

Kryptologie

Die Anforderungen an die Vertraulichkeit und Integrität von Nachrichten werden immer grösser. Das Verschlüsseln und/oder Signieren von Nachrichten gewährleistet beide Anforderungen. Dieser INFONEWS 2/12 geht unter anderem auf folgende Themen ein:

- Wie funktionieren symmetrische und asymmetrische Verschlüsselung?
- Wie funktionieren moderne Verschlüsselungsverfahren?
- Wie wird eine eigene Certificate Authority betrieben?

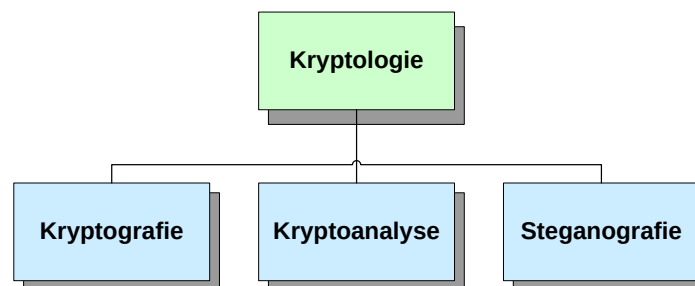
Inhaltsverzeichnis

1	KRYPTOLOGIE	2
1.1	Einleitung	2
1.2	Angriffsarten, Bedrohungen	2
1.3	Sicherheitsanforderungen	3
1.4	Verschlüsselung	3
1.5	Kryptoanalyse	9
1.6	Steganografie	9
2	PUBLIC-KEY-INFRASTRUKTUR	11
2.4	PGP - Web of Trust	11
2.5	X.509	12
2.6	Gesetzliche Vorschriften in der Schweiz	13
2.7	Diffie Hellman	13
3	QUELLEN	14
4	EIGENE CA INSTALLIEREN UND BETREIBEN	15
4.1	CA Rolle installieren	15
4.2	Webserver über HTTPS zugänglich machen	20
4.3	Email-Zertifikat beantragen	23

1 Kryptologie

1.1 Einleitung

Die Kryptologie ist die Wissenschaft der Verschlüsselung und der Entschlüsselung von Informationen.



Die Kryptologie lässt sich wie folgt unterteilen:

- Kryptografie: Verschlüsselung von Informationen
- Kryptoanalyse: Entschlüsselung von Informationen (ohne Kenntnis des Schlüssels)
- Steganografie: Verstecken von Informationen

Nachdem die Kryptologie früher fast ausschliesslich für das Militär eine Rolle spielte, findet sie heute immer mehr Zugang in zivilen Bereichen. Besonders im Internet ist die sichere Übertragung von Informationen, wie z.B. Passwörtern oder Kreditkartennummern, unerlässlich geworden.

Viele Regierungen, darunter Irak, Myanmar, die Volksrepublik China, USA und Frankreich, wollen Verschlüsselung verbieten oder ineffektiv machen. Sie befürchten, Kriminelle oder Regierungskritiker könnten auf diese Weise kommunizieren, ohne dass dies von ihnen kontrol-

liert werden kann. Gegner dieser Massnahmen kritisieren jedoch die damit einhergehende Einschränkung des Grundrechts auf Vertraulichkeit des Wortes, da es - mit Hilfe technischer Massnahmen - für einen Staat heute möglich ist, die gesamte elektronische Kommunikation der Bevölkerung zu überwachen.

1.2 Angriffsarten, Bedrohungen

Die Informationen präsentieren sich in der heutigen Zeit immer mehr in digitaler Form. Die digitale Information ist verschiedenen Angriffen oder Bedrohungen ausgesetzt. Angreifer können unterschiedliche Attacken gegen digitale Informationen ausführen. Die Angriffsmethoden oder Bedrohungen werden in folgende Klassen unterteilt:

- **Abhören** von Nachrichten oder Einsicht in Nachrichten. Personen nehmen Einblick in Informationen oder Nachrichten, obwohl dies vom Verfasser der Nachricht oder der Information unerwünscht oder ungewollt ist.
- **Löschen** (Delete) von Nachrichten oder Teile davon. Informationen, welche aufbewahrt oder gesandt werden sollen, werden vom Verfasser der Nachricht ungewollt oder von einem unberechtigten Dritten vorsätzlich gelöscht.
- **Verändern** von Nachrichten. Hier wird eine Nachricht soweit verändert, dass der Sinn oder Zweck der ursprünglichen Nachricht nicht mehr mit der veränderten übereinstimmt.
- **Bestreiten des Versands** von Nachrichten (Non Repudiation of origin). Hier wird vom Absender einer Nachricht bestritten, die Nachricht versandt zu haben.

- **Bestreiten des Empfangs** von Nachrichten (Non Repudiation of receipt). Hier wird vom Empfänger einer Nachricht bestritten, die Nachricht erhalten zu haben.
- **Einspeisen** von Nachrichten (Insertion). Hier werden von einer Person Nachrichten in die Kommunikation zweier oder mehrerer Teilnehmer eingefügt, welches von diesen Teilnehmern nicht erwünscht oder gewollt ist.
- **Wiederholen** von Nachrichten (Reply). Bei diesem Angriff werden von einer Person bereits versandte Nachrichten noch einmal in die Kommunikation eingespielt. Doch dies ist den Kommunikationsteilnehmern unerwünscht.
- **Vortäuschen** einer anderen Identität (Masquerade). Eine Person gibt sich als eine andere Person aus, um eine andere Person in die Irre zu führen.

1.3 Sicherheitsanforderungen

Die verschiedenen Anforderungen an die Sicherheit der Information werden in verschiedene Sparten aufgeteilt:

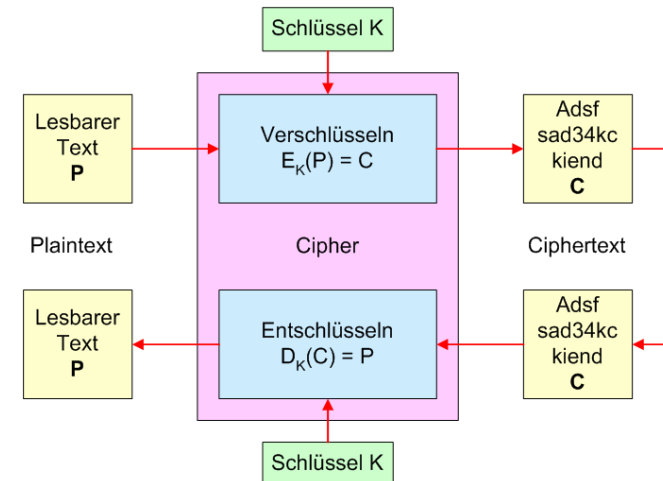
- **Vertraulichkeit**
Mit der Vertraulichkeit soll erreicht werden, dass die Nachricht so übermittelt werden kann, dass niemand Fremdes darauf zugreifen kann.
- **Authentizität**
Mit der Authentizität will erreicht werden, dass der Empfänger einer Nachricht den Absender der Nachricht bestimmen kann.
- **Integrität**
Mit dem Schutz der Integrität einer Nachricht

wird bezweckt, dass nicht gewollte oder unberechtigt verursachte Veränderungen der Nachrichten erkannt werden.

- **Verfügbarkeit**
Mit der Verfügbarkeit ist gemeint, dass die Informationen bei Bedarf zur Verfügung stehen.

1.4 Verschlüsselung

1.4.1 Begriffe

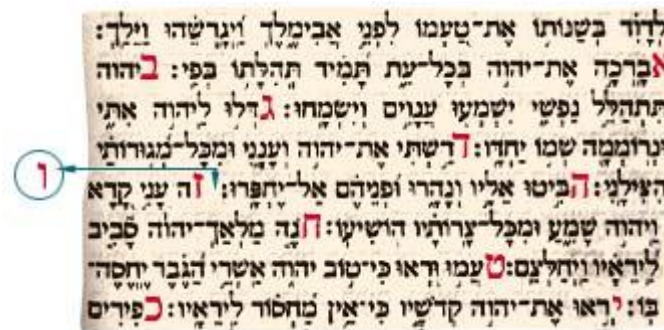


Ein lesbarer Text P wird mit dem Schlüssel K (Key) und der Funktion $E_k(P)$ (E = Encryption) in einen verschlüsselten Text C (Ciphertext) umgewandelt. Die Umkehrfunktion entschlüsselt mit dem identischen Schlüssel K den Ciphertext mit der Funktion $D_k(C)$ (D = Decryption) wieder in den lesbaren Text P .

Wesentliches Merkmal der symmetrischen Verschlüsselung ist also, dass sowohl für die Verschlüsselung wie die Entschlüsselung derselbe Schlüssel K verwendet wird.

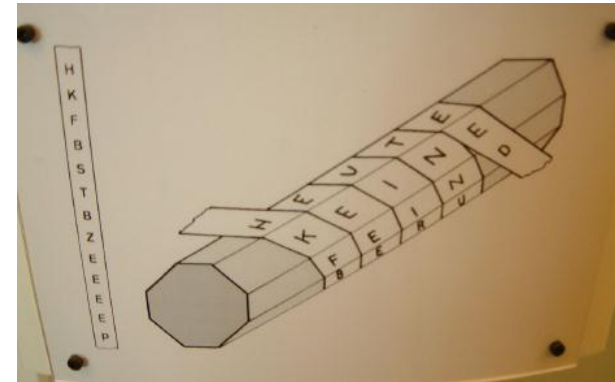
1.4.2 Geschichte

Der früheste Einsatz von Kryptografie findet sich bei dem Einsetzen von unüblichen Hieroglyphen bei den Ägyptern um 1900 v. Chr. Hebräische Gelehrte verwendeten ungefähr 600-500 a. D. einfache Zeichenaustauschalgorithmus (wie beispielsweise die Atbash-Verschlüsselung).



