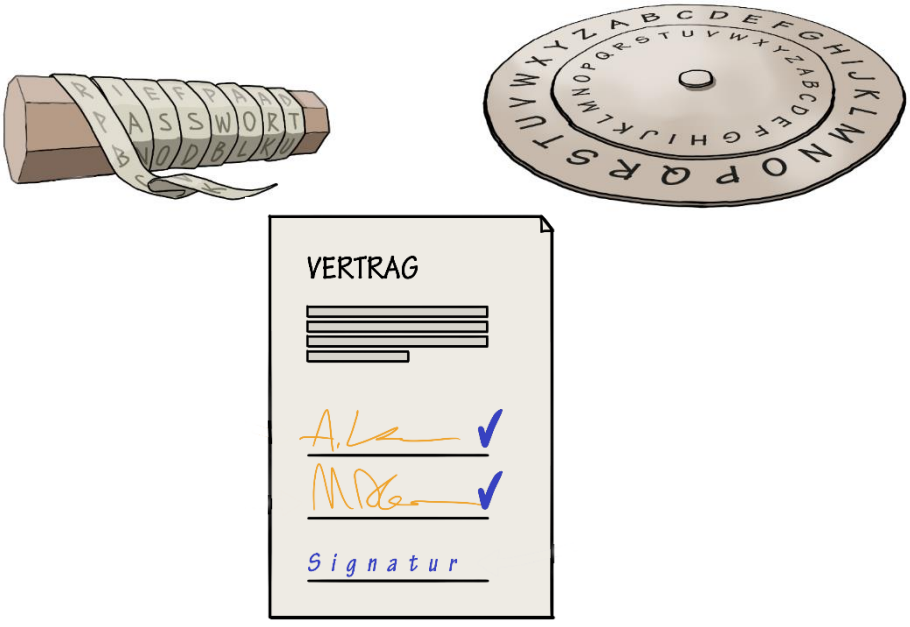
AKADEMIE FÜR LEHRERFORTBILDUNG UND PERSONALFÜHRUNG
DILLINGEN

Datensicherheit durch

Verschlüsselung

Von geheimen Botschaften zur elektronischen Unterschrift



SCHULNETZ

Handreichung für Lehrkräfte

INHALT

IMPRESSUM

Herausgeber: Akademie für Lehrerfortbildung und Personalführung
Kardinal-von-Waldburg-Str. 6-7
89407 Dillingen

Autoren: Georg Schlagbauer, Akademie Dillingen
Markus Bader, Staatliche Berufsschule III, Fürth
Thomas Pickel, Maximilian-Kolbe-Schule Neumarkt
Wolf Gebele, Staatliche Realschule Gemünden am Main
Susanne Schaffer, Carl-von-Linde Schule, Kulmbach
Wolfgang Plank, Goethe-Gymnasium Regensburg
Christian Maushart, Bürgernetz Dillingen e. V.
Markus Rawitzer, Akademie Dillingen
Kurt Windberger, Akademie Dillingen
Peter Botzenhart, Akademie Dillingen
Markus Hahn, Regierung von Oberbayern

Grafiken: David Kremer, Augsburg

URL: http://schulnetz.alp.dillingen.de/materialien
Mail: schlagbauer@alp.dillingen.de
Stand: Dezember 2020

GEHEIME BOTSCHAFTEN

Geheimsprachen haben schon immer unser Interesse geweckt. Wollten wir als Schüler unserem Klassenkameraden eine Nachricht zukommen lassen, die nur er verstehen sollte, nutzten wir eine nur uns bekannte Sprache, unsichtbare Tinte oder wir erfanden einen einfachen Code, indem wir z. B. Buchstaben durch Zeichen oder andere Buchstaben ersetzten. Verschlüsselung ist den meisten Menschen also nicht unbekannt.

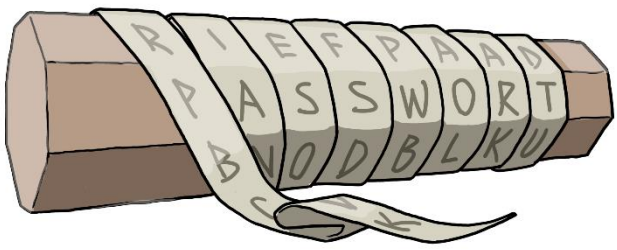
Heute nutzen wir ganz unterschiedliche Kanäle zur Kommunikation und viele davon basieren auf dem Internet. Aber gerade hier wird eine sichere und vertrauliche Kommunikation immer wichtiger, vor allem deshalb, weil der Kommunikationsweg über viele Stationen führt und immer mehr kritische Anwendungen über das Internet erfolgen, die Vertraulichkeit erfordern, wie z. B. die Steuerung von Maschinen oder das Homebanking.

Die folgende Handreichung gibt einen kurzen Einblick, wie Verschlüsselungstechniken eingesetzt werden, um die Authentisierung von Personen oder Computern zu ermöglichen und die Vertraulichkeit, Integrität und Verfügbarkeit von Daten zu gewährleisten.

HISTORISCHE VERSCHLÜSSELUNGSTECHNIKEN

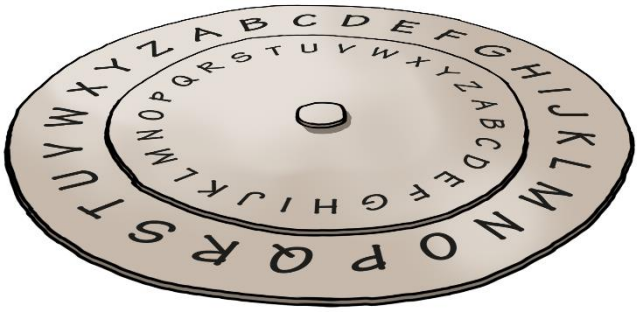
Verschlüsselung ist keine Erfindung des Computerzeitalters. Es wurden schon immer Wege gesucht, um eine vertrauliche Kommunikation zu ermöglichen, hauptsächlich um militärische Nachrichten vor dem unbefugten Mitlesen abzusichern. Dazu einige Beispiele:

SKYTALE



Die Skytale ist ein Verschlüsselungsverfahren, das bereits von den Spartanern vor 2500 Jahren eingesetzt wurde. Der Sender der Nachricht wickelt dabei ein Pergament um einen Stock und schreibt darauf die Nachricht. Die Zwischenräume werden mit willkürlichen Buchstaben aufgefüllt. Ohne den zugehörigen Stock erkennt man nur vermeintlich unsinnig aneinander gereihte Buchstaben. Der Empfänger kann die Nachricht nur mit einem Stock des gleichen Durchmessers entschlüsseln. Dieser Durchmesser muss zwischen Sender und Empfänger als gemeinsamer „Schlüssel“ vereinbart sein.

CÄSAR

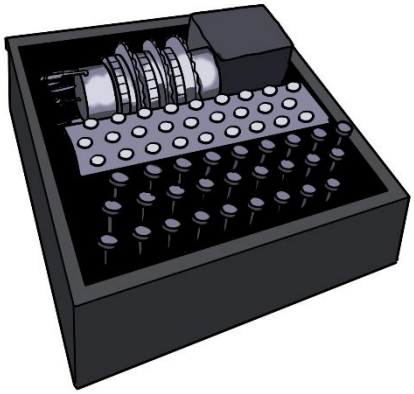


Die Cäsar-Verschlüsselung ist ein Verschlüsselungsverfahren, bei dem jeder Buchstabe auf einen anderen Buchstaben abgebildet wird. Handelt es sich nur um eine Verschiebung des Alphabets, muss lediglich der Verschiebungswert als „Schlüssel“ bekannt sein, damit die Nachricht entschlüsselt werden kann.

Bei einem Verschiebungswert von 3 wird aus einem A ein D, B wird zu E, usw. Das Wort „WAHR“ lautet verschlüsselt ZDKU. Werden die Buchstaben des Alphabets willkürlich auf einen jeweils anderen Buchstaben abgebildet, muss jeder Kommunikationsteilnehmer die Verteilung als Schlüssel kennen.

Zur Vereinfachung benutzten die Römer zwei verdrehbare Scheiben.

ENIGMA

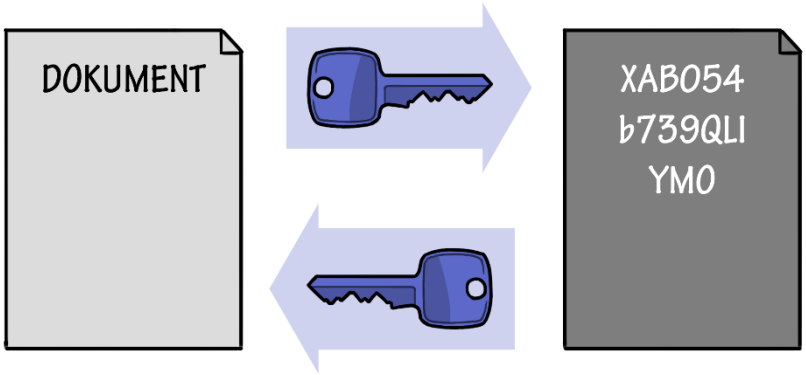


Die Enigma wurde vor allem bekannt, weil sie im zweiten Weltkrieg von der deutschen Wehrmacht zur Verschlüsselung des Nachrichtenverkehrs verwendet wurde. Sie sieht aus wie eine alte Schreibmaschine, besitzt aber drei bewegliche Walzen die miteinander verdrahtet sind. Der Schlüssel, der jedem Kommunikationspartner bekannt sein muss, setzt sich aus mehreren Faktoren zusammen, wie zum Beispiel der Auswahl der Walzen, der Reihenfolge der Montierung, der Verdrahtung oder auch der Grundstellung.

