Global Information Assurance Certification Paper

Hans Chvojka

Digital Signature in Austria

The Internet is rapidly growing with new technologies in Internet security. One such technology, which is becoming increasingly important in Europe, as well as in Austria, is *Digital Signature*. Many companies who have done nothing or very little in the way of Information Technology (IT) security are now faced with this issue. Many companies recognize that using *Digital Signature* technology could solve their security concerns. These companies will no doubtlessly have to rethink their security strategies and react promptly.

Electronic business (e-business) is almost complete in the US in ways of security. As of this year, U.S. companies are the leaders in digital applications associated with the Internet. Most Web sites on the Internet are in English. Ninety-four of one hundred of the most accessed Web servers are physically located in the U.S.

The European Union (EU) has set a goal in the next ten years to use the Internet as a knowledge-based industry and to play a major role in the world of e-business. If the EU wants to become successful in e-business, a number of adjustments have to be made. One such adjustment will be to adopt “digital signature” technology as one of the new securities in e-business. Austria has already passed a law this year regarding digital signature and its application (http://www.a-sit.at/Deutsch/dokument.htm).

The European Union has published a document on electronic signature formats. This document is a very important source of information since Austria is part of the EU. The document can be found at http://www.etsi.org/. The electronic signature formats are specified in the ETSI ES 201 733 V1.1.3 (2000-05). This document specifies the signature policy and the signature validation policy, identifiers, the data structure of an electronic signature and validation data.

The head of the certification service provider in Austria is the Telekom-Control-Commission. The Commission is responsible for the certification service provider and must ensure that the Certification Policies are used correctly and that the certificates and the revocation lists are made available.

Where could a digital signature be used:
- public authorities on the Internet
- secure e-mail
- e-commerce
- e-business
- access control
- identification card
- software distribution
- time stamp service

How should it work and what is needed:

1. Certification Service Provider (CSP)

A CSP is a trusted organization that issues certificates. The CSP generates two types of keys: a private key used for signature creation and a public key used for signature verification. Important is the unique assignment of the public key to the owner. The public key will be stored in a database so everyone has access to it, typically through a Web server.

The Certification Service Provider is required to provide the following services:

- Registration Authority: The individual requesting a certificate to use a digital signature has to apply with the Registration Authority by submitting legal and valid documents with a photo that authenticates that the requestor is who they say s/he is.
- Key Generation: This is where the keys will be generated.
- Certification Authority: Once the personal information is authenticated the Registration Authority will apply the information to a public key and a certificate will be issued. The Certification Authority is also the body who signs the certificate.
- Personalization Service: The Personalization Service provides a Smart Card that contains: the certificate; the private key to sign documents; the name of the owner; the public key; the period of validity; the name of the certification authority and the algorithm.
- Provide a revocation list (a list of blocked and revoked certificates).
- Provide Time stamping service (the Federal Electronic Signature Law, section 1, § 2, section 12: electronically signed confirmation from a CSP that specific electronic data were submitted at a specific time).

For each user of the signature system a pair of keys will be generated (RSA algorithm). The private key will be stored on a Smart Card. The public key will be published on a web server.

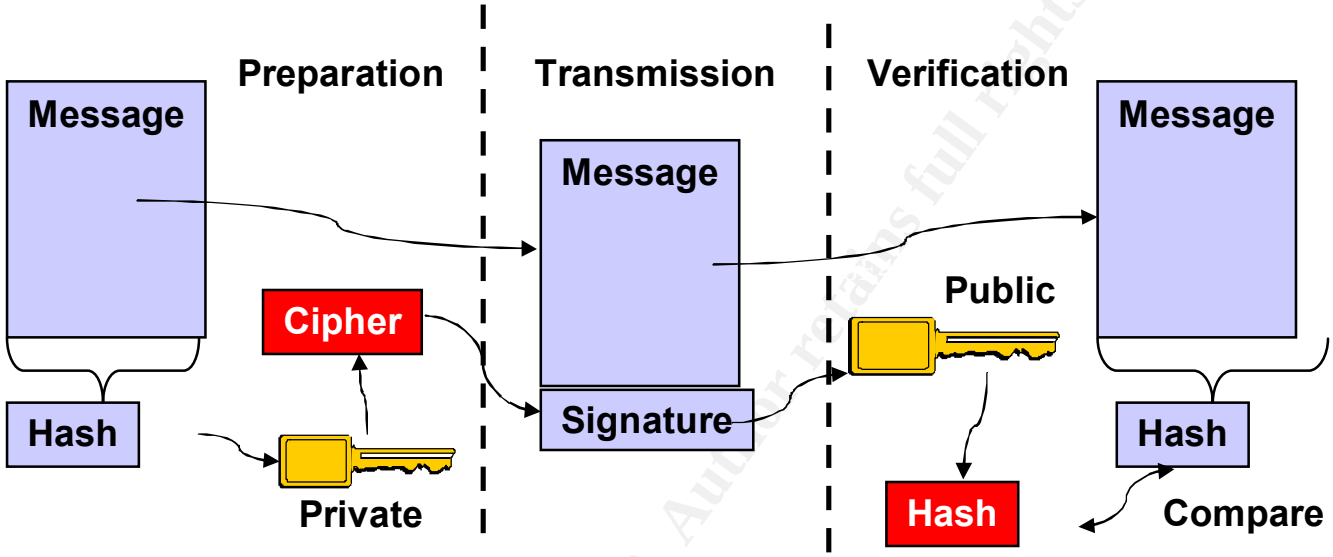
What is needed to use digital signature:

- a PC
- a Smart Card
- a Smart Card reader
- Internet connection
- Software to sign }
- Software to verify } Typically found in the same software package
- Software to check the certificate }

The three parts of the use of digital signature are:

1. Preparation: A hash value will be generated from the message; hash will be encrypted using the private key.
2. Transmission: Both the message and the encrypted hash will be transmitted.

3. Verification: The encrypted message will be decrypted to get the hash value. A hash value will be generated from the message. The hash values will be compared.



The digital signature can be stored on a Smart Card, GSM SIM cards, special programs for digital signatures, etc. However, the two certification service providers in Austria will offer the secure digital signature on Smart Cards (http://www.e-sign.at/ and http://www.a-sign.at/). One provider (A-sign) is offering different levels of certification. The first level “LIGHT” is an e-mail authentication certificate. It can only be used for e-mail. The second level “MEDIUM” is an authentication after the requester has sent the verified documents. The medium level can be used for e-mail and secure web access. To get the third level “STRONG” the requester is required to go to the CSP personally and prove with documents, that he/she is the person who they say they are. The strong certificate can be used for e-mail, secure web access and e-business. (Additional they offer a “PREMIUM” certificate, which is the same as the strong, but includes a Smart Card). The CSP are planning to offer the strong certification service this year (2000).

The Smart Card user will also be provided separately with a PIN code, which is used to activate the digital signature. Another possibility to activate a digital signature is to use biometrics such as a fingerprint. Right now only a few computers have a Smart Card reader and even less use biometrics for identification. As well biometrics technology is more costly and the availability for mass distribution is scarce. Thus PIN codes will continue to be the most common form of digital signature activation.

With the use of Smart Cards we have to take a closer look at the Smart Cards and the reader.

2. What is a Smart Card?

A Smart Card is a card that has either a microprocessor or a memory chip embedded. The most common Smart Cards conform to the ISO 7810. The ISO 7810 defines the physical characteristics of Smart Cards.

There are three categories of Smart Cards:
- Integrated Circuit (IC) Microprocessor Cards
- Integrated Circuit (IC) Memory Cards
- Optical Memory Cards

The microprocessor cards can have an additional cryptographic chip embedded. This cryptographic chip will be used for secure digital signature.

3. Card Reader:

For those using Smart Cards and accepting digital signatures a Card Reader will be needed in order to interpret the information being received.

There are several possible solutions for Card Readers:
- Keyboard with integrated reader (http://www.cherry.de/d/produkt/produkte.htm)
- Smart disk, a card reader as floppy (http://www.smartdisk.com/smarty.html)
- Separate reader offered by various companies
- Card reader for PCMCIA

A card reader integrated in the keyboard or separate devices needs a serial connection (or USB) to the PC. The Smart Card readers are available in different types, key click, soft contact or linear key action.

Sources:

Secure Information Technology Center: http://www.a-sit.at/Deutsch/dokument.htm
European Telecommunications Standards Institute: http://www.etsi.org/
Datakom Austria: http://www.a-sign.at/
A-Trust: http://www.e-sign.at
Smart Card Industry Association: http://www.scia.org/
Smart Card Forum: http://www.smartcart.org/
Austrian Smart Card solution provider http://www.smartcard-solutions.com/
Cherry http://www.cherry.de/d/produkt/produkte.htm
Smarty: http://www.smartdisk.com/smarty.html

Last Updated: May 28th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event