Die Spartaner wickelten einen Papierstreifen auf einen Stab und beschrifteten den Papierstreifen mit einer

Nachricht. Die Empfänger des Papierstreifens konnten die Nachricht nur lesen, falls sie einen gleich dicken Stab verwendeten.



Cäsar verschlüsselte seine Nachrichten, indem er das Alphabet um ein paar Stellen verschob. So wurde z. B. ein A zu einem C, ein B zu einem D usw. (Cäsar-Chiffre).



Im Mittelalter waren in ganz Europa vielfältige Geheimschriften zum Schutz des diplomatischen Briefverkehrs in Gebrauch, so etwa das Alphabetum Kaldeorum.

Sowohl Kryptografie als auch Kryptoanalyse spielen eine Rolle im Babington-Komplot während der Regierungszeit von Königin Elizabeth I. Die Anfänge der mathematischen Kryptografie wurden in dieser Zeit mit der Erzeugung von schlüsselgestützten Zeichenaustauschalgorithmus gemacht.

Ende des 19. Jahrhunderts kam es aufgrund der weiten Verbreitung des Telegrafen (den man auf einfache Weise anzapfen und abhören konnte) zu neuen Überlegungen in der Kryptografie. So wurde von Auguste Kerckhoffs von Nieuwenhof ein Grundsatz (das nach ihm benannte Kerckhoff-Prinzip) formuliert, der besagt, dass die Sicherheit eines kryptographischen Verfahrens allein auf der Geheimhaltung des Schlüssels basieren soll - das Verfahren selbst muss also nicht geheim gehalten werden; im Gegenteil: es kann veröffentlicht und von vielen Experten untersucht werden.

Im Zweiten Weltkrieg wurden mechanische und elektromechanische (T52, SZ42) Kryptographiesysteme zahlreich eingesetzt, auch wenn in Bereichen, wo dies nicht möglich war, weiterhin manuelle Systeme verwendet wurden. In dieser Zeit wurden grosse Fortschritte in der mathematischen Kryptografie gemacht. Notwendigerweise geschah dies jedoch nur im Geheimen.



Die Deutschen machten regen Gebrauch von einem als Enigma bekannten System.

In den Jahren 1974 bis 1976 wurde der DES Algorithmus und das Public Key Kryptographie von W. Diffie und M. Hellman publiziert. Daraus resultierten 1976 das Diffie Hellman Verfahren, 1978 RSA und die 1985 Elliptische Kurven. Es folgten danach 1990 IDEA (Xuejia Lai und James Massey an der ETHZ) und 2000 AES (Advanced Encryption Standard), der Nachfolger von DES.

1.4.3 Techniken der Chiffrierung

Die Techniken der Chiffrierung bestehen grundsätzlich aus:

- **Substitution:** Ersetzen von Buchstaben oder Buchstabenfolgen durch andere Buchstaben oder Buchstabenfolgen.

- **Transposition:** Verändern der Reihenfolge von Buchstaben.
- **Direkte Schlüsseloperationen:** Hier wird direkt eine Operation oder Verknüpfung vom Text mit einem geheimen Schlüssel durchgeführt.

1.4.4 Substitution

Bei der Substitution werden einzelne Buchstaben, resp. Buchstabenfolgen, durch andere Buchstaben, resp. Buchstabenfolgen ersetzt.

MESSAGE FROM MARY STUART KILL THE QUEEN



1.4.5 Transposition

Bei der Transposition wird die Reihenfolge der Buchstaben verändert. Die einzelnen Buchstaben werden dabei aber nicht ersetzt.

MESSAGE FROM MARY STUART KILL THE QUEEN



MOAEE MRQSM TUSAK EARIE GYLNE SLFTT RUH
SMTUE SLGYL NMOAE ARIER UHSAK EFTTE MRQ

Die Nachricht wird von links nach rechts aufgefüllt. Der Schlüssel ist dabei die Anzahl Spalten. Der verschlüsselte Text wird anschliessend von oben nach unten ausgelesen.

Das Auslesen der einzelnen, vier Spalten kann jedoch auch in unterschiedlicher Reihenfolge vorgenommen. Z. Bsp. kann zuerst die Spalte 3, dann 7, 6 usw. ausgelesen werden.

1.4.6 XOR Transformation

Der Ausgang einer XOR-Funktion (von engl. eXclusive OR - exklusives Oder, entweder oder) ergibt genau dann logisch "1" ist, wenn an einer ungeraden Anzahl von Eingängen "1" anliegt und an den restlichen "0". Die XOR-Verknüpfung wird auch als Antivalenz bezeichnet.

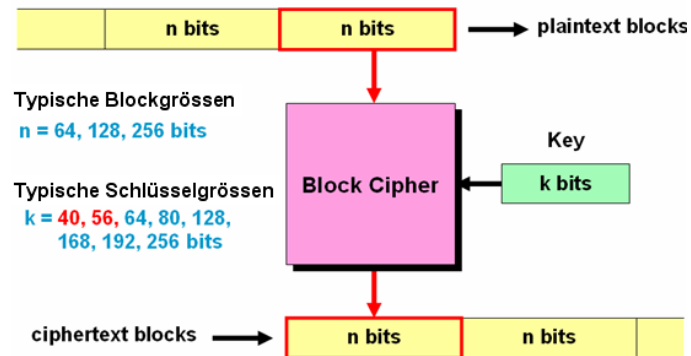
Die folgende Wahrheitstabelle zeigt, wie die XOR-Funktion funktioniert:

Schlüssel	ASCII	Ergebnis aus XOR
1	1	0
1	0	1
0	1	1
0	0	0

Egal welche Spalte fehlt, wenn zwei Spalten vorhanden sind, kann die Dritte immer errechnet werden. So sind beim Sender die Spalten „Schlüssel“ und „ASCII“ bekannt, beim Empfänger aber das „Ergebnis“ und der zuvor definierte „Schlüssel“.

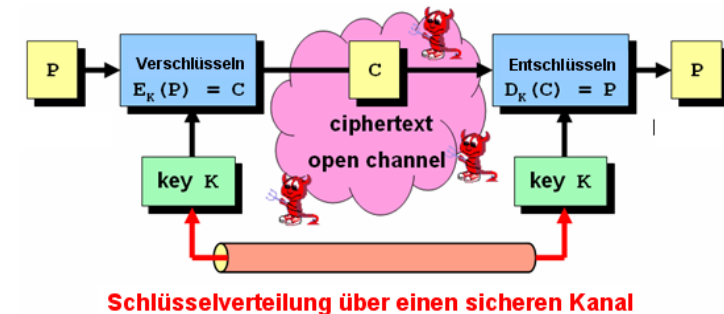
Moderne Algorithmen wie AES, 3DES usw. arbeiten Blockweise. Bei solchen Blockalgorithmen wird der Klartext zum Beispiel in Portionen zu 64 Bit aufgeteilt und aus jeder solchen Portion jeweils ein Geheimtext von 64 Bit Länge

erzeugt. Das entspricht in der Theorie einem Substitutionsalgorithmus, dessen Tabelle 264 Einträge umfasst. Allein die Grösse dieser Zahl verhindert statistische Analysen analog zu den klassischen Verfahren.



In der Praxis konstruiert man oft eine Transformation, in die alle Bits aus dem Klartextblock sowie ein Schlüssel mit eingehen und die sowohl statistische Analyse erschwert als auch kompliziert genug ist, um deterministische Angriffe zu verhindern. Diese Transformation wird mehrfach hintereinander angewandt, jedes Mal mit einem anderen Schlüssel.

1.4.7 Symmetrische Übertragung

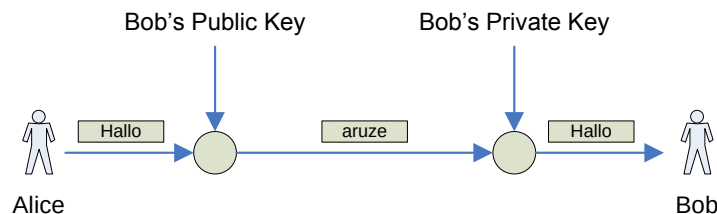


Der grosse Nachteil symmetrischer Verfahren liegt in der Nutzung ein und desselben Schlüssels zur Ver- und Entschlüsselung. Ist der Schlüssel einem Angreifer bekannt, ist es für ihn leicht möglich, an Information zu gelangen und Fehlinformationen durch Veränderung der Originalnachricht zu verbreiten. Ein weiteres typisches Problem beim Einsatz von symmetrischen Verfahren ist, wie der Schlüssel erstmals über unsichere Kanäle zum Gegenüber übertragen werden kann.

Symmetrische Codes (Auszug)

Algorithmus	Blockgrösse	Schlüssellänge
DES (IBM)	64	56
Skipjack (NSA, clipper chip)	64	80
3DES (Triple DES)	64	168
IDEA (Lai / Massey, ETH Zürich)	64	128
CAST (Canada)	64	128
Blowfish (Bruce Schneier)	64	128 ... 448
RC2 (Ron Rivest, RSA)	64	40 ... 1024
RC5 (Ron Rivest, RSA)	64 ... 256	64 ... 256
AES (NIST)	128 ... 256	128 ... 256

1.4.8 Asymmetrische Übertragung



Bei der asymmetrischen Verschlüsselung wird für die Transformation der Information (Verschlüsselung) und die Rücktransformation je ein unterschiedlicher Schlüssel verwendet.