GRUNDLAGEN AKTUELLER VERSCHLÜSSELUNGEN

SYMMETRISCHE VERSCHLÜSSELUNG

Die symmetrische Verschlüsselung ist das Standardverfahren bei der Verschlüsselung von Dateien, Dokumenten, Datenträgern und auch für die verschlüsselte Kommunikation. Sie ist sehr schnell durchführbar, da sie nur auf einfachen Datenmanipulationen besteht. Das bekannteste und heute allgemein übliche Verfahren ist AES (Advanced Encryption Standard) mit unterschiedlichen Schlüssellängen.

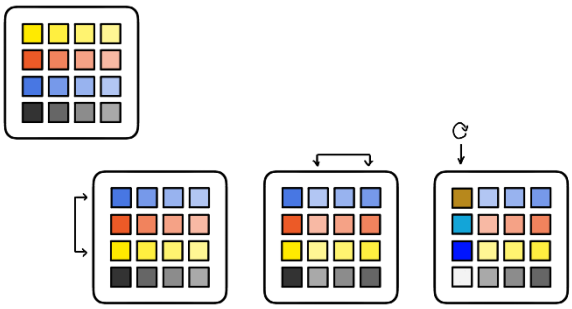


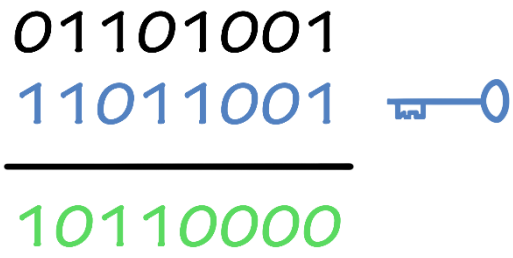
Verschlüsselung eines Dokuments: Zum Verschlüsseln und zum Entschlüsseln wird der gleiche Schlüssel verwendet.

KENNZEICHEN DER SYMMETRISCHEN VERSCHLÜSSELUNG

- Zum Verschlüsseln und zum Entschlüsseln wird der gleiche Schlüssel verwendet. Dieser Schlüssel muss demnach geheim gehalten werden.
- Die Herausforderung beim Einsatz dieses Verschlüsselungsverfahrens stellt der sichere Schlüsselaustausch dar (Schlüsselverteilungsproblem).

GRUNDSÄTZLICHE FUNKTIONSWEISE DER SYMMETRISCHEN VERSCHLÜSSELUNG



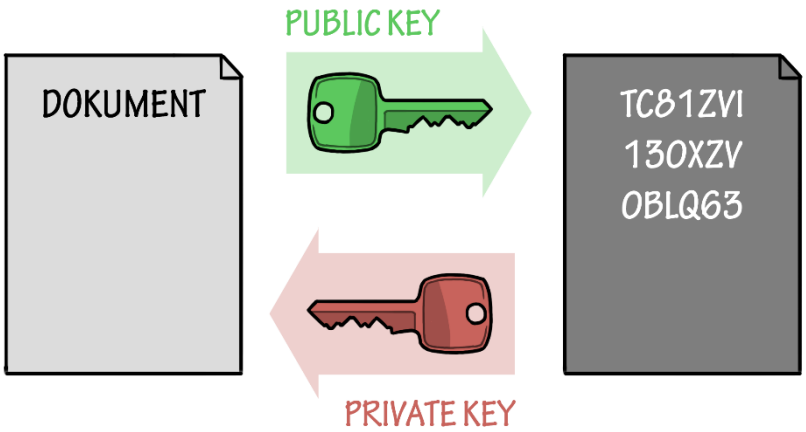


Die zu verschlüsselnden Daten werden in Blöcken angeordnet und nach einem festgelegten Algorithmus „verwürfelt“ (z.B.: Vertausche erste und dritte Zeile, vertausche zweite und vierte Spalte, invertiere in der ersten Spalte jeweils das erste Bit, etc). Danach wird für jeden Block aus dem geheimen Schlüssel ein sogenannter Rundenschlüssel erzeugt und die einzelnen Blöcke und der Rundenschlüssel werden bitweise mit einer XOR-Operation verknüpft. Daraus entsteht das verschlüsselte Dokument. Alle diese Operationen sind umkehrbar und können von einem Computer sehr schnell durchgeführt werden.

ASYMMETRISCHE VERSCHLÜSSELUNG

Bis in die 1970er-Jahre ging man davon aus, dass zum Verschlüsseln und zum Entschlüsseln immer der gleiche Schlüssel notwendig ist, der demnach natürlich geheim gehalten werden muss.

Erst 1975 wurden erste Ideen und kurz darauf auch konkrete Verfahren veröffentlicht, wie eine Verschlüsselung auch ohne ein solches „gemeinsames Geheimnis” funktioniert.



Verschlüsselung eines Dokuments: Zum Verschlüsseln und zum Entschlüsseln werden unterschiedliche Schlüssel verwendet.

KENNZEICHEN DER ASYMMETRISCHEN VERSCHLÜSSELUNG:

- Es gibt ein zusammengehörendes Schlüsselpaar A, B. Wenn man einen Text mit dem Schlüssel A verschlüsselt, kann man diesen mit dem Schlüssel B entschlüsseln und umgekehrt.
- Obwohl das Schlüsselpaar A, B zusammengehört, gibt es keinen Weg, wie man aus A den Schlüssel B berechnen kann oder umgekehrt.

In der Praxis werden asymmetrische Verfahren immer so eingesetzt, dass man einen der beiden Schlüssel öffentlich bekannt gibt (public key) und den anderen geheim hält (private key). Deshalb werden asymmetrische Verschlüsselungen auch als Public-Key-Verfahren bezeichnet. Das bekannteste asymmetrische Verschlüsselungsverfahren ist die RSA-Verschlüsselung, benannt nach ihren Entwicklern Rivest, Shamir und Adleman.

WIE WIRD EIN SCHLÜSSELPAAR A, B ERZEUGT?

Das Schlüsselpaar A, B wird aus zwei sehr großen Primzahlen (in der Praxis mit mehr als 300 Dezimalstellen) berechnet. Nach der Berechnung wirft man die beiden Primzahlen weg und hat nur noch das Schlüsselpaar A, B. Ohne Kenntnis der beiden ursprünglichen Primzahlen gibt es keinen praktikablen Weg, aus A den Schlüssel B zu berechnen oder umgekehrt.

Die konkreten Algorithmen (z. B. für RSA) sind in der einschlägigen Literatur gut dokumentiert.

ASYMMETRISCHE VERFAHREN IN DER PRAXIS

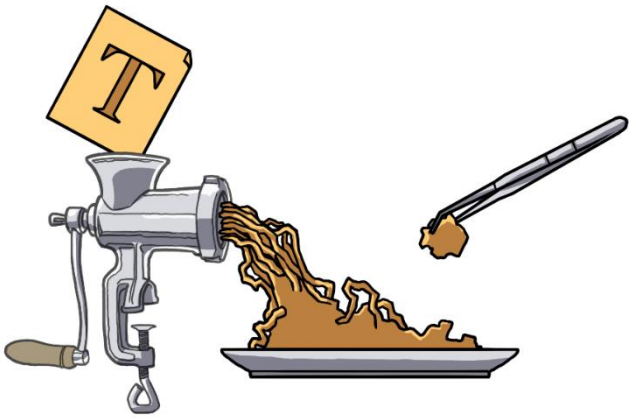
Asymmetrische Verfahren ermöglichen die Verschlüsselung, ohne dass vorher ein gemeinsamer Schlüssel ausgetauscht wird. Da sie im Vergleich zu symmetrischen Verfahren sehr langsam sind, werden damit in der Praxis z. B. symmetrische Schlüssel ausgetauscht. Die eigentliche Verschlüsselung großer Dokumente oder der Datenübertragung erfolgt symmetrisch (Hybride Verschlüsselung). Des Weiteren kommt die asymmetrische Verschlüsselung bei Signaturen oder digitalen Zertifikaten zum Einsatz.

HASHWERTE

Man kann sich einen Hashwert wie einen Fingerabdruck eines Textes vorstellen. Aus einem vorgegebenen Text kann man einen eindeutigen Hashwert erstellen. Der gleiche Text ergibt immer den gleichen Hashwert, ein anderer Text, auch wenn nur ein Zeichen verändert wurde, ergibt einen anderen Hashwert.

