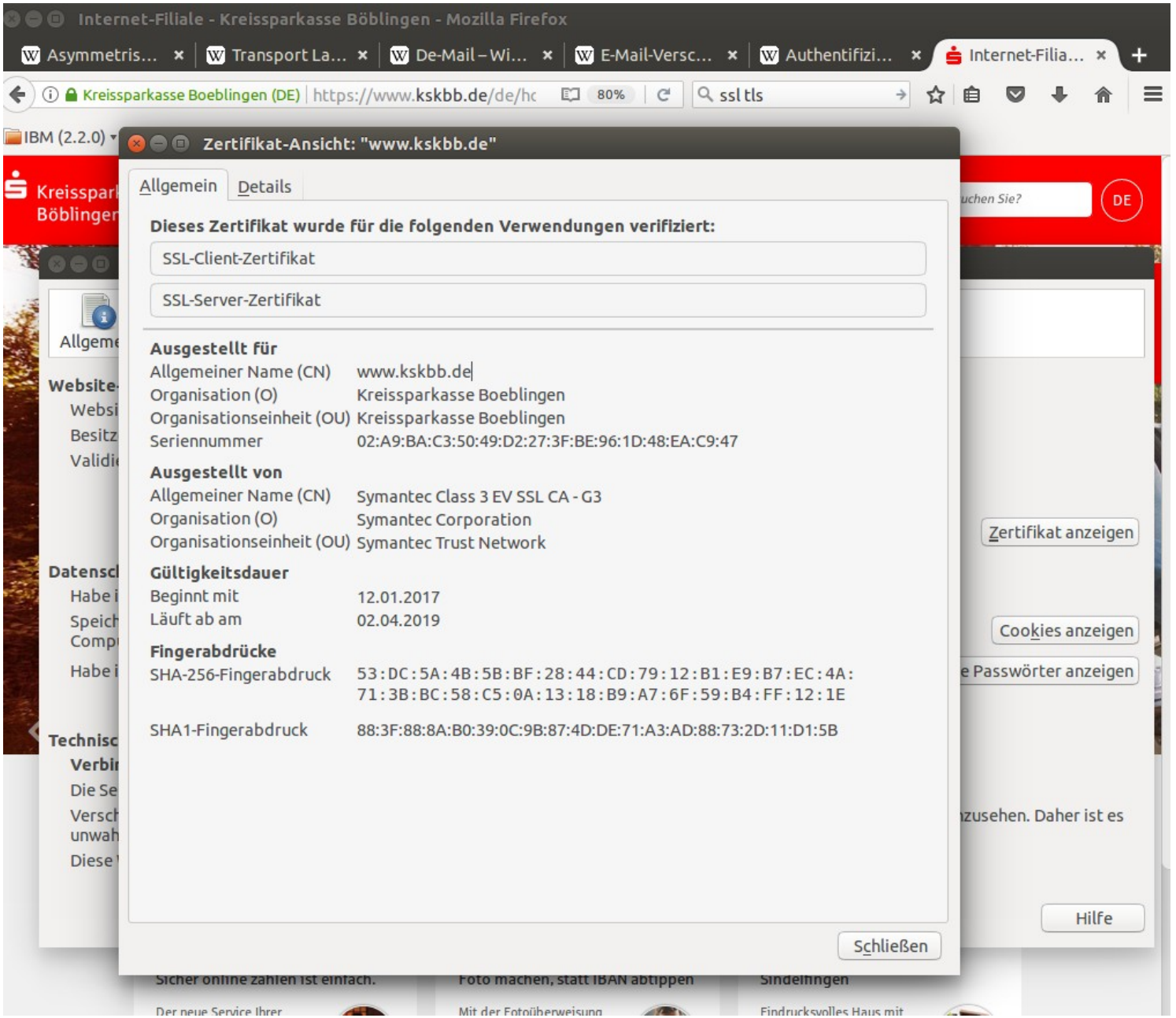


Quelle: Von Miraceti - Eigenes Werk, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=5672044