Asymmetrische Codes (Auszug)

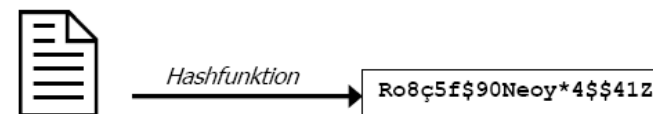
Algorithmus		Schlüssel
RSA	1977 von Rivest, Shamir und Adleman entwickelt.	Variabel
Diffie Hellman	1976 von W. Diffie M. Hellman für den Schlüsselaustausch	Variabel
Elliptische Kurven	1985 von N. Koblitz und V.S. Miller unabhängig voneinander entdeckt.	Variabel

1.4.9 Authentisierwert Methoden

Mit der Authentisierwertmethode sollen die Integrität und die Authentizität von Daten geschützt werden. Die Authentisierwertmethode basiert auf einer Prüfsumme. Es wird eine Hashfunktion eingesetzt.

Ähnlich wie eine Komprimierungssoftware verkleinert eine Hashfunktion beliebig grosse Dokumente und Nachrichten. Eine Hashfunktion reduziert allerdings das Do-

kument auf eine so kleine Grösse, dass das Original-Dokument nicht mehr aus der durch die Hashfunktion resultierende Informationswert hergestellt werden kann. Dieser Informationswert, d.h. das Ergebnis wird Hashwert genannt.



Dokument
z.B. 150 MB gross

Hashwert
z.B. 20 Byte gross

Die Änderung eines einzelnen Bits in einem Dokument sollte 50% der Bits im Hash-Wert ändern!

Wie bei einer Prüfsumme resultieren aus verschiedenen Texten unterschiedliche Werte. Im Unterschied zu einer gewöhnlichen Prüfsumme hat die Hashfunktion folgende wichtigen Eigenschaften:

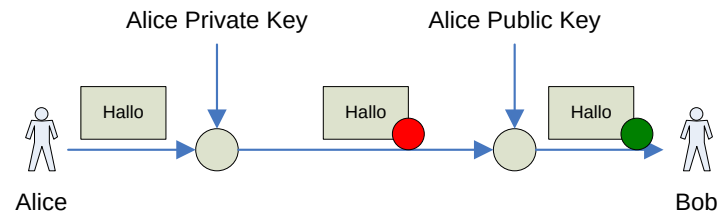
- Bei einem gegebenen Hashwert h lässt sich nur mit grossem Aufwand ein anderer Text T' finden, welcher den gleichen Hashwert h ergibt.
- Es lässt sich nur mit grossem Aufwand zwei verschiedene Texte T und T' generieren, welche den gleichen Hashwert ergeben. Die Hashfunktion arbeitet möglichst kollisionsfrei, d.h. aus zwei verschiedenen Dokumenten resultiert mit grosser Wahrscheinlichkeit immer ein anderer Hashwert; sei der Unterschied der beiden Dokumente noch so klein.

Hash-Funktionen (Auszug)

MD5 Message Digest #5, Ron Rivest, RSA
SHA Secure Hash Algorithm, NIST/NSA

Will man einen zu versendenden Text T vor Veränderung schützen, reicht es nicht aus, einen Hashwert H zu bilden und den an den Text T anzuhängen und dann T und H zu versenden. Denn ein aussenstehender Dritte vermag sowohl den Text T und H zu entfernen und durch einen Text T' und dem dazu passenden Hashwert H' zu ersetzen.

Daher wird der Hash-Wert zusätzlich mit dem privaten Schlüssel verschlüsselt. Diesen Vorgang wird Signierung genannt:



1.4.10 Weitere Schutzmöglichkeiten

Folgende Methoden helfen die immer noch vorhandenen Schwachstellen zu beheben.

- Aktuelles Datum und Systemzeit
- Sequenznummern
- Nachrichtenbestätigung
- Gegenseitige Authentisierung

1.5 Kryptoanalyse

Grundsätzlich wird beim Design und vor allem beim Einsatz eines Chiffrierverfahrens davon ausgegangen,

dass die Angreifer oder Hacker das eingesetzte Verfahren kennen. Man geht aber davon aus, dass sie den Schlüssel nicht kennen. Die Kryptoanalyse teilt die Angriffe auf den Schlüssel oder auf den Klartext.

- **Ciphertext Only**
Manchmal wird diese Methode auch als Known Ciphertext bezeichnet. Der Angreifer kennt einen oder mehrere Geheimtexte und versucht mit deren Hilfe, auf den Klartext beziehungsweise den Schlüssel zu schliessen.
- **Known Plaintext**
Der Angreifer besitzt Geheimtext(e) und die/den zugehörigen Klartext(e). Beide werden benutzt, um den Schlüssel zu ermitteln.
- **Adaptive Chosen Plaintext / Differential Cryptanalysis**
Ähnlich dem vorhergehenden Angriff; der Angreifer hat längere Zeit Zugang zu einem Verschlüsselungssystem und kann sich immer wieder frei gewählte Klartexte verschlüsseln. Insbesondere kann er nach der Analyse des erhaltenen Kryptotextes je nach Ergebnis gezielt einen neuen Klartext zum Verschlüsseln wählen. → Differential Cryptanalysis.
- **Probable Plaintext**
Der Angreifer besitzt Geheimtext und hat Grund zu der Annahme, dass dieser bestimmte Wortgruppen oder markante Wörter enthält, mit denen eine Analyse versucht werden kann.

1.6 Steganografie

Das Wort "Steganografie" kommt aus dem Griechischen und heisst übersetzt "verborgenes Schreiben". Sie wird oft defi-

niert als "die Kunst und Wissenschaft der Kommunikation auf einem Weg, welcher die Existenz der Nachricht verbirgt". Somit ist Sinn und Zweck die "Vertuschung" von Informationen. Die Sicherheit einer geheimen steganografischen Botschaft liegt also darin, dass dem Angreifer die Existenz einer solchen nicht auffällt. Folgende Arten der Steganografie werden in Wikipedia beschrieben:

1.6.1 Technische Steganografie

Dazu zählen die Verwendung von Geheimtinten (beispielsweise Zitronensaft), doppelten Böden oder Briefumschlägen, hohle Absätze und ähnliches, klassische Requisiten von James Bond also. Auch die Verschlüsselung an der Luftschnittstelle des Polizeifunks arbeitet mit technischer Steganografie, hier werden schlicht die verwendeten Frequenzbänder permutiert. Zusätzlich wird der Polizeifunk anders moduliert als die im etwa gleichen Wellenlängenbereich angesiedelten UKW-Rundfunksender, so dass ein Abhören mit einem einfachen Radiogerät erschwert wird. Mit entsprechenden, legal erhältlichen so genannten Funkscannern ist jedoch ein Empfang ohne grössere Schwierigkeiten möglich, wenn auch verboten. Aus älteren Krimis ist der Einsatz von Mikrofilmen bekannt, wobei teilweise auf der Grösse eines Schreibmaschinenpunktes eine A4-Seite versteckt werden kann. Ein solcher Punkt lässt sich dann leicht verstecken. In der Antike wurde ein etwas aufwändigeres Verfahren praktiziert: Einem Sklaven wurde der Kopf geschoren und eine Nachricht auf die Kopfhaut tätowiert. Sobald die Haare wieder nachgewachsen waren, konnte der Sklave zum Empfänger geschickt werden.

1.6.2 Computergestützte Steganografie

Mit der Entwicklung der Computer liessen sich diese Verfahren auch auf die elektronische Übermittlung von Daten anwenden. Neben den analogen Möglichkeiten einer linguistischen Steganografie entwickelten sich aber noch raffiniertere Verfahren, die für diejenigen, die keinen expliziten Verdacht auf eine versteckte Nachricht schöpfen, nahezu unbemerktbar sind.

Als Grundlage hierzu dient das so genannte Datenrauschen. Hierbei handelt es sich um kein wirkliches Rauschen, sondern eher darum, dass auch elektronische Daten einer gewissen unmerklichen Fehlertoleranz unterliegen. Dementsprechend kann man gewisse Datenformen (Audiodateien und Bilder) leicht manipulieren und so seine Daten unterbringen, ohne dass das Gesamtbild bzw. der Ton sich verändert. Nehmen wir beispielsweise an, wir hätten eine beliebige Audiodatei im .WAV-Format. Nach dem einleitenden Header (den man nicht manipulieren sollte, da sonst die Programme nicht mehr in der Lage sind, die Datei richtig einzulesen) sind die Audiodaten - wie nicht anders zu erwarten - in simplen Byteblöcken abgelegt. Ein Byteblock umfasst 8 Bits und kann somit die Zahlen 0-255 darstellen.

Der Trick hierbei ist nun, dass man in jeden Byteblock das letzte Bit (auch LSB genannt => least significant Bit) nach Belieben manipuliert und die zu versteckende Datei so Bit für Bit in das Audio Format unterbringt. Das letzte Bit symbolisiert lediglich 2^0 - entscheidet also beispielsweise, ob eine Zahl 2^{30} oder 2^{31} lautet und verändert so die originale Datei um maximal $1/256$ (oder 0.39%). Das ist ein Unterschied, der in einer Audiodatei nicht hörbar ist.

Entsprechend der oben genannten Methode lassen sich bei reiner Nutzung des LSBs immer Dateien in der Trägerdatei unterbringen, die maximal $1/8$ der Grösse haben, da ein

Byteblock der zu versteckenden Datei auf 8 Byteblöcke der Trägerdatei aufgesplittet wird.