Es ist umgekehrt nicht möglich, aus einem Hashwert den Text zu rekonstruieren. Man spricht deshalb von einer Einwegfunktion. Hashwerte haben auch immer die gleiche fest vorgegebene Größe (je nach Hashverfahren z. B. 256 Bit), unabhängig von der Länge des Textes oder der Größe einer Datei. Sie eignen sich deshalb sehr gut, um zu kontrollieren, ob große Dateien oder Dokumente verändert wurden, indem man überprüft, ob sich die Hashwerte verändert haben.

Ein Beispiel:



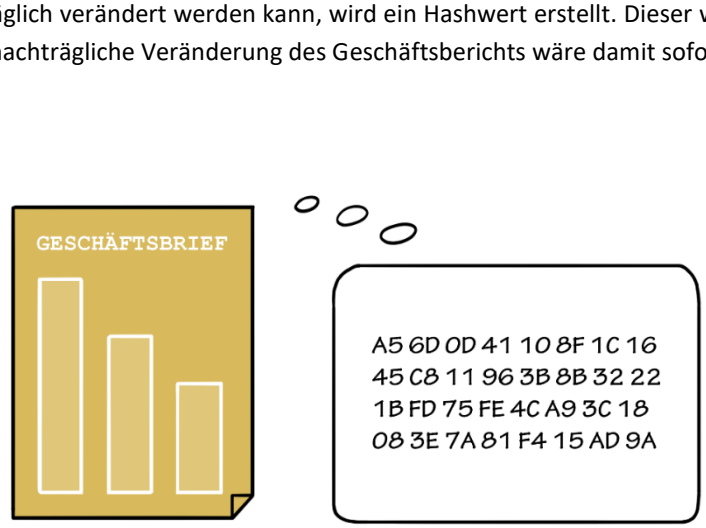
Ein Stück weit kann man sich eine Hashfunktion wie einen Fleischwolf vorstellen. Der Fleischwolf symbolisiert die Einwegfunktion, er produziert „Haschee“. Es ist nicht möglich, das Ergebnis rückgängig zu machen.

Bleiben wir bei diesem Beispiel:

Eine Probe des Gehackten, aber auch die Gesamtmenge, besitzt eine einmalige sehr spezifische relative Zusammensetzung (Inhaltsstoffe, Vitamine, Mineralstoffe etc.). Dies entspricht dem Hashwert. Nur ein identisches Fleischstück besitzt die genau gleiche Zusammensetzung und ergäbe einen identischen Hashwert. Theoretisch könnte auch ein anderes Fleischstück die exakt gleiche Zusammensetzung bieten. In der Informationsverarbeitung spricht man in diesem Fall von einer „Kollision“. Das ist theoretisch möglich, soll aber durch die Wahl des Hashverfahrens praktisch auszuschließen sein.

Geschäftsbericht eines Unternehmens:

Der Geschäftsbericht eines Unternehmens ist ein umfangreiches Dokument. Um sicherzugehen, dass der Bericht nicht nachträglich verändert werden kann, wird ein Hashwert erstellt. Dieser wird beispielsweise veröffentlicht. Eine nachträgliche Veränderung des Geschäftsberichts wäre damit sofort erkennbar.



Hashwert eines Dokuments: In der Grafik ist das Ergebnis einer Hash-Funktion mit 128 Bit dargestellt.

Kennzeichen von Hashverfahren:

- Hashwerte haben eine fest vorgegebene Länge (z. B. 256 Bit), unabhängig von der Länge des Originaldokuments.
- Selbst eine kleine Veränderung des Originaldokuments ergibt einen völlig anderen Hashwert.
-
- Es ist in der Praxis nicht möglich, zwei verschiedene Dokumente zu finden, die den gleichen Hashwert besitzen (Kollisionssicherheit).

Obwohl man leicht beweisen kann, dass es verschiedene Dokumente geben muss, die zum gleichen Hashwert führen, soll es in der Praxis nicht möglich sein, gezielt solche Dokumente zu finden. Wenn dies mit schnellen Computern oder neuen Verfahren einmal möglich sein sollte, müsste man sich ein anderes Hashverfahren ausdenken. Dies war beispielsweise bei MD5 der Fall.

Einsatzbereiche für Hash-Verfahren

- Verschlüsselung von Passwörtern
- Elektronische Signatur von Dokumenten
- Kryptographische Prüfsummen
- Ausstellen von Zertifikaten

Gebräuchliche Hash-Funktionen

- MD5: Länge 64 Bit; sehr weit verbreitet, gilt mittlerweile als zu unsicher
- SHA-1: Länge 128 Bit; gilt mittlerweile als eventuell unsicher
- SHA-2: Länge üblicherweise 256 Bit; aktueller Standard
- SHA-3: (unterschiedliche Längen); evtl. zukünftiger Standard

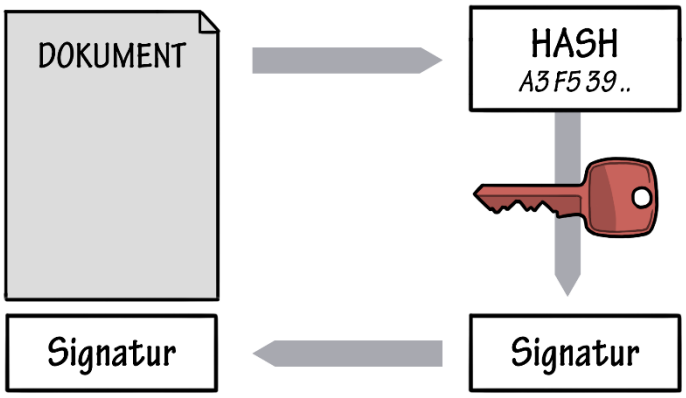
DIGITALE SIGNATUREN

Die digitale Signatur ist mit der Unterschrift unter einem Dokument vergleichbar. So wie man mit einer analogen Unterschrift bestimmte Gütekriterien verbindet, muss auch die digitale Signatur verschiedenen Überprüfungen standhalten:

- Die Signatur muss einer bestimmten Person oder Organisation zugeordnet werden können und muss auf Echtheit überprüfbar sein.
- Die Signatur muss einem Dokument zugeordnet werden können. Man darf das Dokument nicht nachträglich verändern oder die Signatur unter ein anderes Dokument setzen können.

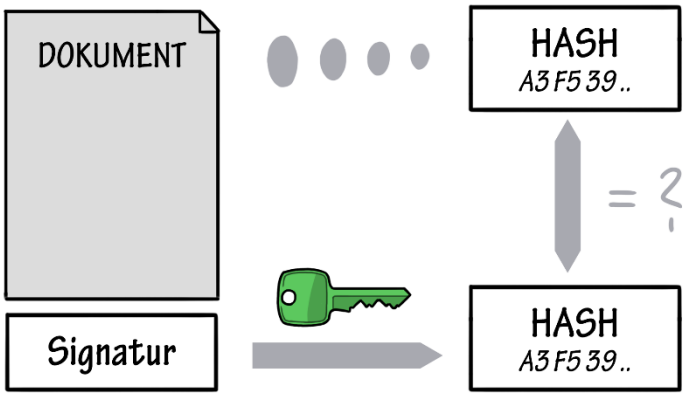
Hashwerte eines Dokuments ermöglichen einen eindeutigen Fingerabdruck. Die Verschlüsselung des Hashwertes mit dem privaten Schlüssel des Unterzeichners ergibt die Signatur.

Signatur eines Dokuments:



- Der Unterzeichner bildet einen Hashwert des Dokuments und verschlüsselt diesen mit seinem privaten Schlüssel.
- Der so verschlüsselte Hashwert wird als Anhang dem Dokument beigefügt. Diesen Anhang bezeichnet man als Signatur.

Überprüfung der Signatur und Echtheit des Dokuments



- Der Empfänger bildet einen Hashwert des Dokuments mit dem gleichen Hashverfahren wie der Unterzeichner.
- Der Empfänger entschlüsselt den vom Unterzeichner im Anhang des Dokuments mitgelieferten verschlüsselten Hashwert mit dem allgemein zugänglichen öffentlichen Schlüssel des Unterzeichners.
- Wenn die beiden Ergebnisse identisch sind, wird die Signatur und die Echtheit des Dokuments akzeptiert.

Selbst eine geringe Veränderung am Dokument würde zu einem völlig anderen Hashwert und damit zu einer anderen Signatur führen. Die Signatur kann nur jemand durchführen, der im Besitz des privaten Schlüssels des Unterzeichners ist.

