Electronic Signatures – a Position Paper

Marc Sel - 2001-01

A short summary of electronic signatures

In 1977 Rivest, Shamir and Adleman made their discovery public that a simple mathematical function could actually be used to construct a practical system for (what they called at that time) digital signatures. Their system was based on Integer Factoring.

Such a system would use data, the RSA algorithm, a private key and a public key. The private key is used to create the signature, and the public key is used to verify the signature (refer to Technical Note #1 below for the distinction between signatures with appendix and with message recovery). A hash function is often used to be able to sign a short representation of the data, rather than the full-length original data. As such, the creation and standardisation of hash functions is fundamental to digital signatures.

Over the years, other digital signature systems were created besides RSA, such as those based on Discrete Logarithm (e.g. the Digital Signature Algorithm) and on Elliptic Curves.

Originally, the RSA company defined basic standards for encrypting and signing in their PKCS (Public Key Cryptographic Standards) series. Their PKCS #7 document became a de-facto standard for cryptographic messages and it is still in use today.

However, over the years a number of standardisation initiatives led to a wide range of standards, including amongst the most influential ones:

- ISO/IEC 9796 (1991): This specifies a digital signature mechanism based on the RSA public-key technique and a specifically designed redundancy function;
- ISO/IEC 9796-2 (1997): This specifies digital signature mechanisms with partial message recovery that are also based on the RSA technique but make use of a hash-function.
- ISO/IEC CD 9796-4: Discrete logarithm based mechanisms.

Other standards include ISO/IEC FCD 14888-1, -2 and –3, as well as ISO/IEC WD 15946-2 (ECC). Also the ANS (American National Standards body) issues a number of digital signature standards, mainly for use by the Financial Services industry.

Underlying hash functions include MD2, MD4, MD5, SHA, SHA-1, RIPEMD, and RIPEMD-160.

In Europe, bodies such as the CEN (Comité Européen de Normalisation) work on taking over existing standards into a European context. This includes the EESSI (European Electronic Signature Standardisation Initiative) project.

For telephony, ETSI (European Telecommunications Standards Institute) established a number of standards, including those for securing GSM (Groupe Spécial Mobile) and DECT (Digital European Cordless Telephone) systems.

In an Internet context, it is important to mention the RFC (Request for Comment) documents, which reflect the Internet adagio of ‘rough consensus and running code’. As such, they do not establish standards, but such RFC’s sometimes spread already well-known algorithms to a wider audience, or they do present a new solution. RFC documents often represent a somewhat American view to problems and solutions, which is not necessarily shared by European experts. However, in an Internet-centric society, they obviously cannot be ignored.

Today in Europe, we have the European Directive 1999/93/EC defining the Community framework for electronic signatures. In this context, we prefer to use the term ‘electronic signatures’ (as opposed to ‘digital’ signatures) to indicate that various electronic technologies need to be considered (biometrics, smart pens, …).

The Directive specifies ‘advanced electronic signatures’ that are created by ‘secure signature-creation devices’. Such signatures are verified on the basis of public keys residing in ‘qualified certificates’ provided by ‘qualified certification providers’. Such signatures will satisfy legal requirements in the same manner as hand-written signatures do. It is clear that a PKI-based solution can meet the requirements for an ‘advanced electronic signature’ as laid down in the Directive.

The Directive does not detail which technical standards are required. However, in the context of the CEN (Comité Européen de Normalisation), work is done on the EESSI (European Electronic Signature Standardisation Initiative). Here a set of technical standards is proposed to form the foundation with regard to underlying algorithms and data formats for use in Europe.

This set is deliberately kept fairly rich, in order to allow systems to be build which meet stringent security requirements for a number of specific cases. Signature verification techniques used for road pricing are subject to totally different constraints as those in the context of e.g. Internet banking. However, as a consequence, the designer (and to a certain extent the user) of the system should be aware of all possibilities at his disposal.

The commonly uttered phrase ‘the good thing about standards is that there are so many to choose from’ certainly applies to electronic signatures. For systems to be secure, well-performing and inter-operable, the selection of appropriate signature standards is critical. EESSI seems to be well underway to facilitate secure ebusiness.

Technical Note # 1

Essentially, there are two classes of signatures, “with appendix” or “with message recovery”.

“With appendix” refers to a separate signature file, created by the algorithm when providing the private key and the data as input. However, the original data is first transformed into a short hash value, which is encrypted rather than the full-length data. The encrypted hash functions as a signature and is sent as appendix to the original message. The relying party will use the original data, the signature file, the algorithm and the public key to perform verification.

“With message recovery” refers to the fact that the full data is formatted and encrypted, and successful recovery of the original data (complemented by some redundant information) is considered as verification of the signature.

Signatures “with appendix” are more common.

Technical Note # 2

For those interested, the original publication of the RSA algorithm was in the article “A method for obtaining digital signatures and public-key cryptosystems”, Communications of the ACM, 21, (1978), 120-126.

An excellent source of information on cryptography and digital signatures is the ‘Handbook of Applied Cryptography’ by Menezes, van Oorschot and Vanstone (1997 – CRC Press LLC).

Further information with regard to electronic signatures and cryptography can be found at the website of PricewaterhouseCoopers’ Cryptographic Centre of Excellence (www.pwcglobal.com/cce) or at the website of our Trusted Third Party, www.betrusted.com .