1.6.3 Linguistische Steganografie

Eine Unterklasse der linguistischen Steganografie ist das Semagramm. Dabei werden durch kleine Details in einer an sich unverfänglichen Nachricht, in einem Bild oder einer Zeichnung Informationen übertragen. Beispielsweise können durch die Wahl unterschiedlicher Schriftarten die Zeichen einer geheimen Nachricht im Text maskiert werden. Allerdings sind diese kleinen Unterschiede auch für ein ungeübtes Auge deutlich sichtbar. Immerhin werden Verfahren beschrieben, die etwas weniger auffällig sind, wie beispielsweise die Verwendung von An- oder Abstrichen, kleinen Tintepatzern, scheinbar hängenden Schreibmaschinen-Typen und ähnliches. Neben diesen Textsemagrammen lassen sich auch in Bildern hervorragend Nachrichten verstecken. So könnte die Länge von Grashalmen an einem Bachlauf ein Morsecode sein, die Zahl und Anordnung der Wolken in einer scheinbar von Kinderhand gezeichneten Landschaft für einen Buchstaben stehen. Auch der Versand einer Kiste mit Uhren kann ein Semagramm sein, schliesslich könnte deren Anordnung und Zeigerstellung wichtige Informationen verbergen. In der modernen Computerwelt sind die Tricks nicht mehr so kunstvoll - in einer hochauflösenden Grafikdatei lassen sich sehr einfach grosse Datenmengen unauffällig und unsichtbar verstecken - sofern keine Kompressionsalgorithmen zum Einsatz kommen.

2 Public-Key-Infrastruktur

Einleitung aus Wikipedia, der freien Enzyklopädie.

Als Public Key Infrastruktur (PKI) bezeichnet man in der Kryptologie ein System, welches es ermöglicht, digitale

Zertifikate auszustellen, zu verteilen und zu prüfen. Die innerhalb einer PKI ausgestellten Zertifikate sind meist auf Personen oder Maschinen festgelegt und werden zur Absicherung computergestützter Kommunikation verwendet. Mit solchen Zertifikaten lassen sich beispielsweise die folgenden Aufgaben lösen:

- IPSec
- Verschlüsselte, signierte Emails
- Sicheres Anmelden mittels Smart Cards
- Remote Access Zutritt, usw.

Der zu Grunde liegende Gedanke bei der Anwendung von Zertifikaten ist der folgende: Mit Hilfe eines Public-Key-Verschlüsselungsverfahrens können Nachrichten im Internet signiert und verschlüsselt werden. Das Signieren garantiert, dass die Nachricht in dieser Form wirklich vom angegebenen Absender stammt. Allerdings benötigt man hierzu den Public-Key des Absenders. Dieser könnte z.B. per Email versendet werden. Es stellt sich genau an diesem Punkt aber die Frage, wie man sicher ist, dass es sich tatsächlich um den Schlüssel des Absenders handelt und nicht um eine Fälschung eines Betrügers. Hierzu kann der zu verschickende Schlüssel selbst wieder mit einem vertrauenswürdigen Schlüssel signiert sein. Auf diese Weise lässt sich eine Hierarchie aus vertrauenswürdigen Institutionen aufbauen. Auf die Echtheit der Schlüssel der obersten Institutionen dieser Hierarchie muss man sich aber verlassen können.

2.4 PGP - Web of Trust

Die Frage jeder Verschlüsselung bezieht sich auf die Vertrauensstellung. Mit wem können Nachrichten ausgetauscht werden? Wie garantiere ich, dass die Gegenseite wirklich die Person ist, als die sie sich ausgibt? Eine Möglichkeit ist das weit verbreitete PGP (Pretty Good Privacy).

INFONEWS

infonews.ch

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

www.goSecurity.ch
Mit Sicherheit an der richtigen Adresse.

Phil Zimmermann schrieb die erste Version 1991. Sein Ziel war es, dass andere Atomkraftgegner sicher Nachrichten und Daten speichern konnten. PGP durfte in seinen Anfangsjahren nicht aus den USA exportiert werden, da es unter das US-Waffengesetz fiel. Danach unterliegen Kryptosysteme mit Schlüsseln von mehr als 40 Bit Länge den Exportbestimmungen. PGP lag mit 128 Bit weitaus höher. Durch die Verbreitung im Internet wurde Phil Zimmermann Ziel von Untersuchungen wegen unerlaubter Waffenexporte. Mitte der 90er Jahre liberalisierten die USA diese Gesetze.

Um die Exportbeschränkung zu umgehen, wurde die Version 5 als Quellcode in Form eines Buches aus den USA legal exportiert und von einigen Freiwilligen per Hand eingescannt. Aus dem gescannten Programmcode wurde dann eine international verfügbare Version von PGP (PGPi) kompiliert.

PGP ist Plattformübergreifend, das heisst, es gibt Versionen für DOS, Windows (ab 95), MacOS und fast alle UNIX-Derivate. Ebenfalls ist PGP leicht portierbar, da PGP in C geschrieben ist. Daher ist PGP auch weltweit verfügbar. PGP wurde verschiedenen Tests unterzogen, diese wurden alle bestanden. Da PGP weder durch staatliche Institutionen noch durch Standardisierungsgremien entwickelt und kontrolliert wird, existieren sehr viele Anwendungsformen.

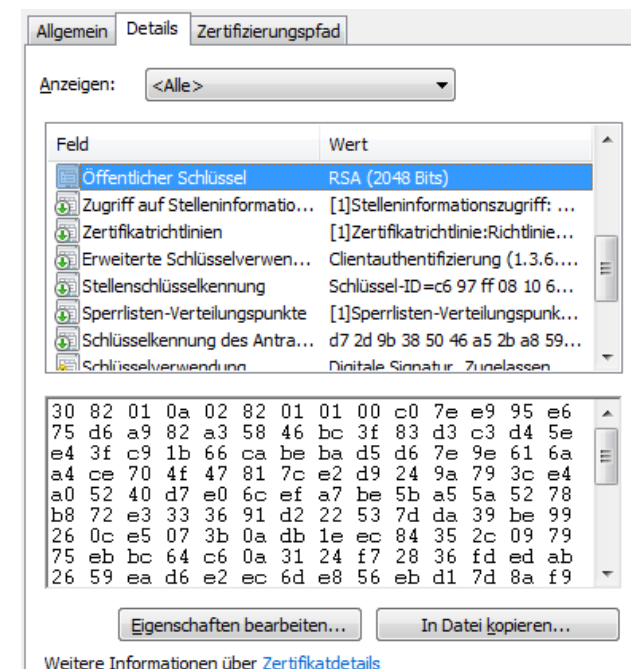
PGP verwendet für die Verschlüsselung und die digitale Signatur die folgenden Algorithmen:

Dienst	Algorithmen
Nachrichtenverschlüsselung	CAST-128, IDEA, 3DES, DH, RSA
Digitale Signatur	DSS/SHA oder RSA/SHA

Kompression	ZIP
Email-Kompatibilität	Radix-64 Konversion

2.5 X.509

Bei X.509 werden Zertifikate von einer Zertifizierungsstelle ausgegeben. Ein digitales Zertifikat entspricht etwa dem Personalausweis und dient dazu, einen bestimmten öffentlichen Schlüssel einer Person oder Organisation zuzuordnen. Diese Zuordnung wird von der Zertifizierungsstelle beglaubigt, indem sie sie mit ihrer eigenen digitalen Unterschrift versieht.



Die Zertifikate enthalten „Schlüssel“ und Zusatzinformationen, die zur Authentifizierung sowie zur Verschlüsselung und Entschlüsselung sensibler oder vertraulicher Daten dienen, die über das Internet und andere Netze verbreitet werden. Als Zusatzinformationen sind zum Beispiel Lebensdauer, Verweise auf Zertifikatssperrlisten, etc. enthalten, die durch die Zertifizierungsstelle mit in das Zertifikat eingebracht werden.

Die Aufgabe einer Beglaubigungsinstitution ist es, solche digitalen Zertifikate herauszugeben und zu überprüfen. Sie ist dabei für die Bereitstellung, Zuweisung und Integritätssicherung der von ihr ausgegebenen Zertifikate verantwortlich. Damit ist sie ein wichtiger Teil der Public-Key-Infrastruktur.

In dem meisten Betriebssystemen und Internet-Browsern sind die wichtigsten Zertifizierungsstellen bereits hinterlegt.

2.6 Gesetzliche Vorschriften in der Schweiz

Seit 1. Januar 2005 werden elektronische Signaturen der handschriftlichen Unterschrift gleichgestellt. Der Bundesrat hat die ausführende Verordnung zum Bundesgesetz über die elektronische Signatur verabschiedet.

Das Parlament hat am 19. Dezember 2003 das Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (Bundesgesetz über die elektronische Signatur, ZertES) verabschiedet. Dieses definiert die Bedingungen, unter denen Anbieterinnen von Zertifizierungsdiensten auf freiwilliger Basis anerkannt werden können, und regelt ihre Tätigkeiten im Bereich der elektronischen Zertifikate. Es legt zudem die Voraussetzungen fest, die eine elektronische Signatur erfüllen

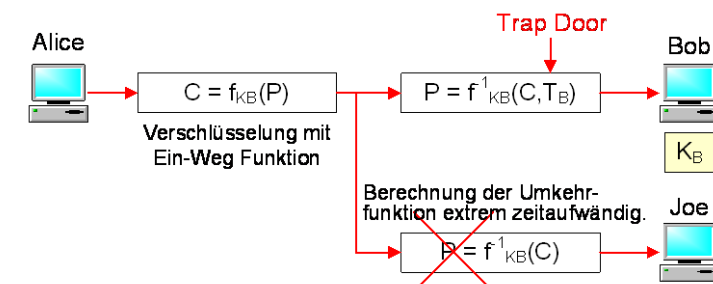
muss, um die gleichen Wirkungen wie eine handschriftliche Unterschrift erzielen zu können. Ausserdem regelt es die Frage der Verantwortung der Anbieterinnen von Zertifizierungsdiensten, der Anerkennungsstellen und der Inhaberinnen und Inhaber von Signaturschlüsseln.

Gleichzeitig hat der Bund die Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur (Verordnung über die elektronische Signatur, VZertES) verabschiedet. Diese Verordnung hebt das vom Bundesrat im Jahr 2000 versuchsweise eingeführte Zertifizierungssystem auf. Sie konkretisiert insbesondere die Verpflichtungen, die anerkannten Anbieterinnen von Zertifizierungsdiensten auferlegt werden, und erteilt dem BAKOM den Auftrag, die nötigen technischen und administrativen Vorschriften zu erlassen.