Voraussetzungen für eine digitale Signatur:

Aus dem oben beschriebenen Verfahren für eine digitale Signatur ergeben sich folgende Voraussetzungen:

- Der Unterzeichner des Dokuments ist im Besitz eines privaten und eines öffentlichen Schlüssels.
- Der private Schlüssel ist geheim. Niemand, außer dem Unterzeichner des Dokuments darf Zugriff auf dessen privaten Schlüssel haben.
- Der öffentliche Schlüssel des Unterzeichners ist dem Empfänger des Dokuments zugänglich. Es muss auch gewährleistet sein, dass der Empfänger den richtigen öffentlichen Schlüssel verwendet.

Wie die genannten Voraussetzungen erfüllt werden können, ist in den Kapiteln „Digitale Zertifikate“ und „Elektronische Unterschrift“ dargestellt.

DIGITALE ZERTIFIKATE

Das Ausstellen eines Zertifikats ist mit der Ausstellung eines Führerscheins vergleichbar. Der Führerschein muss von einer vertrauenswürdigen Institution ausgestellt und signiert werden (z. B. dem Landratsamt). Der Führerschein selbst muss auf Echtheit überprüfbar sein und es muss überprüfbar sein, dass der Führerschein zu der entsprechenden Person gehört.

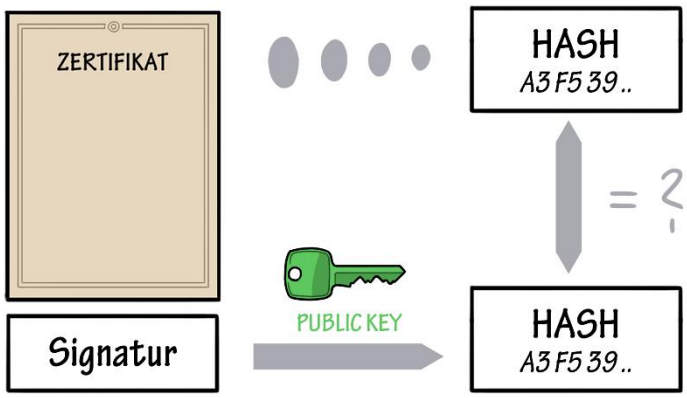
Qualifizierte Zertifikate

Technisch gesehen ist ein digitales Zertifikat ein von einer anerkannten vertrauenswürdigen Institution ausgestelltes und signiertes Dokument. Ein qualifiziertes Zertifikat muss zudem einige rechtliche Voraussetzungen erfüllen.

Üblicherweise enthält ein Zertifikat folgende Informationen:

- den Namen des Inhabers des Zertifikats
- Versionsnummer, Seriennummer und Gültigkeitsdauer
- Informationen zum Verwendungszweck
- den öffentlichen Schlüssel des Inhabers
- den Namen der Zertifizierungsstelle
- die digitale Signatur des Zertifikats

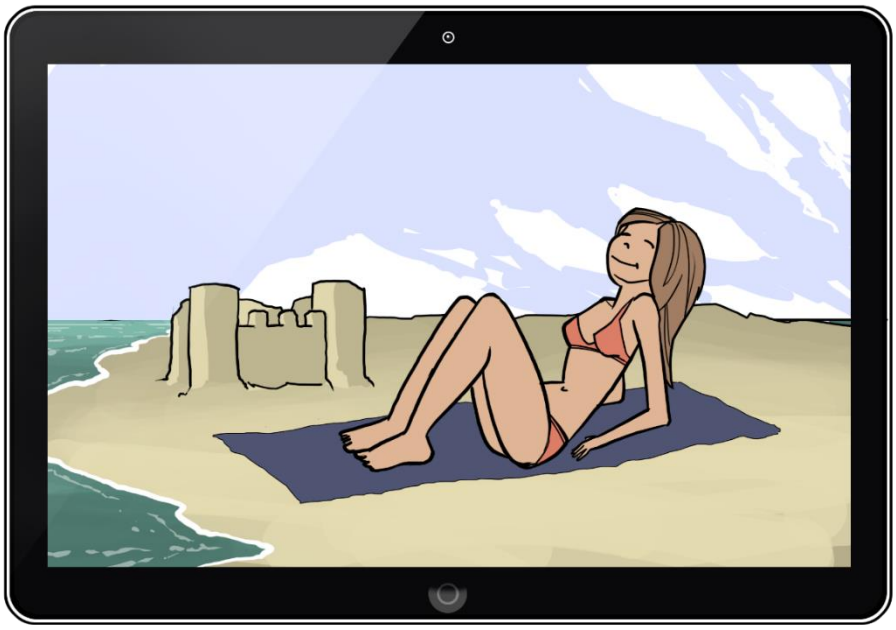
Wie überprüft ein Empfänger die Echtheit eines Zertifikats?



- Der Empfänger bildet einen Hashwert des Zertifikats mit dem gleichen Hashverfahren wie der Unterzeichner.
- Der Empfänger entschlüsselt die Signatur des Zertifikats mit dem allgemein bekannten und öffentlich zugänglichen Schlüssel der Zertifizierungsstelle.
- Wenn die beiden Ergebnisse identisch sind, wird das Zertifikat akzeptiert.

Üblicherweise sind auf einem Computer viele öffentliche Schlüssel der vertrauenswürdigen Zertifizierungsstellen gespeichert. Der Empfänger braucht also nicht unbedingt eine Internetverbindung, um die Echtheit eines Zertifikats zu bestätigen.

VERSCHLÜSSELUNG VON DATEIEN UND DATENTRÄGERN



Private Dokumente sollen eventuell nicht für jeden sichtbar sein. Gegebenenfalls ist es sinnvoll, solche Dokumente zu verschlüsseln.

Wenn vertrauliche Daten an Orten gespeichert werden sollen, die eventuell auch nicht berechtigten Personen zugänglich werden könnten, ist es sinnvoll, diese Daten zu verschlüsseln. Ebenso macht es Sinn, vertrauliche Daten oder die Datenträger zu verschlüsseln, wenn diese auf einem nicht vertrauenswürdigen Weg transportiert werden.

Das Ziel einer Verschlüsselung von Dateien oder Datenträgern ist die Vertraulichkeit. Obwohl man Zugriff auf eine Datei oder ein Dokument hat, soll es nicht möglich sein, den Inhalt zu lesen, ohne im Besitz des richtigen Passwortes oder Schlüssels zu sein.

Wenn die Verschlüsselung gut ist, können die Daten ohne den Schlüssel nicht wiederhergestellt werden. In vielen Fällen begnügt man sich mit einem Passwort, aus dem das jeweilige Programm den Wiederherstellungsschlüssel generiert. In diesem Fall ist die Verschlüsselung nur so gut wie das Passwort.

Der Vorteil einer Verschlüsselung ist gleichzeitig deren größter Nachteil. Ohne das Passwort oder den Wiederherstellungsschlüssel und ohne das zugehörige Programm sind die Daten nicht mehr zugänglich. Wer Daten verschlüsselt speichert, muss sich immer auch überlegen, wie er diese wieder entschlüsseln kann:

- Welche Programme sind erforderlich?
- Wo sind die Passwörter oder Schlüssel gespeichert?
- Können die Daten notfalls auch auf einem anderen Computer oder auf einem anderen System wiederhergestellt werden?
- Funktioniert die Wiederherstellung auch in einigen Jahren noch?

Häufig gibt es Alternativen zu einer Verschlüsselung:

- Daten nur an sicheren Orten aufbewahren
- Sichere Netzwerkstruktur mit Zugriffsschutz
- Sensible Daten nicht elektronisch speichern

Verschlüsselung von Einzeldokumenten

Der Inhalt eines Dokuments wird verschlüsselt. Der Dateiname ist normalerweise im Klartext vorhanden. Gegebenenfalls kann auch aus der Größe der Datei Rückschluss auf den Inhalt gezogen werden. Beispiel: Verschlüsselung in Office-Programmen

Dokumente in einem verschlüsselten Container

Die Dokumente liegen in einem verschlüsselten Container (z. B. eine große Datei). Nach dem Öffnen des Containers stehen alle Dokumente im Klartext zur Verfügung. Die Sicherheit hängt in der Praxis sehr stark davon ab, wie mit dem geöffneten Container umgegangen wird. Beispiele: Veracrypt, 7-Zip.

Verschlüsselung von Dateisystemen

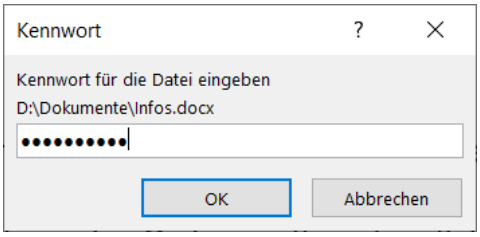
Dateisysteme (Festplattenpartitionen oder mobile Datenträger) können verschlüsselt werden. Wenn ein verschlüsseltes Dateisystem hochgefahren (gemountet) wird (z. B. beim Einschalten eines Computers oder beim Einstecken einer verschlüsselten USB-Festplatte), ist ein Passwort erforderlich. Danach kann mit den Daten ganz normal gearbeitet werden. Je nach Implementierung sind die Daten erst wieder geschützt, wenn der Benutzer abgemeldet wird, der Computer heruntergefahren oder vom Strom genommen wird.

