INFONEWS

goSecurity.ch/infonews

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.

Elektronische Signatur

Der aktuelle INFONEWS kümmert sich um das Thema „elektronische Signatur“. Das Parlament hat das „Bundesgesetz über die elektronische Signatur, ZertES“ bestätigt. Dieses Gesetz tritt auf den 1. Januar 2005 in Kraft. Grund genug, sich mit diesem Thema etwas genauer zu beschäftigen.

Dies ist eine kostenlose Dienstleistung der GO OUT Production GmbH (www.goSecurity.ch/INFONEWS).

Inhaltsverzeichnis

1 Bedeutung der elektronischen Signatur

Die Entwicklung der Informations- und Kommunikationstechnik eröffnet neue Möglichkeiten des Informationsaustausches und der wirtschaftlichen Betätigung. Warenbestellungen, Zahlungsanweisungen an Banken, Anträge oder Einsprüche bei Behörden, die Übermittlung sensitiver Daten im medizinischen Bereich und eine Vielzahl weiterer Kommunikationsbeziehungen, die in der Vergangenheit über Papier abgewickelt wurden, erfolgen bereits zu einem grossen Teil auf elektronischem Wege.

Da sich die Dokumentationserstellung, Kommunikation und Archivierung auf der Basis digitaler Daten etabliert hat und expandiert, ergibt sich der dringende Bedarf nach einer digitalen Lösung, die einerseits den Anforderungen einer offenen Kommunikation (in der sich die Teilnehmer nicht kennen müssen) gerecht wird, bei der andererseits zuverlässig auf den Urheber geschlossen werden kann und die Daten vor unbemerkter Veränderung geschützt sind. Diese Forderungen erfüllt die elektronische Signatur.

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

2 Einführung in die Funktionsweise der elektronischen Signatur

Eine elektronische Signatur ist eine Art von Siegel zu digitalen Daten. So wird unter Einsatz mathematischer Verfahren einen privaten kryptografischen Schlüssel erzeugt. Mit Hilfe des dazugehörigen öffentlichen Schlüssels kann die Signatur jederzeit überprüft und damit der Signaturschlüssel-Inhaber und die Unverfälschtheit der Daten festgestellt werden.

Die jeweils einmaligen Schlüsselpaare (privater und öffentlicher Schlüssel) werden durch anerkannte Stellen natürlichen Personen fest zugeordnet. Die Zuordnung wird durch ein Signaturschlüssel-Zertifikat beglaubigt. Es handelt sich dabei um ein signiertes "digitales Dokument", das den jeweiligen öffentlichen Schlüssel sowie den Namen der Person, der er zugeordnet ist, oder ein Pseudonym enthält. Das Zertifikat erhält der Signaturschlüssel-Inhaber, so dass er signierten Daten für deren Überprüfung beifügen kann. Darüber hinaus ist es über öffentlich erreichbare Telekommunikationsverbindungen (z. B. Internet) jederzeit für jedermann nachprüfbar.

Der breite Einsatz von elektronischen Signaturverfahren erfordert eine zuverlässige und effektive Sicherheitsinfrastruktur für die Zuordnung der Signaturschlüssel durch Zertifikate (Zertifizierungsdiensteanbieter) sowie sichere technische Komponenten. Weiter müssen die Signaturschlüssel-Inhaber darüber unterrichtet sein, welche Massnahmen sie in ihrem eigenen Interesse für sichere elektronische Signaturen zu treffen haben.

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

3 Sichere elektronische Signatur

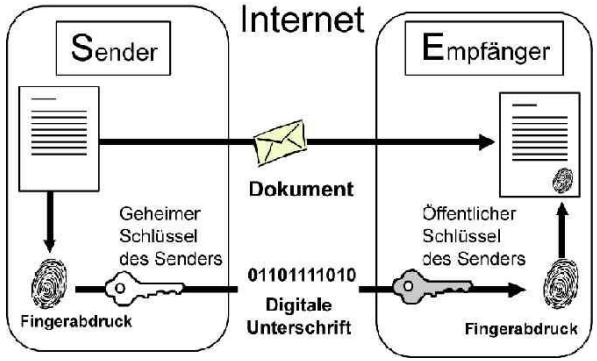
Zusammenfassend kann gesagt werden, dass eine sichere elektronische Signatur:

- ausschliesslich dem Signator zugeordnet ist,
- die Identifizierung des Signators ermöglicht,
- mit Mitteln erstellt wird, die der Signator unter seiner alleinigen Kontrolle halten kann,
- mit den Daten, auf die sie sich bezieht, so verknüpft ist, dass jede nachträgliche Änderung der Daten festgestellt werden kann, sowie
- auf einem qualifizierten Zertifikat beruht und unter Verwendung von technischen Komponenten und Verfahren, die den Sicherheitsanforderungen des Signaturgesetzes und der auf seiner Grundlage ergangenen Verordnungen entsprechen.