Die neuen gesetzlichen Bestimmungen sind mit der geltenden Regelung der Europäischen Union kompatibel.

Eine erste Anwendung ist die SuisseID, die den elektronischen Verkehr mit den Bundesstellen vereinfachen soll.

2.7 Diffie Hellman



Der Algorithmus wurde von Martin Hellman gemeinsam mit Whitfield Diffie und Ralph Merkle an der Universität von Stanford (Kalifornien) entwickelt und 1976 veröffentlicht.

INFONEWS

infonews.ch

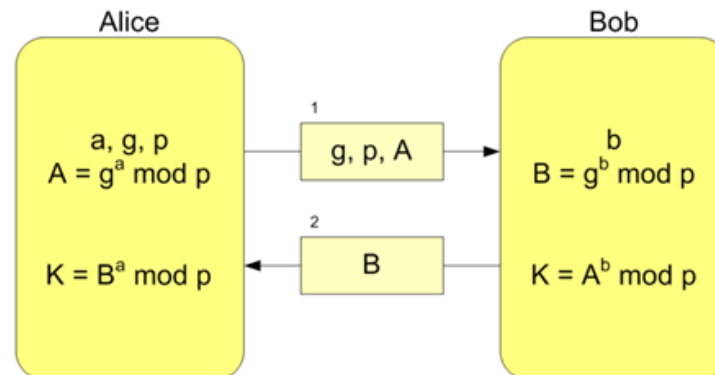
GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

www.goSecurity.ch
Mit Sicherheit an der richtigen Adresse.

Beim Diffie-Hellman-Schlüsselaustausch senden sich beide Kommunikationspartner über einen unsicheren Kanal jeweils eine Nachricht zu. Das Problem, aus diesen beiden Nachrichten den geheimen Schlüssel zu berechnen, wird als Diffie-Hellman-Problem bezeichnet. Von diesem nimmt man an, dass es praktisch nicht lösbar ist. Deshalb kann jemand, der beide Nachrichten mithört, daraus im Allgemeinen nicht den geheimen Schlüssel berechnen.

Zwei Kommunikationspartner (Alice und Bob) wollen über ein unsicheres Medium verschlüsselt kommunizieren. Sie wollen ein symmetrisches Kryptosystem einsetzen. Dazu benötigen beide jedoch zunächst einen Schlüssel, den sie über den Diffie-Hellman-Schlüsselaustausch vereinbaren.



Die Werte a , b , g und p sind dabei Primzahlen. Mit mod wird der Restwert einer Division berechnet.

Beispiel aus Wikipedia

Das Beispiel benutzt sehr kleine Primzahlen. In der tatsächlichen Anwendung werden Zahlen mit mehreren Hundert Dezimalstellen benutzt.

1. Alice und Bob einigen sich auf $p = 13$ und $g = 2$.
2. Alice wählt die Zufallszahl $a = 5$. Bob wählt die Zufallszahl $b = 7$.
3. Alice berechnet $A = 2^5 \mod 13 = 6$ und sendet dieses Ergebnis an Bob.
4. Bob berechnet $B = 2^7 \mod 13 = 11$ und sendet dieses Ergebnis an Alice.
5. Alice berechnet $K = 11^5 \mod 13 = 7$.
6. Bob berechnet $K = 6^7 \mod 13 = 7$.
7. Beide erhalten das gleiche Ergebnis $K = 7$.

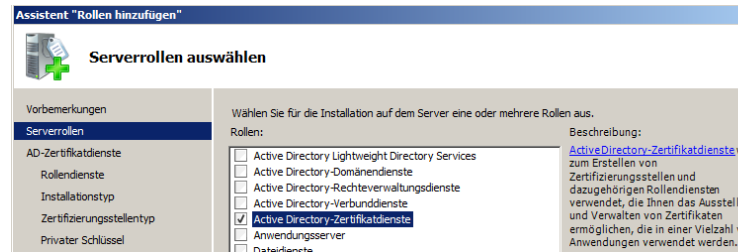
Ein eventuell vorhandener Lauscher könnte zwar die Zahlen 13, 2, 6 und 11 mithören, das eigentliche gemeinsame Geheimnis von Alice und Bob $K = 7$ bleibt ihm aber verborgen.

3 Quellen

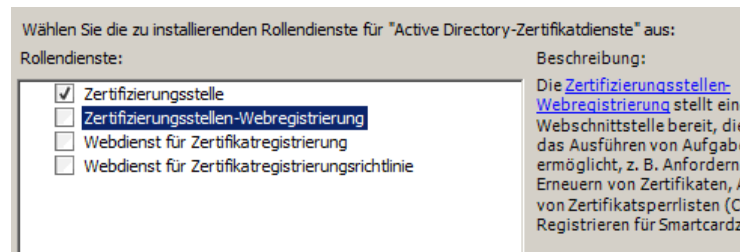
Ein grosser Dank gilt an dieser Stelle meinem Dozenten Andreas Steffen (ZHW, z.Z. Hochschule Rapperswil) und meinem Kollegen Michael Achermann (Hochschule Luzern, z.Z. Klubschule Business).

4 Eigene CA installieren und betreiben

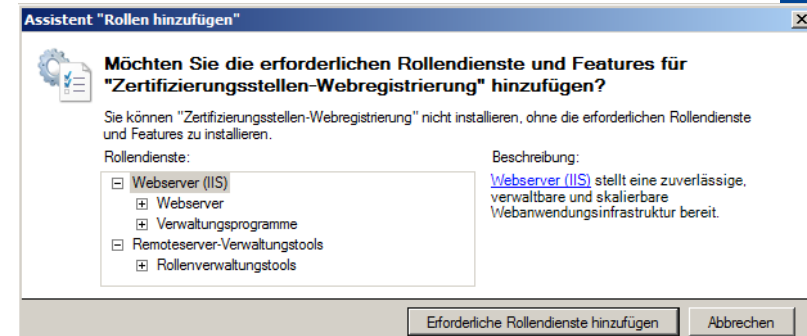
4.1 CA Rolle installieren



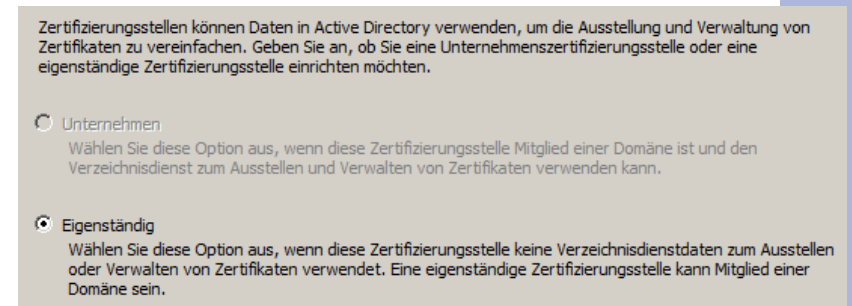
Auch wenn Active Directory Zertifikatdienste steht, kann diese Rolle alleine, d.h. ohne Domäne installiert werden. Die Unterschiede sind, dass Zertifikate vom Client nicht automatisch erstellt werden können. Weiter stehen nicht alle Möglichkeiten für Zertifikate zur Verfügung.



Für die Zertifizierungsstellen-Webregistrierung werden die Rolle IIS mit den folgenden IIS-Modulen benötigt:



Da wir für dieses Beispiel keine Domäne haben, kann nur „Eigenständig“ ausgewählt werden:



Wir installieren eine neue CA, daher wählen wir den ersten Punkt. Es ist auch möglich, eine Unter-CA zu erstellen. Dies wird oft im Internet für verschiedene Schutzstufen von Zertifikaten gemacht.

Sie können eine Kombination aus Stammzertifizierungsstellen und untergeordneten Zertifizierungsstellen konfigurieren, um eine hierarchische Public Key-Infrastruktur (PKI) zu erstellen. Eine Stammzertifizierungsstelle ist eine Zertifizierungsstelle, die eigene selbstsignierte Zertifikate ausstellt. Eine untergeordnete Zertifizierungsstelle empfängt Zertifikate von einer anderen Zertifizierungsstelle. Geben Sie an, ob Sie eine Stammzertifizierungsstelle oder eine untergeordnete Zertifizierungsstelle einrichten möchten.

- ☒ Stammzertifizierungsstelle
Wählen Sie diese Option aus, wenn Sie die erste oder einzige Zertifizierungsstelle in einer Public Key-Infrastruktur installieren.
- ☐ Untergeordnete Zertifizierungsstelle
Wählen Sie diese Option aus, wenn die Zertifizierungsstelle das Zertifizierungsstellenzertifikat von einer anderen übergeordneten Zertifizierungsstelle in einer Public Key-Infrastruktur erhält.

Wir erstellen einen neuen Schlüssel:

Die Zertifizierungsstelle benötigt einen privaten Schlüssel, um Zertifikate für Clients zu generieren und auszustellen. Geben Sie an, ob Sie einen neuen privaten Schlüssel erstellen oder einen vorhandenen Schlüssel verwenden möchten.

- ☒ Neuen privaten Schlüssel erstellen
Verwenden Sie diese Option, wenn Sie keinen privaten Schlüssel besitzen oder einen neuen privaten Schlüssel erstellen möchten, um die Sicherheit zu erhöhen. Sie werden aufgefordert, für den privaten Schlüssel einen Kryptografiedienstleister auszuwählen und eine Schlüssellänge anzugeben. Zum Ausstellen neuer Zertifikate müssen Sie zudem einen Hashalgorithmus auswählen.
- ☐ Vorhandenen privaten Schlüssel verwenden
Verwenden Sie diese Option, um beim erneuten Installieren einer Zertifizierungsstelle zuvor ausgestellte Zertifikate weiterverwenden zu können, um die Kontinuität zu gewährleisten.
- ☐ Zertifikat auswählen und dazugehörigen privaten Schlüssel verwenden
Wählen Sie diese Option aus, wenn auf diesem Computer ein Zertifikat vorhanden ist oder wenn Sie ein Zertifikat importieren und den dazugehörigen privaten Schlüssel verwenden möchten.
- ☐ Vorhandenen privaten Schlüssel auf diesem Computer auswählen
Wählen Sie diese Option aus, wenn Sie private Schlüssel von einer vorherigen Installation beibehalten haben oder einen privaten Schlüssel aus einer anderen Quelle verwenden möchten.