Beispiele: Verschlüsselter USB-Stick, verschlüsselte Partitionen eines Notebooks, verschlüsseltes Volume einer NAS-Box, verschlüsseltes Dateisystem auf einem Smartphone

BEISPIELE FÜR VERSCHLÜSSELUNGSPROGRAMME

Office-Programme

Nahezu alle Office-Programme bieten für Dokumente die Option „Passwortschutz“, die auch eine Verschlüsselung beinhaltet. Beim Öffnen eines Dokuments wird nach dem Passwort gefragt. Ohne dieses kann das Dokument nicht geöffnet werden.



7-Zip

7-Zip (für Windows, Linux) ist ein Kompressionsprogramm, mit dem Dateien oder Ordner komprimiert in einer Datei gespeichert und optional auch verschlüsselt werden können.

7-Zip eignet sich sehr gut, wenn Dateien oder Ordner mit vertraulichen Inhalten verschlüsselt archiviert oder transportiert werden sollen (z. B. Dauerhaftes Speichern von vertraulichen Daten, Ablage in einer Cloud, E-Mail-Anhänge).

Keka

Für MacOS bietet das Programm Keka ähnliche Funktionen wie 7-Zip für Windows. Komprimierte und verschlüsselte Ordner sind zwischen den Programmen kompatibel.

VeraCrypt

VeraCrypt (für Windows. Linux. MacOS) ist ein sehr mächtiges Verschlüsselungsprogramm. Es arbeitet mit verschlüsselten Containern, die beim Öffnen ein Passwort erfordern. VeraCrypt gewährleistet, dass auch während der Bearbeitung keine unverschlüsselten Textteile auf der Festplatte oder in einer temporären Datei abgelegt werden und bietet daher eine sehr hohe Sicherheit.

BitLocker

Bitlocker ist ein Bestandteil des Windows-Betriebssystems, das Teile eines Datenträgers (Partitionen) oder den gesamten Datenträger verschlüsseln kann. Es eignet sich sehr gut zur Verschlüsselung von mobilen Datenträgern (z. B. USB-Sticks), wenn mit Windows gearbeitet wird, oder zur Verschlüsselung von Datenpartitionen bei Windows-Notebooks.

FileVault

FileVault nutzt als Bestandteil des macOS-Filesystems APFS, eine Verschlüsselung, um die Daten auf dem Startvolume eines Macs zu verschlüsseln. Der Wiederherstellungsschlüssel ist an den Benutzeraccount gebunden.

QUALITÄT DER VERSCHLÜSSELUNG

Um die Vertraulichkeit gewährleisten zu können, muss eine Verschlüsselung auch möglichen Angriffsversuchen standhalten. Die Qualität kennzeichnet, wie leicht oder schwer eine Verschlüsselung zu knacken ist. Konkret ist die Qualität von folgenden Kriterien abhängig:

Gewähltes Verschlüsselungsverfahren

Die historischen Verschlüsselungsverfahren sind mit den heutigen Kenntnissen relativ leicht zu knacken. Derzeit aktuelle Verfahren können als sicher eingestuft werden.

Gewähltes Verschlüsselungsprogramm

Das konkret verwendete Verschlüsselungsprogramm könnte Programmierfehler oder eine Hintertüre (z. B. ein Generalpasswort zur Entschlüsselung) enthalten. Bei weit verbreiteten Programmen und insbesondere bei weit verbreiteten Opensource-Programmen reduziert sich diese Gefahr.

Gewähltes Passwort

In der Praxis ist es meist so, dass man die Verschlüsselung mit einem Passwort absichert, aus dem der Schlüssel berechnet wird. Die Verschlüsselung kann natürlich nur so gut sein wie das Passwort.

ANGRIFFE AUF DAS PASSWORT

Das verwendete Passwort ist üblicherweise die Schwachstelle einer Verschlüsselung. Deshalb zielen die meisten Angriffe darauf ab, das Passwort herauszufinden.

Brute-Force-Methode

Bei der Brute-Force-Methode werden systematisch alle möglichen Passwörter getestet. Erfolgversprechend ist diese Methode vor allem bei kürzeren Passwörtern (6-8 Zeichen, je nach Aufwand der betrieben wird).

Wörterbuchattacken

Insgesamt erfolgversprechender sind Wörterbuchattacken. Auch wenn viele Benutzer meinen, ihr Passwort wäre einzigartig, findet man in gesammelten Passwortdateien viele davon. Einige Millionen Passwörter sind in kurzer Zeit durchprobiert. Gute Crackprogramme kombinieren diese Passwörter noch mit häufig verwendeten Ergänzungen (z. B. Peter123).

Neben den genannten Angriffsversuchen auf ein Passwort sind natürlich auch Methoden üblich, die das Ziel haben, das Passwort direkt vom Benutzer zu erhalten (z. B. Phishing, Social Engineering, Keylogger)

VERBERGEN VON VERSCHLÜSSELTEN DOKUMENTEN

Dokumente können zwar gut verschlüsselt werden, verschlüsselte Dokumente sind aber als solche leicht erkennbar. Um mögliche Forderungen nach Herausgabe des Passwortes zu umgehen, kann man in einen verschlüsselten Container, der mit einem bestimmten Passwort geöffnet werden kann, einen weiteren sogenannten „Hidden Container" einbauen, der mit einem anderen Passwort zu öffnen, aber nicht erkennbar ist. Das Programm Veracrypt bietet diese Möglichkeit standardmäßig mit an.

SICHERE KOMMUNIKATION

Das Internet stellt eine Infrastruktur für die Kommunikation zwischen zwei Geräten bereit, die für viele Dienste verwendet wird. Die klassischen sind E-Mail, Dateiaustausch oder Surfen im Web. Heute werden auch Telefonie, Video-Konferenzen, Kurznachrichten, Bankgeschäfte und Einkäufe über das Internet abgewickelt. Bei diesen Diensten ist eine sichere und vertrauliche Kommunikation wesentlich.

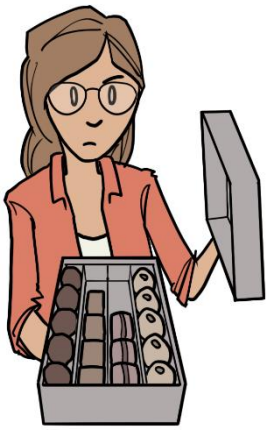
Auch wenn Dokumente im Klartext vorliegen, können sie während der Übertragung im lokalen Netz oder im Internet verschlüsselt werden. Sender und Empfänger vereinbaren einen Key, mit dem sie die Dokumente bei der Übertragung verschlüsseln. Da dieser Key nur dem Sender und dem Empfänger bekannt ist, können die Daten auf diesem Weg auch sicher über das Internet übertragen werden.

Normalerweise geschieht die verschlüsselte Übertragung von Dokumenten automatisch im Hintergrund, so dass Nutzer keinen Einfluss darauf haben.

ZIELE DER SICHEREN KOMMUNIKATION

Authentizität

Vertraulichkeit



Integrität

AUTHENTIZITÄT

Bei jeder Art von Kommunikation möchte man wissen, mit wem man kommuniziert. Im realen Leben ist dies oft indirekt gegeben, ohne dass man sich dessen bewusst ist. Wenn man als Kunde ein Sportgeschäft betritt, sieht man, dass das Geschäft echt ist und nicht einfach ohne Weiteres verschwinden kann. Deshalb hat man ein großes Vertrauen. Wenn man jemanden anruft, weiß man, welche Nummer man gewählt hat und identifiziert den Gesprächspartner gegebenenfalls an der Stimme. Diese „natürliche“ Art der Authentifizierung ist bei der Kommunikation über das Internet nicht gegeben.

Als Mindeststandard in der digitalen Kommunikation hat sich durchgesetzt, dass sich der Server gegenüber dem Client mit einem Zertifikat ausweist. Der Client muss sich ggf. mit Benutzernamen und Passwort ausweisen.

VERTRAULICHKEIT

Nur der rechtmäßige Adressat soll die Nachricht lesen können. Bei der digitalen Kommunikation geschieht dies durch Verschlüsselung, wobei nur die Kommunikationspartner die entsprechenden Schlüssel kennen.

INTEGRITÄT

Wenn eine Nachricht auf dem Kommunikationsweg verfälscht wird, soll dies vom Empfänger erkannt werden.

PRÜFUNG DER AUTHENTIZITÄT

Wenn ein Client die Verbindung zu einem Server aufbaut und diesem Server vertrauliche Informationen übermittelt (z. B. Benutzername und Passwort), sollte er sicher sein, dass er mit dem richtigen Server kommuniziert. Der Server weist sich dazu gegenüber dem Client mit einem Zertifikat aus. Nachfolgend ist am Beispiel einer https-Verbindung dargestellt, wie die Prüfung der Authentizität des Servers erfolgt (Verbindung zu https://alp.dillingen.de).