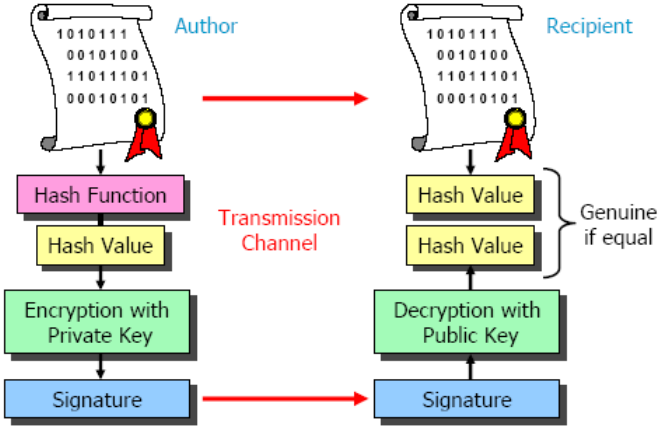
4 Technische Funktionsweise der elektronischen Signatur

Eine qualifizierte elektronische Signatur ist eine Art von Siegel zu digitalen Daten. So wird unter Einsatz mathematischer Verfahren einen privaten kryptographischen Schlüssel erzeugt. Mit Hilfe des dazugehörigen öffentlichen Schlüssels kann die Signatur jederzeit überprüft und damit der Signaturschlüssel-Inhaber und die Unverfälschtheit der Daten festgestellt werden.

Die jeweils einmaligen Schlüsselpaare (privater und öffentlicher Schlüssel) werden durch staatlich anerkannte Stellen natürlichen Personen fest zugeordnet. Die Zuordnung wird durch ein qualifiziertes Signaturschlüssel-Zertifikat beglaubigt. Es handelt sich dabei um ein signiertes digitales Dokument, das den jeweiligen öffentlichen Schlüssel sowie den Namen der Person, der er zugeordnet ist, oder ein Pseudonym enthält. Das Zertifikat erhält der Signaturschlüssel-Inhaber, sodass er es signierten Daten für deren Überprüfung beifügen kann. Darüber hinaus ist es über öffentlich erreichbare Telekommunikationsverbindungen (z. B. Internet) jederzeit für jedermann nachprüfbar.

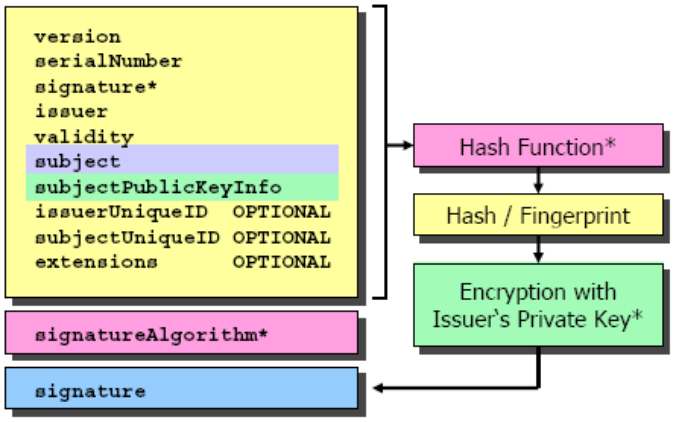


5 Die technischen Details



Aus dem Originaldokument wird ein Hash-Wert generiert. Diese Zahl kann nicht durch geschickte Veränderungen des Dokumentes wiederholt werden. Sobald sich der Inhalt verändert, wird auch der Hash-Wert verändert. Dieser Wert wird nun mit dem privaten, persönlichen Schlüssel signiert. Dadurch wird er eindeutig einer Person zugewiesen. Sollte sich diese Funktion „knacken" lassen, würden automatisch alle Zertifikate ungültig.
Das fertige Dokument wird dem Empfänger auf einem unsicheren Weg zugestellt. Die Signatur wird mit dem öffentlichen Schlüssel zurück in den Hash-Wert verwandelt. Gleichzeitig wird erneut der Hash-Wert aus dem Dokument berechnet. Nun werden beide Hash-Werte miteinander verglichen. Falls genau der gleiche Wert herauskommt, wurde das Dokument nicht verändert.

Ein X.509 Zertifikat ist wie folgt aufgebaut:



Die Hash-Funktion setzt sich aus zahlreichen Informationen zusammen, die aus oben stehendem Bild entnommen werden können.

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

6 Situation in der Schweiz

Obwohl die Schweiz in den meisten E-Governmentranglisten in den Top-10 ist, sieht es bei der Nutzbarkeit dieser Dienste ganz anders aus. Laut einer Statistik befindet sich die Schweiz im letzten Drittel der europäischen Länder (Quelle: Cap Gemini Ernst & Young). An dieser Stelle zeigt sich deutlich, dass eine öffentliche PKI fehlt. Nach dem Auflösen der Firma SwissKey vor etwas mehr als drei Jahren, fehlt hier ein möglicher Nachfolger.