Die von Windows vorgeschlagenen Optionen für den Schlüssel sind als absolutes Minimum anzusehen:

Zum Erstellen eines neuen privaten Schlüssels müssen Sie zunächst einen [Kryptografiedienstleister](#), einen [Hashalgorithmus](#) und eine Schlüssellänge auswählen, die für den beabsichtigten Zweck der von Ihnen ausgestellten Zertifikate geeignet sind. Ein höherer Wert für die Schlüssellänge verstärkt die Sicherheit, erhöht aber auch den Zeitaufwand zum Abschließen von Signaturvorgängen.

Wählen Sie einen Kryptografiedienstleister (CSP) aus: Schlüsselzeichenlänge:

Wählen Sie den Hashalgorithmus zum Signieren von Zertifikaten aus, die von dieser Zertifizierungsstelle ausgestellt werden:

SHA384
SHA512
SHA1
MD5

☐ Administratorinteraktion bei jedem Zertifizierungsstellenzugriff auf den privaten Schlüssel zulassen

Als Zertifizierungsstellenname wird der Rechnername verwendet. Dieser kann anschliessend nicht mehr geändert werden (d.h. es muss zuerst die Rolle CA deinstalliert werden, bevor der Rechnername geändert werden kann).

Geben Sie einen allgemeinen Namen zur Identifizierung der Zertifizierungsstelle an. Dieser Name wird allen von der Zertifizierungsstelle ausgestellten Zertifikaten hinzugefügt. Die Werte für das DN-Suffix werden automatisch generiert, können jedoch geändert werden.

Allgemeiner Name dieser Zertifizierungsstelle:

Je nach Qualität des Schlüssels, kann die Dauer auch länger als 5 Jahre gewählt werden.

Ein Zertifikat wird an diese Zertifizierungsstelle ausgestellt, um die Kommunikation mit anderen Zertifizierungsstellen und mit Clients, die Zertifikate anfordern, zu sichern. Die Gültigkeitsdauer eines Zertifizierungsstellenzertifikats kann von einer Reihe von Faktoren abhängen, beispielsweise dem beabsichtigten Zweck der Zertifizierungsstelle und den Sicherheitsmaßnahmen, die Sie zum Schutz dieser Zertifizierungsstelle getroffen haben.

Wählen Sie die Gültigkeitsdauer für das für diese Zertifizierungsstelle generierte Zertifikat aus:
 Jahre

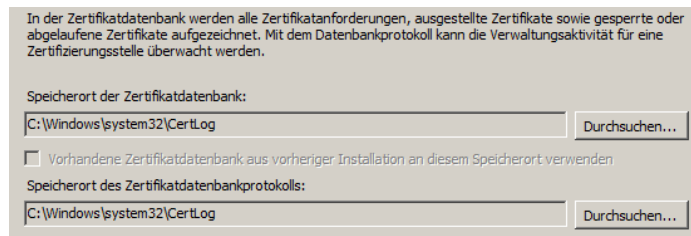
Ablaufdatum der Zertifizierungsstelle: 13.01.2017 17:12

Beachten Sie, dass die von der Zertifizierungsstelle ausgestellten Zertifikate nur bis zu diesem Ablaufdatum gültig sind.

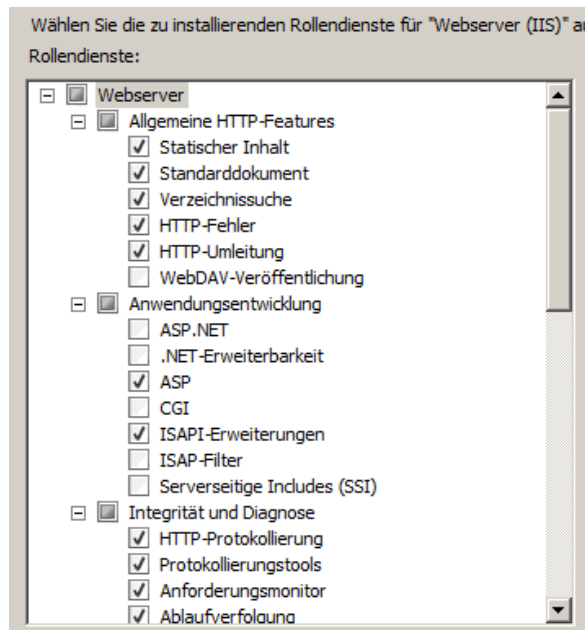
GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

Die Datenbank und die Logs werden am Standardort installiert:

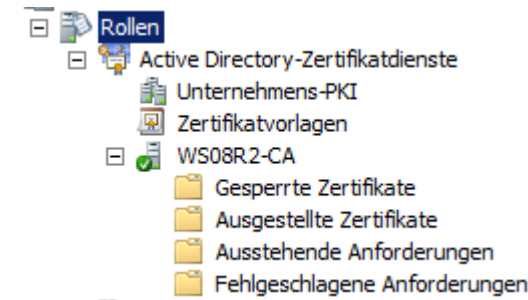


Die Optionen für den Webserver IIS können unverändert übernommen werden:

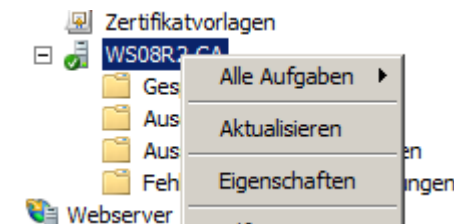


Danach ist die Installation bereit.

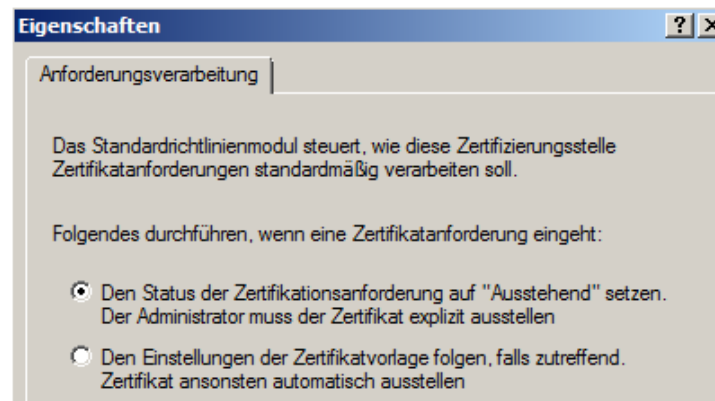
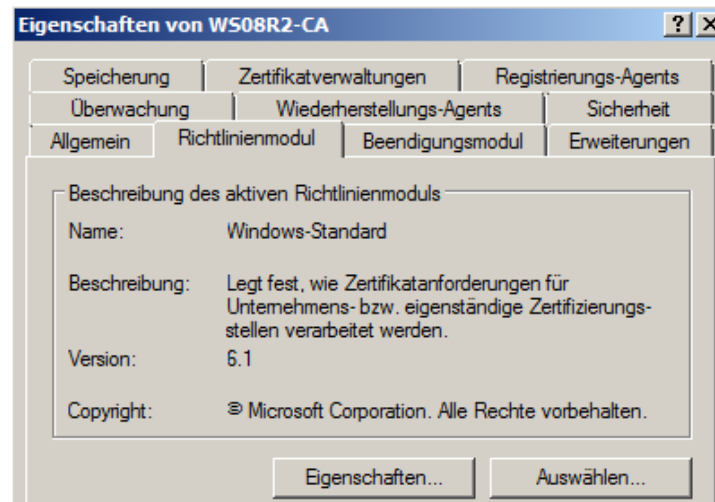
4.1.1 Konfiguration der CA



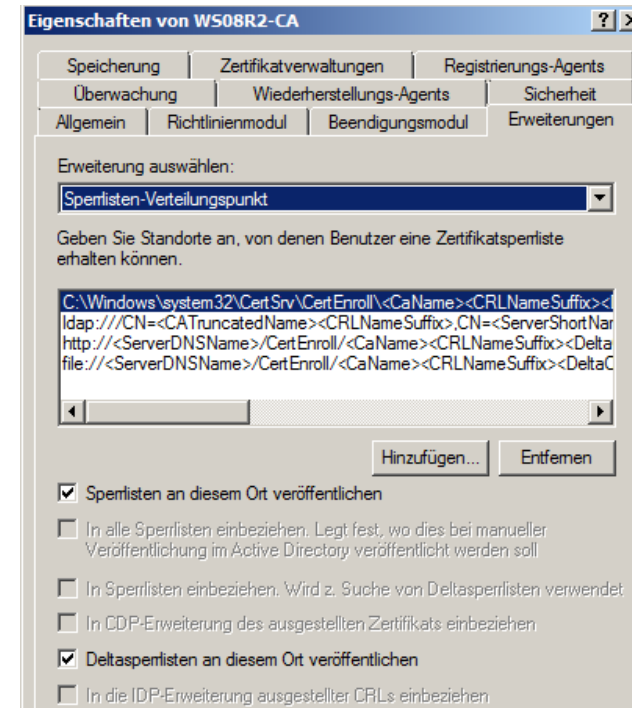
Die Eigenschaften können mit einem Rechtsklick auf den CA-Namen konfiguriert werden:



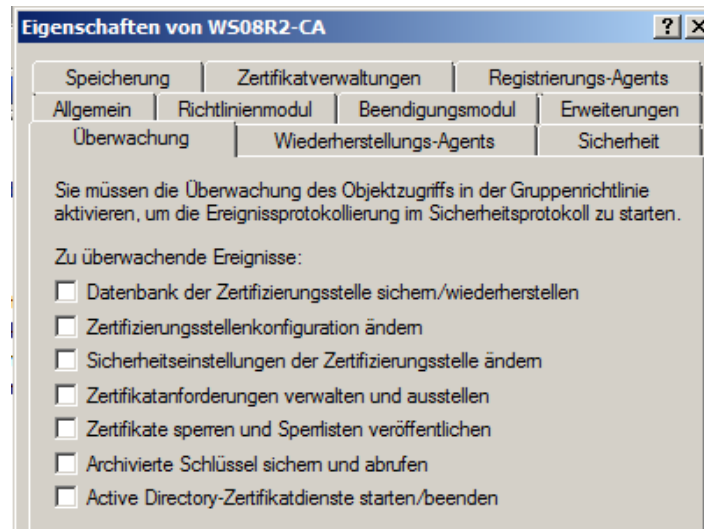
Unter Richtlinienmodul – Eigenschaften wird das automatische Freigeben von Zertifikatsanfragen konfiguriert:



Zu konfigurieren sind noch die Erweiterungen. Die nicht angebotenen Punkte sind zu entfernen, die angebotenen korrekt zu konfigurieren. Diese Angaben sind im Zertifikat enthalten!