ÜBERMITTLUNG DES ZERTIFIKATS

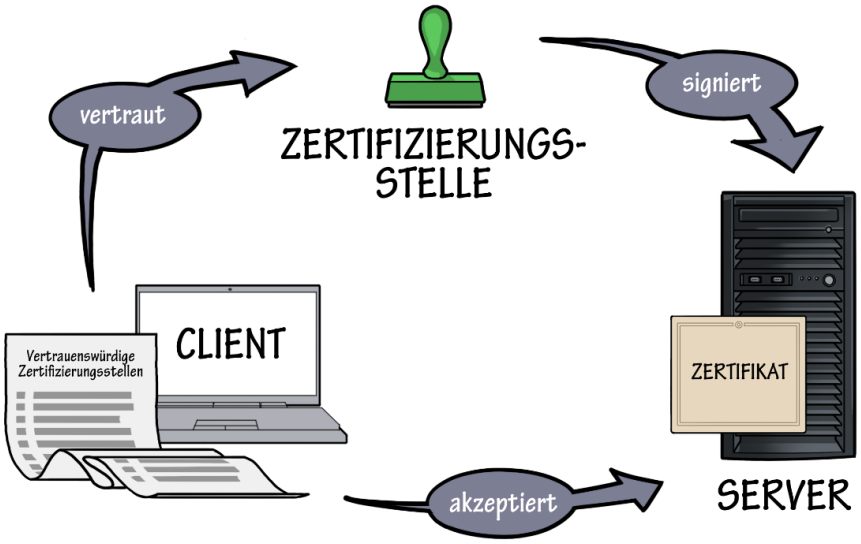
Beim Verbindungsaufbau mit einem Server fordert der Client das Zertifikat der Domäne an (SSL- bzw. TLS-Zertifikat). Jeder Betreiber einer Webseite, der auch https-Verbindungen anbietet, benötigt ein solches Zertifikat.

Das Zertifikat enthält u.a. folgende Informationen:

- allgemeiner Name (Name der Domäne)
- ggfs. Inhaber der Domäne (bei extended validation Zertifikaten)
- öffentlicher Schlüssel des Inhabers der Domäne
- Gültigkeitsdauer des Zertifikats
- Zertifizierungsstelle

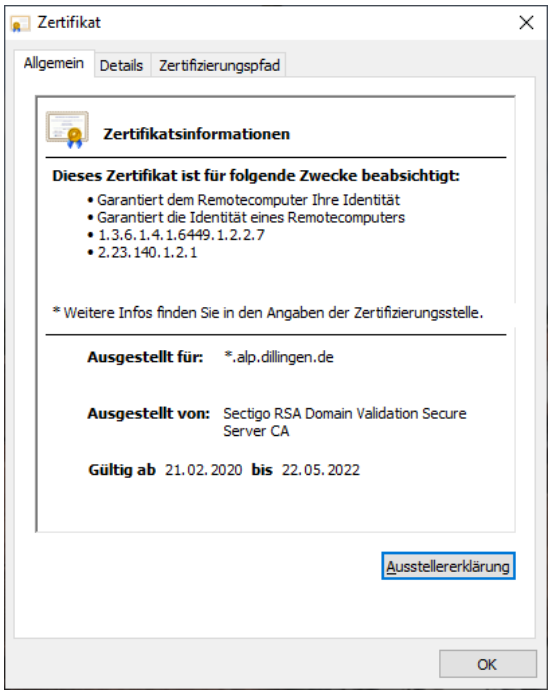
ÜBERPRÜFUNG, OB DAS ZERTIFIKAT ECHT IST

Im Zertifikat ist auch die Zertifizierungsstelle genannt. Der Client überprüft als erstes, ob er dieser Zertifizierungsstelle vertrauen kann. Dazu hat er eine Liste vertrauenswürdiger Zertifizierungsstellen (mit den zugehörigen öffentlichen Schlüsseln) gespeichert. Wenn der Client der Zertifizierungsstelle vertraut und die Zertifizierungsstelle die Echtheit des Zertifikats bestätigt, dann akzeptiert der Client das Zertifikat.



Der Client vertraut der Zertifizierungsstelle, die das Zertifikat des Servers bzw. der Domäne signiert hat. Deshalb akzeptier der Client das Zertifikat.

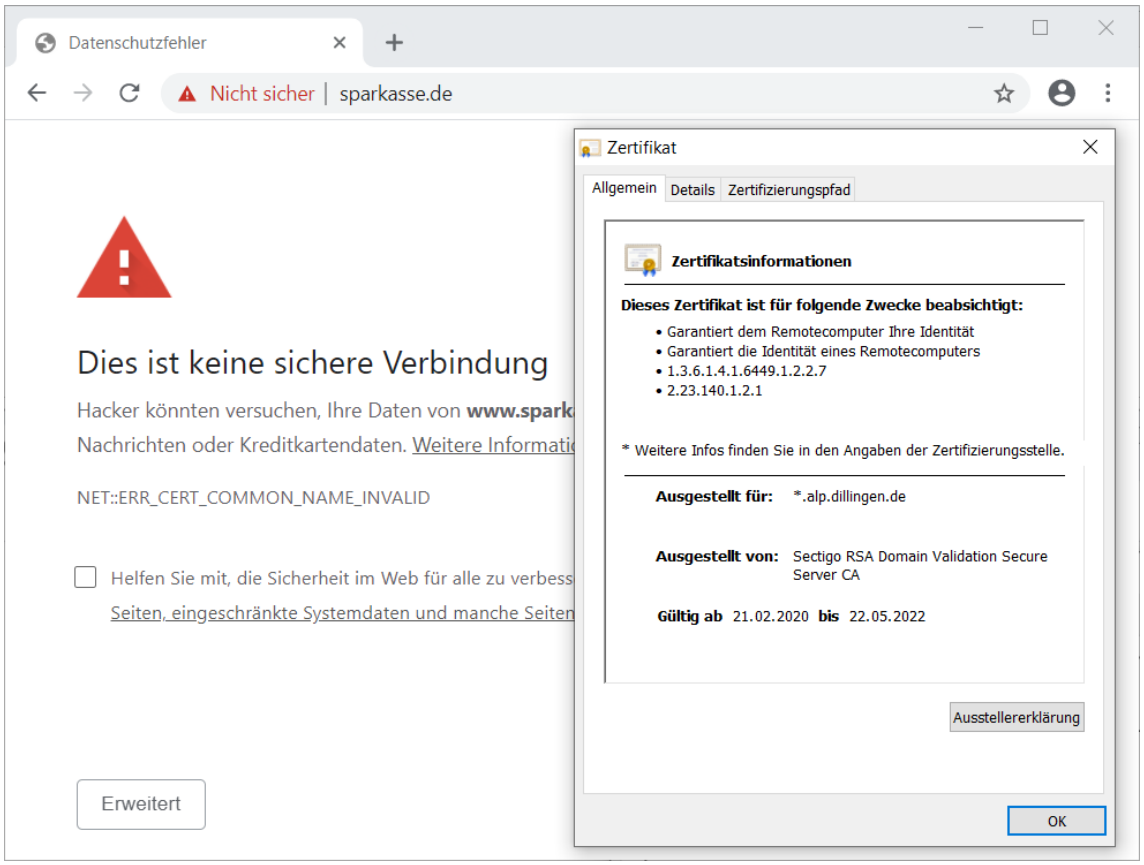
Das Zertifikat kann am Browser eingesehen werden.



Gültiges Zertifikat für *.alp.dillingen.de. Dieses Zertifikat passt zu Verbindungen wie https://alp.dillingen.de, https://schulnetz.alp.dillingen.de oder https://fibs.alp.dillingen.de.

ÜBERPRÜFUNG, OB DAS ZERTIFIKAT ZUR WEBSEITE PASST

Im nächsten Schritt überprüft der Client, ob das Zertifikat zur aufgerufenen Webseite passt. In der nachfolgenden Grafik ist ein Beispiel gezeigt, bei dem das Zertifikat nicht zur Webseite passt. Es wurde die Webseite https://www.sparkasse.de aufgerufen. Das angezeigte Zertifikat ist gültig, gehört aber nicht zur aufgerufenen Seite. Der Browser gibt eine Warnung aus und unterbricht gegebenenfalls die Verbindung.



Das Zertifikat ist echt, passt aber nicht zur aufgerufenen Webseite. Dies könnte ein Phishing-Versuch sein oder ein „Man-in-the-Middle“-Angriff.

