ww&p Walder Wyss & Partners
Attorneys at Law

NewsLetter

Nr.19 February 2000

Digital Signatures in Switzerland

It is well known that e-commerce is rapidly expanding. However, recent studies show that Internet users' concerns about security of data transmission through the Internet is a relevant factor restraining this expansion. After numerous and extensive discussions about digital signatures it is worthwhile giving a summary of the cryptographic techniques and functions in general and outlining various legal aspects of digital signatures.

Consumers, but also companies offering products or services, are mainly concerned about the following security issues in relation to electronic communication: (1) **authentication**, i.e. certainty regarding the sender of a message (is X really the sender of the message ?);

by Dr. Jasmin Ghandchi
+41 1 265 75 36
jghandchi@wwp.ch

(2) **integrity**, i.e. certainty that the message has not been modified between the time of sending and the time of receipt of the message (is this the content of the message which was originally sent ?); (3) **non-repudiation**, i.e. certainty about non-repudiation of origin and of delivery (sender / recipient cannot deny to having sent / received the message); (4) **confidentiality**, i.e. certainty, that sender and recipient have exclusive knowledge of the content of the message (has anyone been able to intercept the message ?).

Cryptosystems

All four of the concerns set forth above can be eliminated with cryptographic techniques. There are two types of cryptosystems: **secret-key** (symmetric cryptography) and **public-key** (asymmetric crypotgraphy). In secret-key cryptography, the same key is used for both encryption (transformation of data into a form that is as close to impossible as possible to read without appropriate knowledge, i.e. a key) and decryption (transformation of encrypted data back into intelligible form). The secret-key technique is only applicable among a very small number of persons who know and rely on each other. Since parties communicating for e-commerce purposes usually do not know each other the public-key cryptography is the more popular technique. In public-key cryptography, each user has a public and a matching private key. The future recipient publishes his public key but keeps his private key secret. This enables an indefinite number of persons to send a message to the recipient which is encrypted with the recipient's public key. Only the recipient can decrypt the message with his private key. This technique ensures only confidentiality between the electronically communicating parties. However, it does not ensure authentication, integrity or non-repudiation.

Digital signatures

Authentication, integrity or non-repudiation can be ensured with digital signatures. This is a popular public-key technique in which only a so-called digital fingerprint (which is shorter than the message) is encrypted with sender's private key. The recipient can decrypt the digital fingerprint with sender's public key. Typically, the digital fingerprint is created by using a hash function which takes a message of arbitrary length and shrinks it down to a fixed length which is then added to the message itself (which can also be encrypted). After application of the hash function, the sender encrypts the digital fingerprint with his private key and sends the message together with the encrypted digital fingerprint. The recipient of the message must apply the same hash function as the sender and has to decrypt the digital fingerprint with the sender's public key. If the result of recipient's application of the hash function is identical with the decrypted digital fingerprint which the sender forwarded, it is certain that the message was sent by the sender (authentication; non-repudiation) and that it was not modified between sending and receiving (integrity).

Certification Authorities («CA»)

To additionally enhance the confidence in public key cryptography generally and in digital signatures in par-

ticular, it must be certain that no impostor can secretly substitute his own public key (to which he has the matching private key) for the public key of another person. Therefore, trusted third parties such as CA are being created to bind a key pair to the identity of the owner. CA will keep a register in which the owner's public key is registered. The CA certifies that a public key belongs to a specific owner. This certificate will be issued by a digital certificate which is also digitally signed by the CA.

Ordinance on Public Key Infrastructure («OPKI»)
In order to further enhance confidence of the public, the CA must be absolutely trustworthy. Therefore, the Swiss Federal Council drafted the OPKI which shall be enacted probably on May 1, 2000. The purpose of the OPKI is to set standards ensuring quality of certificates issued by CA in Switzerland. Complying with OPKI's standards is on a voluntary basis. If CA comply with such standards the Swiss Authority for Accreditation shall award the status of Accredited Certification Authorities («ACA»). It is expected that the public will prefer to use services of ACA rather than those of non-accredited CA. The OPKI sets forth very general technical, administrative, regulatory and organizational standards for the ACA itself and for granting and issuing a certificate. More specific technical standards will be set forth separately in ordinances issued by the Swiss Authority for Accreditation.

Validity and enforceability of digital signatures
Contrary to the EU Directive for Digital Signatures, which was enacted on January 19, 2000, the OPKI is silent on the question of validity and enforceability of digital signatures. Therefore, the OPKI will be followed by a statute which should also include provisions regarding the validity and enforceability of digital signatures. The Federal Department of Justice has been charged with the drafting of a proposal for such law, to be completed at the end of this year. This is only the beginning of a legislation procedure which may take another year or years.

The legal validity and enforceability of a digital signature can refer to various areas of law, namely:
(1) **Contracts:** the majority of the contracts can be validly concluded without complying with formal requirements. However, certain types of contracts can only be validly concluded if certain formal requirements have been met by the parties. Such formal requirements include the personal signature by the parties, the requirement that the document must be in holographic form (handwritten), or the requirement that the contract must be notarized etc. (2) **Debt enforcement:** for example, if a creditor can produce a document in which debtor explicitly acknowledges to owe a certain amount and this document is personally signed by the debtor debt enforcement law provides a special procedure which simplifies enforcement of such debt. (3) **Registrations in the commercial register and the register for land property:** applicable statutes presently require that the application for registration and/or certain enclosed documents have to be submitted in hardcopy and/or added with a personal signature and eventually, the documents have to be submitted in a notarized form. In all three areas it remains uncertain whether or even improbable that courts will recognize a digital signature complying with the formal requirement of personal signatures without any statutory basis. However, the law in work is intended to contain provisions which would recognize a digital signature complying with the formal requirement of a personal signature. (4) **Evidence:** although existing laws on civil procedure may not explicitly enumerate electronically transmitted messages (with digital signatures) as admissible evidence, this statutory omission may not exclude this as a form of evidence. It may very well be that electronically transmitted messages with digital signatures certified by ACA will be admitted as evidence, especially if they also carry a time stamp of an ACA.

ww&p **Walder Wyss & Partners**
Attorneys at Law

Münstergasse 2
P.O. Box 4081
CH-8022 Zurich
Phone +41 1 265 75 11
Fax +41 1 265 75 50
reception@wwp.ch
www.wwp.ch

London Office
9 Gray's Inn Square
London WC1R 5JQ
Phone +44 171 405 2043
Fax +44 171 405 0605