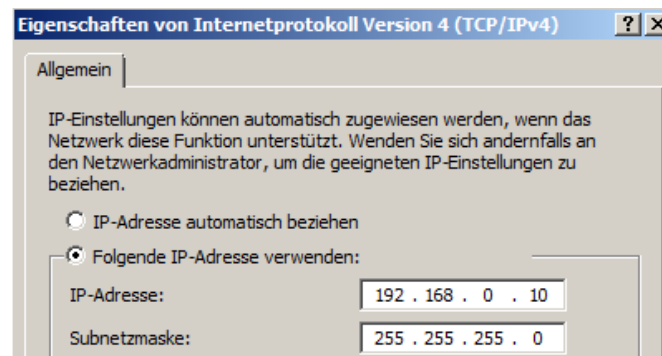


Weiter können die überwachten Elemente konfiguriert werden:

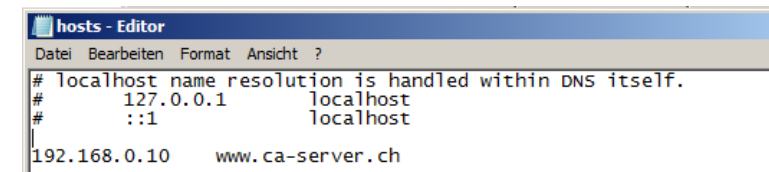


4.1.2 Webserver konfigurieren

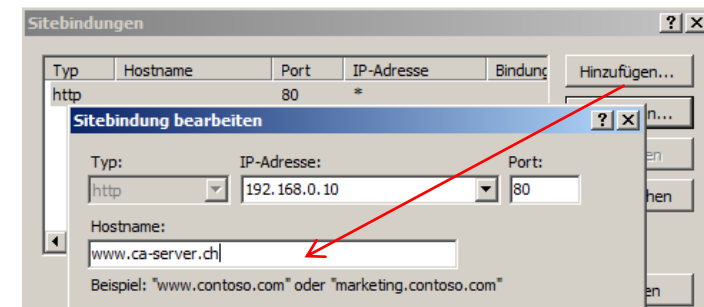
Bevor die CA unter Windows Server 2008 korrekt funktioniert, müssen wir diese via HTTPS erreichbar machen. Zuerst konfigurieren wir eine fixe IP-Adresse für den Server:



Nun definieren wir in der Hosts-Datei (c:\windows\system32\drivers\etc) einen Domainnamen und verweisen auf die soeben eingestellte IP-Adresse.



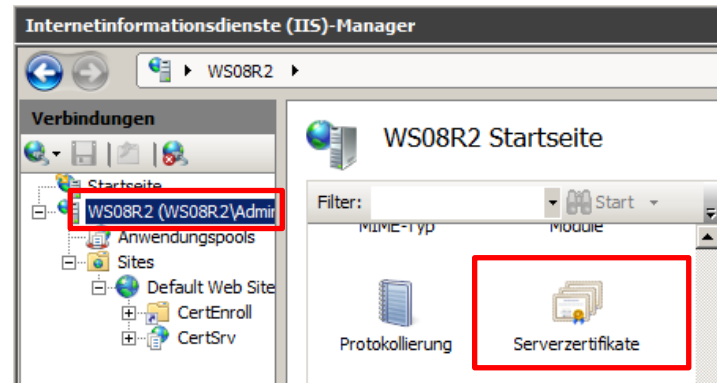
Im IIS erstellen passen wir die Bindung an:



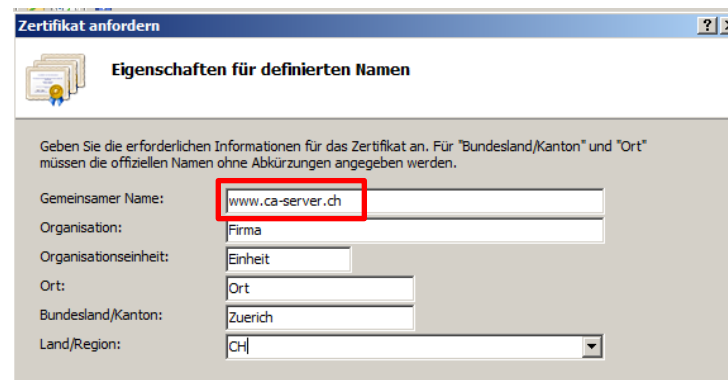
Ab sofort ist die Webseite auch über den Domainnamen erreichbar.

4.2 Webserver über HTTPS zugänglich machen

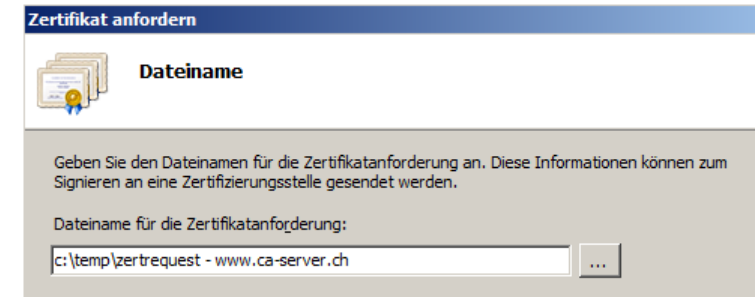
Im IIS erstellen wir einen Antrag für ein SSL Zertifikat:



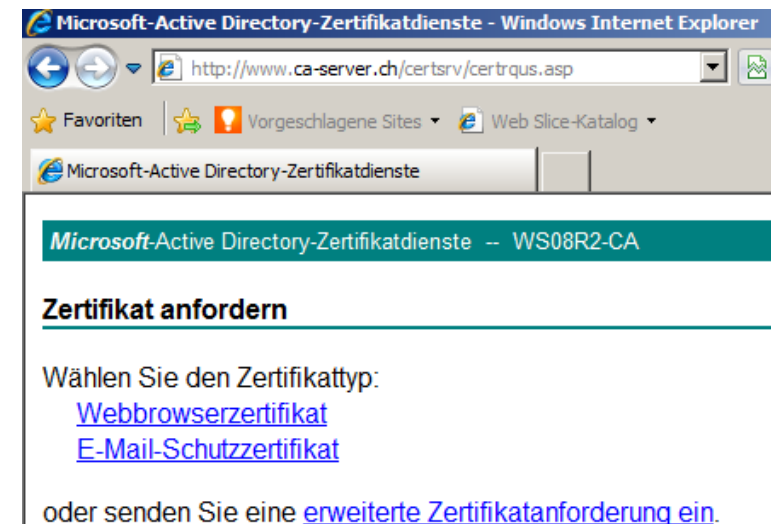
Und füllen die Felder entsprechend aus. Der erste Eintrag ist der Domainname und darf nicht falsch geschrieben werden!



Und den Request entsprechend abspeichern:



Nun fordern wir unter <http://www.ca-server.ch/certsrv/> und dem Menüpunkt „Ein Zertifikat anfordern“ unser Zertifikat an. Wir stellen eine „erweiterte Anforderung“ (zweiter Schritt).



GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

INFONEWS

infonews.ch

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

www.goSecurity.ch
Mit Sicherheit an der richtigen Adresse.

Microsoft Active Directory-Zertifikatdienste -- WS08R2-CA

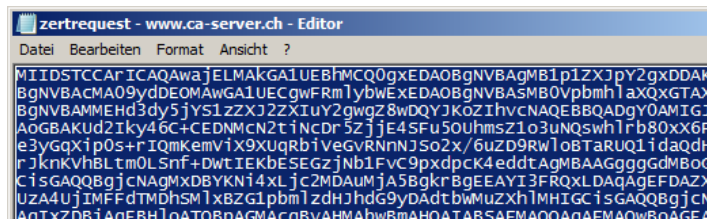
Erweiterte Zertifikatanforderung

Die Richtlinie der Zertifizierungsstelle legt fest, welche Zertifikattypen angefordert werden können. K auf ein der folgenden Optionen:

[Eine Anforderung an diese Zertifizierungsstelle erstellen und einreichen](#)

[Reichen Sie eine Zertifikatanforderung ein, die eine Base64-codierte CMD- oder PKCS10-Dat verwendet, oder eine Erneuerungsanforderung, die eine Base64-codierte PKCS7-Datei verwer](#)

Nun wird der Request in die Zwischenablage kopiert und in das entsprechende Feld eingefüllt:



Microsoft Active Directory-Zertifikatdienste -- WS08R2-CA

Startseite

Zertifikat- oder Erneuerungsanforderung einreichen

Fügen Sie eine Base-64-codierte CMC- oder PKCS #10-Zertifikatanforderung oder eine PKCS #7-Erneuerungsanforderung, die von einer externen Quelle (wie z.B. einem Webserver) generiert wurde, in das Feld "Gespeicherte Anforderung" ein, um eine gespeicherte Anforderung bei der Zertifizierungsstelle einzureichen.