ÜBERPRÜFUNG, OB DIE AUFGERUFENE WEBSEITE ZUM RECHTMÄßIGEN INHABER DES ZERTIFIKATS GEHÖRT

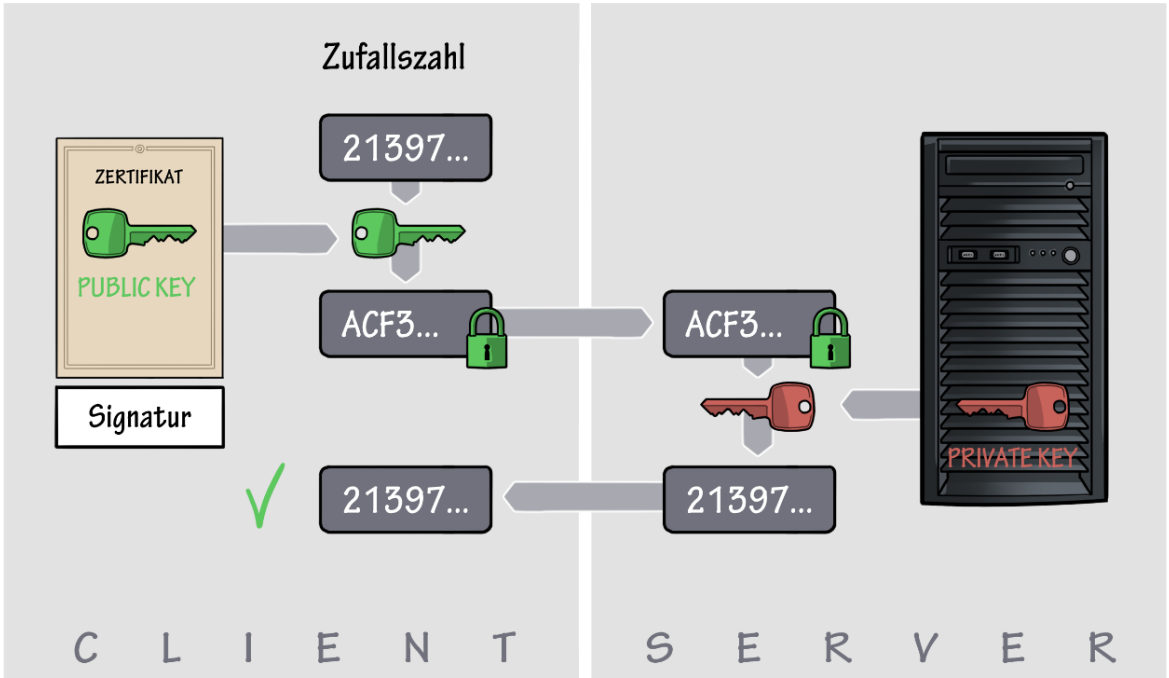
Der Client weiß nun, dass das Zertifikat echt ist und zur angegebenen URL passt. Es könnte aber sein, dass er auf eine gefälschte Webseite umgeleitet wurde und dennoch das (kopierte) Zertifikat der Originalseite präsentiert bekommt.

Vergleichbar ist dies mit dem Vorzeigen eines Führerscheins. Der Führerschein ist echt; aber ist die Person, die ihn vorzeigt auch der rechtmäßige Besitzer des Führerscheins?

Der Führerschein ist echt, aber ist die Person, die ihn vorzeigt auch der rechtmäßige Besitzer?

Der rechtmäßige Inhaber des Zertifikats ist im Besitz des privaten Schlüssels, der zum im Zertifikat gespeicherten öffentlichen Schlüssel gehört. Um zu überprüfen, ob die aufgerufene Webseite auch zum rechtmäßigen Inhaber des Zertifikats gehört, muss der Client überprüfen, ob auf dem Webserver der private Schlüssel hinterlegt ist, der zum Zertifikat passt.

Das Problem dabei ist, dass der private Schlüssel natürlich nicht herausgegeben werden darf. Aber auch dieses Problem lässt sich lösen:



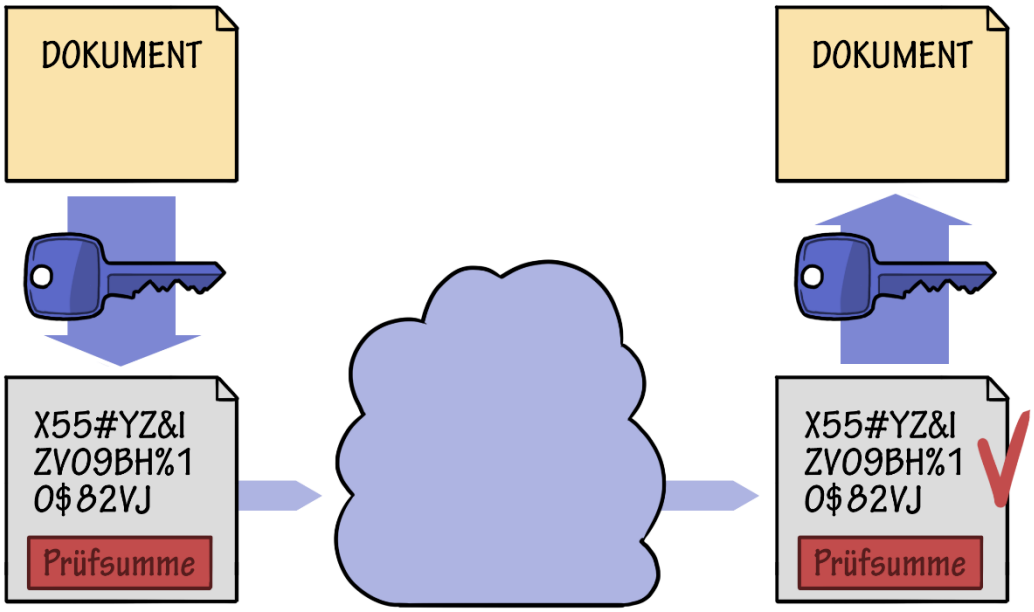
Im Zertifikat ist der öffentliche Schlüssel des Inhabers der Domäne gespeichert. Der Client generiert eine Zufallszahl, verschlüsselt diese mit dem im Zertifikat genannten öffentlichen Schlüssel und sendet das Ergebnis an den Server. Wenn der Server diese Zufallszahl entschlüsseln kann, ist gewährleistet, dass er im Besitz des zugehörigen privaten Schlüssels ist. Damit ist er der rechtmäßige Inhaber des Zertifikats.

Nach Abschluss dieses Verfahrens geht der Client davon aus, dass er mit dem echten Server kommuniziert.

AUFBAU EINER VERSCHLÜSSELTEN VERBINDUNG

Die weitere Kommunikation zwischen Client und Server soll verschlüsselt erfolgen. Der Client hat bereits den öffentlichen Schlüssel des Servers und weiß, dass der Server den zugehörigen privaten Schlüssel hat. Ziel ist jedoch eine symmetrische Ende-zu-Ende-Verschlüsselung zwischen Client und Server mit einem gemeinsamen Schlüssel, den sonst niemand kennt.

Der Client generiert einen solchen symmetrischen Schlüssel, verschlüsselt diesen mit dem öffentlichen Schlüssel des Servers und sendet ihn an den Server. Ab diesem Zeitpunkt erfolgt die Kommunikation zwischen Client und Server verschlüsselt mit dem symmetrischen Schlüssel, den nur die beiden kennen.



Verschlüsselte Übertragung eines Dokuments mit einer symmetrischen Verschlüsselung

PRÜFUNG DER INTEGRITÄT DER ÜBERTRAGENEN DATEN

Um sicher zu gehen, dass die übertragenen Daten unterwegs nicht verfälscht wurden, wird von den zu übertragenden Daten ein Hashwert berechnet, der als kryptographische Prüfsumme mitgeschickt wird. In Verbindung mit der verschlüsselten Übertragung ist gewährleistet, dass eine zufällige oder auch bewusste Veränderung der Daten erkannt wird.

DIE ELEKTRONISCHE UNTERSCHRIFT

Die elektronische Unterschrift oder elektronische Signatur soll ein rechtlich verbindliches Gegenstück zur handschriftlichen Unterschrift sein.

Aus kryptographischer Sicht ist es kein Problem, ein Dokument zu signieren (siehe Kapitel „Digitale Signatur“). Ein praktisches Problem bei der Beweiskraft der Unterschrift ist das Vertrauen in die Identität des Unterzeichners und der Nachweis, dass es tatsächlich der Unterzeichner war, der das Dokument signiert hat. Je nachdem, wie strikt diese Überprüfung durchgeführt wird, trifft man folgende rechtliche Unterscheidungen:

- Einfache elektronische Signatur (ohne Identitätsprüfung)
- Fortgeschrittene elektronische Signatur (mit einfacher Identitätsprüfung z. B. durch Telefon oder Kopie des Personalausweises)
- Qualifizierte elektronische Signatur (mit genauer Identitätsprüfung)

Bei der qualifizierten elektronischen Signatur (QES) soll die gleiche Rechtswirksamkeit wie bei der handschriftlichen Unterschrift gegeben sein. Bei ihr überprüft ein qualifizierter Vertrauensdienste-anbieter, z. B. die Bundesdruckerei, die Identität des Unterzeichners und stellt ein Zertifikat aus.

Vor allem für Privatpersonen ist eine weitere praktische Herausforderung die sichere Aufbewahrung des privaten Schlüssels, mit dem die Unterrschrift erstellt wird. Ein Verlust hätte bei einer rein digitalen Unterschrift zur Folge, dass sich der Unterzeichner nicht mehr als dieser ausweisen könnte. Der Computer zu Hause ist zu unsicher - zumindest, wenn die Signatur rechtsverbindlich sein soll.