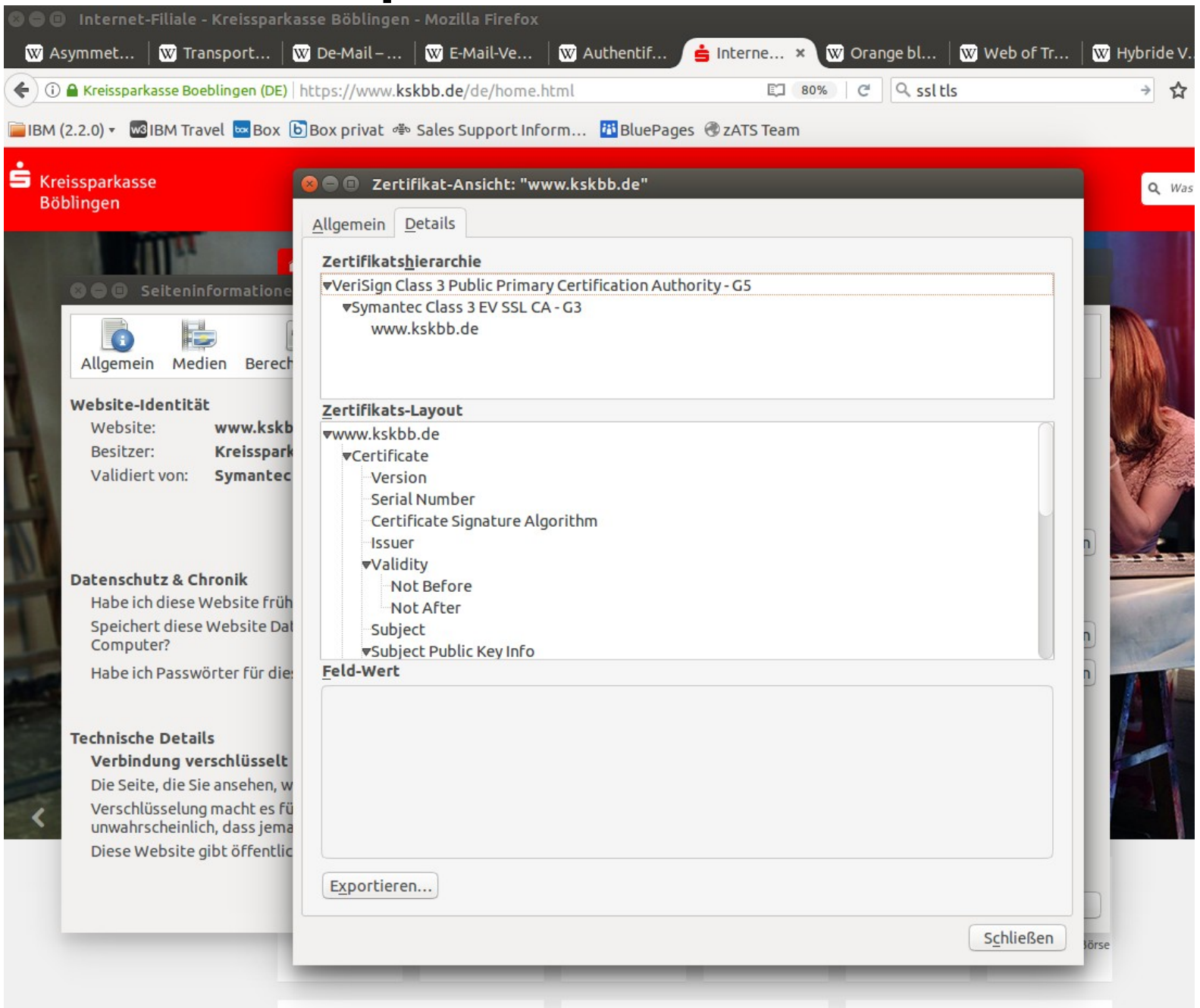
Beispiel: Webseite



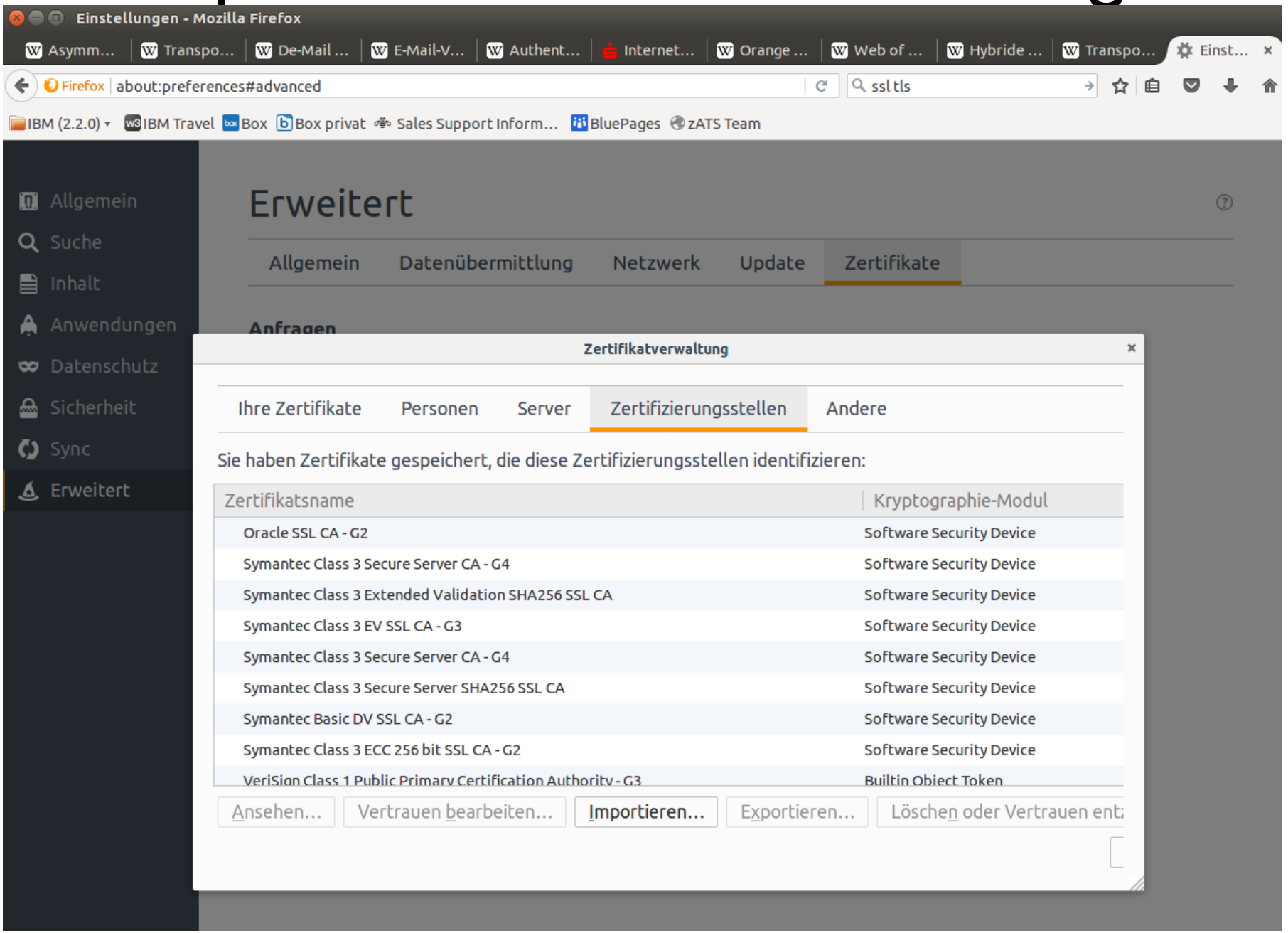
Beispiel: Webseite . . .



Beispiel: Webseite . . .



Beispiel: Browser-Einstellungen



E-mail Verschlüsselung

E-Mail-Verschlüsselung wird verwendet, um vertrauliche Informationen so per E-Mail vom Absender zum Empfänger zu schicken, dass niemand außer Absender und Empfänger sonst Zugang zu diesen Informationen bekommt (Ende-zu-Ende-Verschlüsselung).

Die **E-Mail-Verschlüsselung geht oft einher mit der digitalen Signatur** und wird in vielen Szenarien tatsächlich mit ihr kombiniert. Das Ziel einer digital signierten E-Mail ist es, Informationen so vom Absender zum Empfänger zu schicken, dass sie niemand unbemerkt auf dem Weg vom Absender zum Empfänger manipulieren kann. Die E-Mail-Signatur befriedigt das Bedürfnis nach Authentizität und Integrität.