Gespeicherte Anforderung:

Base-64-codierte Zertifikatanforderung (CMC oder PKCS #10 oder PKCS #7):

```
HQ4EFgQUAz66z120xclpLwaQfoozFGQ60TawDQYJ
/sqx0yH38w6THJFg23toh+fHwczj8Izwc1pB9Q
1X4x3mDGJHKEhAmyHcZMRA7Qn12q1DUzho4Nbhx0
xSWVC1TGxZrLc0USXK9oxG9Tu8CKEKIt/VRjWks=
-----END NEW CERTIFICATE REQUEST-----
```

Als Ergebnis erhalten wir eine Bestätigung:

Microsoft Active Directory-Zertifikatdienste -- WS08R2-CA

Startseite

Zertifikat steht noch aus

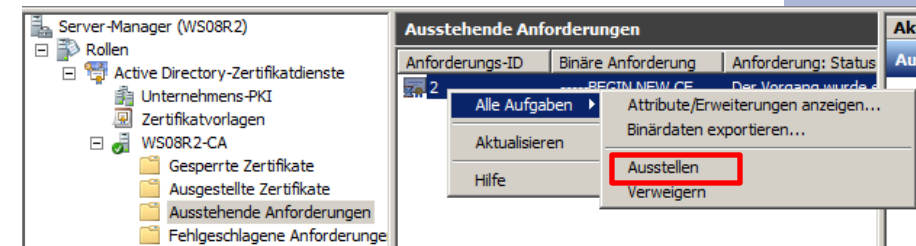
Die Zertifikatanforderung wurde empfangen. Sie müssen warten, bis ein Administrator das angeforderte Zertifikat ausstellt.

Ihre Anforderungs-ID ist 2.

Warten Sie zwei bis drei Tage, und besuchen Sie diese Website erneut, um Ihr Zertifikat abzurufen.

Note: Sie müssen mit diesem Webbrowser innerhalb von 10 Tagen diese Site erneut besuchen, um Ihr Zertifikat abzurufen.

Da das Zertifikat nicht automatisch bewilligt wird, müssen wir dies von Hand nachholen (Hinweis: domain-ingegrierte CAs geben das Zertifikat sofort frei). Dies kann in der CA unter „Ausstehende Anforderungen“ mit einem Rechtsklick auf die Anforderung mit der obenstehenden ID erledigt werden:



Es ist nun unter „Ausgestellte Zertifikate zu finden“. Wir holen nun auf der Webseite das angeforderte Zertifikat ab (Link: Status ausstehender Zertifikate anzeigen). Dazu wird auf das Zertifikat geklickt:

Microsoft-Active Directory-Zertifikatsdienste -- WS0

Status ausstehender Zertifikatanforderung

Wählen Sie die Zertifikatanforderung, die an
[Gespeichertes angefordertes Zertifikat \(M](#)

Und im DER-Format abgespeichert:

Microsoft-Active Directory-Zertifikatsdienste -- WS08R2-CA

Zertifikat wurde ausgestellt

Das angeforderte Zertifikat wurde ausgestellt.

☒ DER-codiert oder ☐ Base-64-codiert



[Download des Zertifikats](#)

[Download der Zertifikatkette](#)

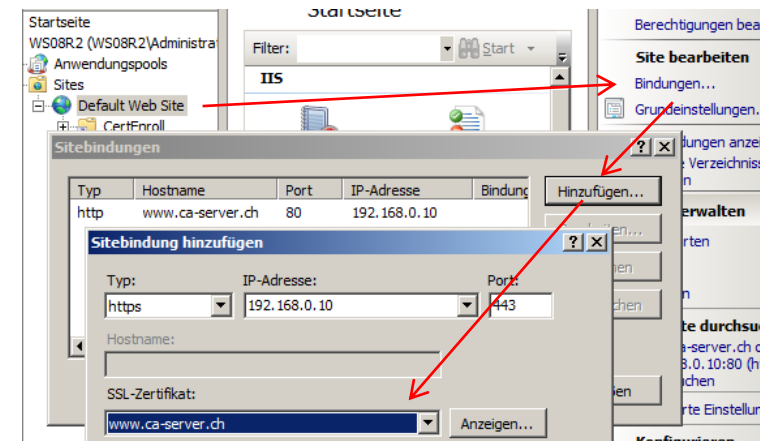
Dateiname: certnew - www.ca-server.ch

Dateityp: Sicherheitszertifikat

Zurück im IIS kann der Request abgeschlossen werden.
Als Anzeigename ist der Domainname empfohlen.



Bei der gewünschten Webseite (in unserem Fall die Default Web Seite) muss nun eine neue Bindung HTTPS erstellt und das entsprechende Zertifikat ausgewählt werden:



Der anschliessende Test zeigt, dass alles in Ordnung ist:



4.3 Email-Zertifikat beantragen

Wir fordern nun ein Zertifikat unter „Ein Zertifikat anfordern“ an. Wir möchten eines für den Emailverkehr:

Microsoft-Active Directory-Zertifikatdienste -- WS08R2-CA

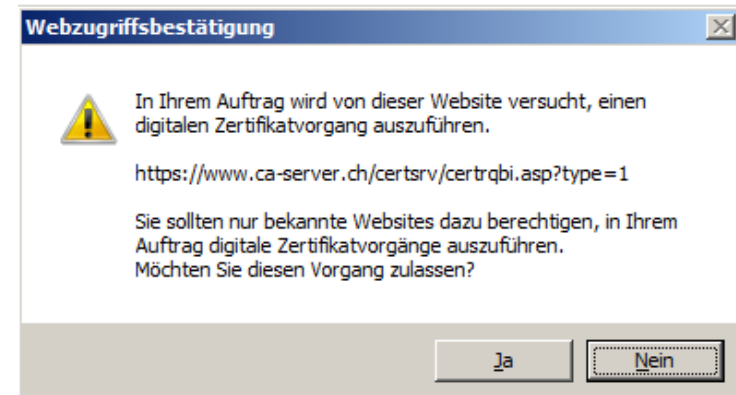
Zertifikat anfordern

Wählen Sie den Zertifikattyp:

[Webbrowserzertifikat](#)

[E-Mail-Schutzzertifikat](#)

Die erscheinende Warnung bestätigen wir mit „Ja“ und füllen anschliessend die Felder wie gewünscht aus.



Weitere Optionen sind nicht zwingend notwendig.

E-Mail-Schutzzertifikat - Identifizierungsinformationen

Geben Sie den erforderlichen Informationen in den folgenden Feldern an, um

Name:	Name
E-Mail:	email@email.ch
Firma:	Firma
Abteilung:	Abteilung
Stadt:	Stadt
Bundesland/Kanton:	Zurich
Land/Region:	CH

Dieses Zertifikat muss analog dem Webserver-Zertifikat freigegeben werden (siehe Screenshots oben).

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

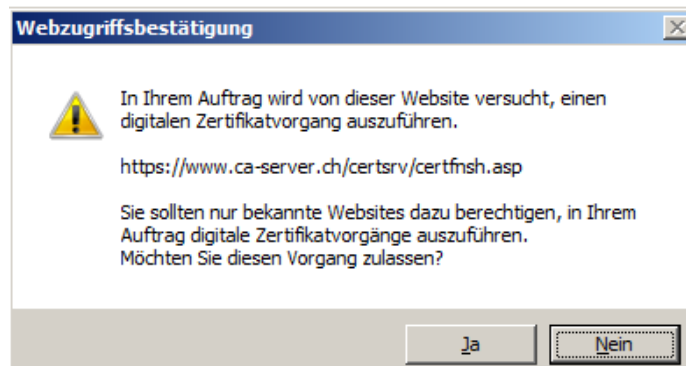
Das ausstehende Zertifikat kann nun geholt werden:

Microsoft-Active Directory-Zertifikat

Status ausstehender Zertifikate

Wählen Sie die Zertifikatanforderung:
[E-Mail-Schutzzertifikat \(Monte Carlo\)](#)

Die Warnung kann ebenfalls mit „Ja“ bestätigt werden:



Ein Klick auf „Dieses Zertifikat installieren“ installiert das Zertifikat:

Microsoft-Active Directory-Zertifikatdienste -- WS08R2-CA

Zertifikat wurde ausgestellt

Das angeforderte Zertifikat wurde ausgestellt.



[Dieses Zertifikat installieren](#)

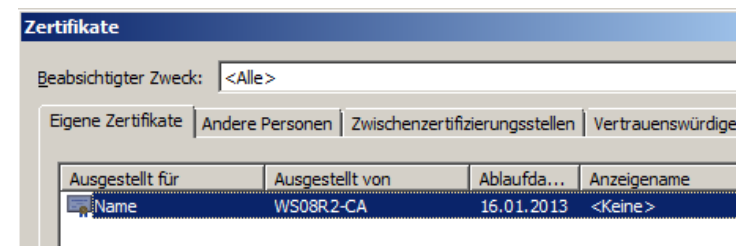
Das Zertifikat kann nun installiert werden.

Microsoft-Active Directory-Zertifikatdienste -- WS08R2-CA

Zertifikat wurde installiert

Das neue Zertifikat wurde installiert.

Ersichtlich ist es im Zertifikatsstore, erreichbar via MMC oder via Internet Explorer „Extras – Internetoptionen – Inhalte – Zertifikate“:



Ab sofort können Emails digital signiert werden.