Im Folgenden sind zwei konkrete Verfahren dargestellt, wie ein Dokument rechtsverbindlich signiert werden kann:

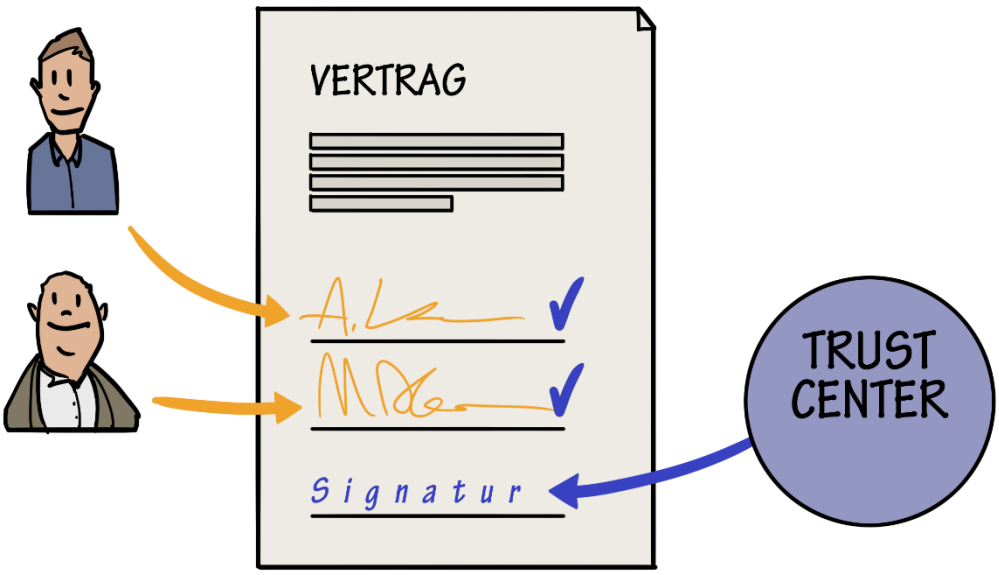
SIGNATUR DURCH EINEN VERTRAUENSWÜRDIGEN DIENSTLEISTER

Insbesondere bei Verträgen wird für die Beglaubigung der elektronischen Unterschrift der Vertrags-partner oft die neutrale Rolle eines Dienstleisters (Trust Center) in Anspruch genommen.

Der Dienstleister prüft die Identität der an einem Vertrag beteiligten Personen. Je nach rechtlicher Bedeutung des Vertrags sind hier unterschiedliche Prüfverfahren üblich, z. B. E-Mail, SMS, Handy, Videokonferenz oder ein Bild des Personalausweises.

Die Vertragspartner bekunden gegenüber dem Dienstleister, dass sie den Vertrag signieren möchten, z. B. durch Versand per E-Mail, durch das Ausfüllen eines entsprechenden Vordrucks oder durch eine Kopie der eigenhändigen Unterschrift auf den Vertrag.

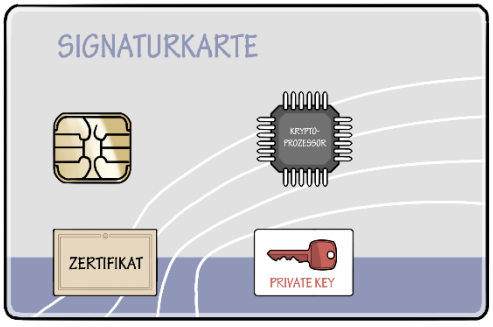
Die eigentliche digitale Signatur erfolgt nicht durch die Vertragspartner, sondern durch den Dienstleister Dieser signiert den Vertrag wie bei der digitalen Signatur beschrieben. Der Dienstleister bestätigt, dass er die Identität der Unterzeichner überprüft hat und dass der Vertrag von den Unterzeichnern anerkannt wurde.



Der Dienstleister (Trust Center) hat die Identität der Vertragspartner und deren Willen, den Vertrag einzugehen überprüft. Dies bestätigt er durch die Signatur.

PERSÖNLICHE SIGNATUR MIT HILFE EINER SIGNATURKARTE

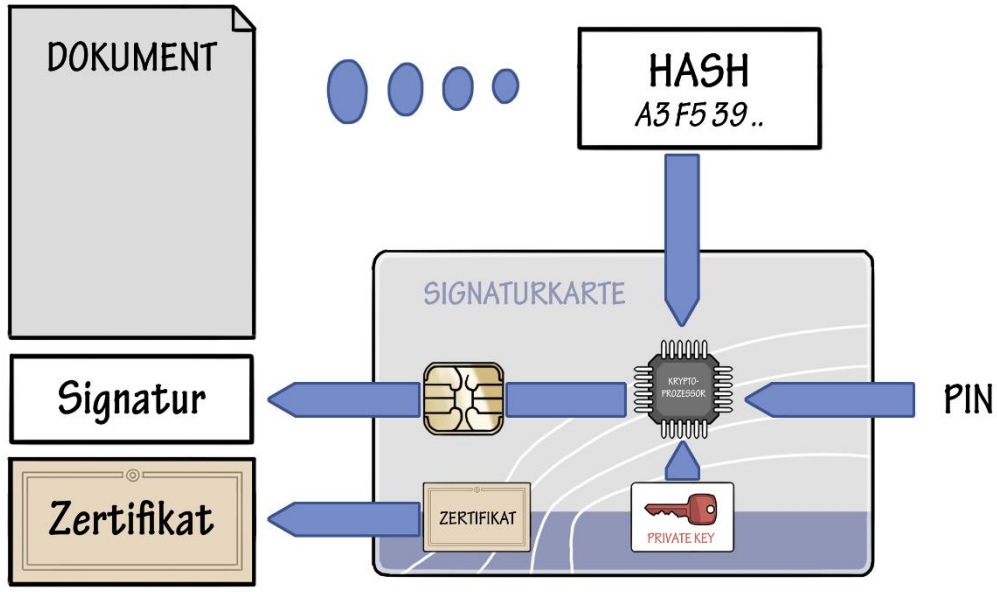
Die Signaturkarte enthält ein Zertifikat der zertifizierenden Organisation (Trust Center, z. B. Bundesdruckerei), den privaten Schlüssel des Karteninhabers (mit PIN gesichert), sowie einen Kryptoprozessor, mit dem alle Verschlüsselungsoperationen durchgeführt werden. Der private Schlüssel verlässt die Karte nie und ist auch nicht auslesbar.



Signaturkarte: Der private Schlüssel muss so geschützt sein, dass er nicht auslesbar ist.

Das zu signierende Dokument wird mit dem privaten Schlüssel signiert. Dazu wird der Hashwert des zu signierenden Dokuments auf die Signaturkarte übertragen und die Signatur berechnet.

Auf der Signaturkarte befindet sich auch ein Zertifikat der ausstellenden Organisation (Trust Center) mit Angaben zum Inhaber der Signaturkarte, zur ausstellenden Organisation, zur Gültigkeit und zum öffentlichen Schlüssel des Karteninhabers. Dieses Zertifikat wird an das signierte Dokument angehängt.



Qualifizierte Elektronische Unterschrift mit Hilfe einer Signaturkarte

Wenn das Dokument auf Echtheit überprüft wird, wird im ersten Schritt die Gültigkeit des Zertifikats überprüft. Mit dem im Zertifikat enthaltenen öffentlichen Schlüssel des Unterzeichners kann die Echtheit des Dokuments bestätigt werden.

Mit der Signaturkarte ist das Problem der sicheren Aufbewahrung des privaten Schlüssels geklärt. Nur wer im Besitz der Signaturkarte und der PIN ist, kann ein Dokument signieren.

Über die Webseite der ausstellenden Organisation kann auch überprüft werden, ob das Zertifikat gegebenenfalls gesperrt wurde, z. B. weil die Signaturkarte verloren ging.

WEITERFÜHRENDE INFORMATIONEN

CrypTool

https://www.cryptool.org/de

CrypTool ist ein Werkzeug zum Erlernen von Grundlagen der Kryptografie. Neben vielen Erklärungen zu historischen Verfahren der Kryptologie sowie Hinweisen zu Schwachstellen bietet es darüber hinaus aber vor allem praktische Demonstrationen, mit denen man die Funktionsweise der Algorithmen gleich ausprobieren kann. Es handelt sich um ein Open-Source-Projekt.

BSI für Bürger – Empfehlungen zur Verschlüsselung

https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Verschluesselung/Verschluesselung_node.html

Empfehlungen des BSI zu Schlüssellängen bei kryptographischen Verfahren:

https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/tr02102_node.html

Selbstlernkurs

Die vorliegende Handreichung ist auch als Selbstlernkurs der Akademie für Lehrerfortbildung und Personalführung verfügbar.