Etwas frischen Wind kommt mit dem neuen Bundesgesetz über die elektronische Signatur, ZertES, welches am 1. Januar 2005 in Kraft tritt. Mit diesem Gesetz werden die Anforderungen an eine Zertifizierungsstelle festgehalten (Artikel 3). Somit kann eine Schweizer Firma Zertifikate ausstellen, wenn Sie diese Bedingungen erfüllen. Auch für ausländische Firmen ist es möglich, in der Schweiz Zertifikate auszustellen. Dabei muss diese Firma durch die schweizerische Anerkennungsstelle bewilligt werden.

Die Generierung und die Verwendung sind in Artikel 6 geregelt. Der Bundesrat zeigt sich verantwortlich, dass die technische Entwicklung eines entsprechend hohen Sicherheitsniveaus garantiert werden kann.

Besonders interessant ist der Artikel 7, in welchem die notwendigen Angaben eines qualifizierten Zertifikates aufgelistet sind:

a) die Seriennummer;
b) den Hinweis, dass es sich um ein qualifiziertes Zertifikat handelt;
c) den Namen oder das Pseudonym der natürlichen Person, die den Signaturprüfschlüssel innehat; im Falle einer Verwechslungsmöglichkeit ist der Name mit einem unterscheidenden Zusatz zu versehen;
d) den Signaturprüfschlüssel;
e) die Gültigkeitsdauer;
f) den Namen, den Niederlassungsstaat und die qualifizierte elektronische Signatur der Anbieterin von Zertifizierungsdiensten, die das Zertifikat ausstellt;
g) den Hinweis darauf, ob die Anbieterin von Zertifizierungsdiensten anerkannt ist oder nicht und bei allfälliger Anerkennung den Namen der Anerkennungsstelle.

Weiter gehören die folgenden Angaben dazu:

a) spezifische Attribute der Inhaberin oder des Inhabers des Signaturschlüssels, wie die Tatsache, dass sie oder er zur Vertretung einer bestimmten juristischen Person berechtigt ist;
b) den Geltungsbereich des Zertifikats;
c) den Wert der Transaktionen, für die das Zertifikat verwendet werden kann.

Mit dem neuen Gesetz werden die Leitlinien für Zertifikate festgelegt. Die Haftung des Ausstellers (Artikel 16) ist ebenso geregelt, wie das Vorgehen bei der Ungültigkeitserklärung von Zertifikaten (Artikel 10).

7 Schlussbemerkung

Es ist zu hoffen, dass mit dieser Grundlage die Schweiz wieder eine eigene Zertifizierungsstelle erhält. Damit wird der Forderung aus der Wirtschaft, von Bund und Kantonen Rechnung getragen. Es gilt zu hoffen, dass die neue Zertifizierungsstelle auf grossen Erfolg stösst.

Die Möglichkeiten von sicheren Zertifikaten würden folgende Dinge ermöglichen:

- einen Überweisungsauftrag in E-Banking,
- einen Kaufauftrag in E-Commerce,
- ein von einem Arzt signiertes Rezept in E-Healthcare,
- ein Reisepassantragsformular in E-Government, oder
- ein EDI-Dokument in E-Business.

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

8 Eigene Zertifizierungsstelle

In allen Windows Server Betriebssystemen ist eine Zertifizierungsstelle integriert. Diese kann einfach unter Systemsteuerung – Software – Windows-Komponenten ausgewählt und installiert werden. Die Installation ist schnell abgeschlossen. Doch bevor gestartet werden kann, sind einige Gedanken notwendig:

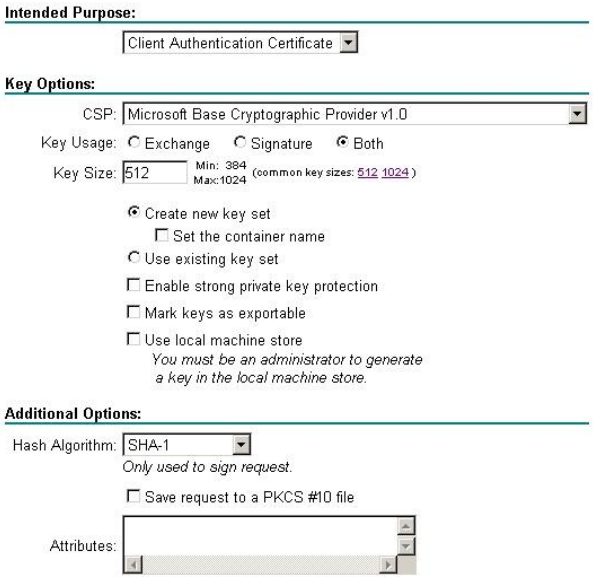
- Wer ist der Aussteller des Root-Zertifikates? (Muss bei der Installation bereits definiert werden)
- Wie wird ein Client-Zertifikat beantragt?
- Welche Anforderungen werden an das Client-Zertifikat gestellt?
- Wie wird die Verwaltung der Zertifikate gelöst?
- Wie werden gesperrte Zertifikate kommuniziert? (Revoke-Liste)