Client-basierte E-Mail-Verschlüsselung und -Signatur

Die klassische E-Mail-Verschlüsselung und -Signatur erfolgt von Client zu Client (Ende-zu-Ende-Verschlüsselung).
Die Verschlüsselung und Signatur der Nachricht übernimmt der E-Mail-Client von Alice. Zur Verschlüsselung wird der öffentliche Schlüssel von Bob verwendet. Die Signatur erfolgt mit dem privaten Schlüssel von Alice.
Die Entschlüsselung und Signaturprüfung der Nachricht übernimmt der E-Mail-Client von Bob. Die Entschlüsselung erfolgt mit dem privaten Schlüssel von Bob. Die Prüfung der Signatur erfolgt mit dem öffentlichen Schlüssel von Alice.

Server-basierte E-Mail-Verschlüsselung und -Signatur

Client-basierte Lösungen haben den Nachteil, dass sie für viele Organisationen (Unternehmen, Vereine, …) zu komplex sind. In solchen Situationen sind Server-basierte Lösungen das Mittel der Wahl. Die Arbeit der Verschlüsselung und Signatur wird dabei nicht von Clients, sondern von Servern erledigt.

E-mail Verschlüsselung

PKI-basierte E-Mail-Verschlüsselung und -Signatur

Die häufig angetroffene Methode, bei der E-Mail Vertraulichkeit und Authentizität zu erreichen, ist die PKI-basierte E-Mail-Verschlüsselung und -Signatur. PKI steht für Public-Key-Infrastruktur. Bei der PKI-basierten E-Mail-Verschlüsselung und -Signatur kommt fast immer einer der zwei folgenden Standards zum Einsatz:

S/MIME: Secure / Multipurpose Internet Mail Extensions
OpenPGP: Open Pretty Good Privacy

PKI-basierte E-Mail-Verschlüsselung und -Signatur kommt sowohl bei Client-basierten Lösungen als auch bei Server-basierten Lösungen zum Einsatz.

Passwort-basierte E-Mail-Verschlüsselung

Die Passwort-basierte E-Mail-Verschlüsselung ist eine Option, die von Server-basierten Lösungen angeboten werden kann.

Kommentar:
Für mich ist die entscheidende Frage, wer erzeugt den privaten Schlüssel?
Wo ist der private Schlüssel abgespeichert?

OpenPGP, GnuPG, PGP, gnupg sind nur unterschiedliche Implementierungen

Quellen und weitere Informationen

Simon Singh, Geheime Botschaften Carl Hanser Verlag – Roman

Bruce Schneier, Applied Cryptography, Secrets and Lies, and Practical Cryptography Paperback – 26 Oct 2007

Aktuell: http://www.spiegel.de/netzwelt/netzpolitik/wikileaks-enthuellung-vault-7-cia-soll-auch-von-deutschland-aus-spionieren-a-1137580.html

Steganographie: https://de.wikipedia.org/wiki/Steganographie
Authentifizierung: https://de.wikipedia.org/wiki/Authentifizierung
Web of Trust: https://de.wikipedia.org/wiki/Web_of_Trust
Man-in-the-Middle-Angriff: https://de.wikipedia.org/wiki/Man-in-the-Middle-Angriff
Kerckhoffs' Prinzip: https://de.wikipedia.org/wiki/Kerckhoffs%E2%80%99_Prinzip
Hybride Verschlüsselung: https://de.wikipedia.org/wiki/Hybride_Verschl%C3%BCsselung
E-Mail-Verschlüsselung: https://de.wikipedia.org/wiki/E-Mail-Verschl%C3%BCsselung
DE-Mail: https://de.wikipedia.org/wiki/De-Mail
Asymmetrisches Kryptosystem: https://de.wikipedia.org/wiki/Asymmetrisches_Kryptosystem
Transport Layer Security: https://de.wikipedia.org/wiki/Transport_Layer_Security
Zertifikate: https://de.wikipedia.org/wiki/X.509
Angiffe: https://de.wikipedia.org/wiki/Diffie-Hellman-Schl%C3%BCsselaustausch#cite_note-GOLDBELL-47

Vortrag von Dr. Reinhard Bündgen, IBM