Die Zertifizierungsstelle richtet sich als IIS-Modul ein, das heisst, es ist möglich, die Seite via Web-Browser zu erreichen. Das macht das Beantragen eines Zertifikates sehr einfach. Es besteht die Möglichkeit, ein Zertifikatsantrag zu bestätigen oder mittels eines Formulars ein neues Zertifikat zu beantragen.

Die noch zu bestätigenden, bereits bestätigten sowie die gesperrten Zertifikate sind mittels eines MMC-Zusatzes erreichbar. Die Verwaltung ist auch hier sehr einfach.

Aussteller des Zertifikates

Aussteller des Zertifikates wird meistens die eigene Firma sein. Hier sollte ein allgemein gültiger Name gewählt werden, der z.B. auch für Serverzertifikate verwendet werden kann, die von Aussen erreichbar sind (nur für Testsysteme zu empfehlen). Leider sind die Anforderungen an das Root-Zertifikat von Microsoft vorgegeben und können nicht direkt editiert werden.



goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

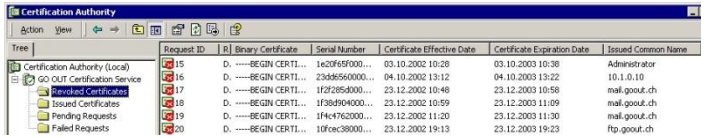
Telefon 052 320 91 20
Fax 052 320 91 21

Antrag und Anforderungen eines Client-Zertifikates
Wie bereits erwähnt, ist es möglich, Zertifikate via Web-Browser zu beantragen. Dies ist eine einfache und schnelle Möglichkeit, neue Zertifikate auszustellen. Wir empfehlen jedoch, die CA nur für bestimmte Gegenstellen freizugeben.
Die Art der Beantragung (Formular / Bestätigung) ist abhängig von den Anforderungen der Applikation. Ein Zertifikatsantrag des IIS ist zum Beispiel als Textdatei verfügbar und kann direkt eingelesen und bestätigt werden. Die Antwort ist eine Datei im .cer oder .der Format.

Verwaltung von Zertifikaten
Hier stellt sich das grosse Problem. Was geschieht mit den Zertifikaten nach der Ausstellung. Da nur ein Teil des Zertifikates vorliegt (Ausnahmen beim Ausfüllen des Formulars), sollte das Zertifikat aus der Applikation, die den Antrag gestellt hat, mit dem privaten Schlüssel exportiert und an einem sicheren Ort gespeichert werden. Vergessen Sie nicht, das gewählte Passwort sicher aufzubewahren, da sonst ein erneuter Import nicht mehr möglich ist.

Gesperrte Zertifikate
Selten kommt es dazu, dass ein Zertifikat vor Ablauf gesperrt werden muss. Doch es nützt wenig, wenn das Zertifikat nur in der ausstellenden Stelle gesperrt wird. Dazu stellt das Microsoft-Tool eine so genannte Revoke-Liste zur Verfügung. Die meisten aktuellen Browser bieten die Möglichkeit, eine Revoke-Liste zu kontaktieren, bevor eine sichere Verbindung zugelassen wird. Wir empfehlen, diese Liste an einer zentralen Stelle der Öffentlichkeit zur Verfügung zu stellen.

Hinweis
Wenn mit einem Browser eine SSI-Geschützte Webseite aufgerufen wird, auf der ein selber ausgestelltes Zertifikat hinterlegt ist, kommt es zu einer Fehlermeldung. Die ausstellende Stelle ist unbekannt. Damit dies nicht zur Verwirrung führt, sollten Sie auf allen Browsern das Root-Zertifikat importieren. Damit dies leicht selber geschehen kann, sollte dieses Root-Zertifikat an einer leicht erreichbaren Stelle hinterlegt und beschrieben werden.



9 Anhang

Folgende ergänzenden Unterlagen empfehlen wir zum Studium:

http://www.a-sit.at/signatur/tutorial/tutorial.htm
Hilfedatei mit vielen Informationen zu den Zertifikaten, Quelle A-SIT Zentrum für sichere Informationstechnologie – Austria

http://www.admin.ch/ch/d/ff/2003/8221.pdf
Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur
(Bundesgesetz über die elektronische Signatur, ZertES)