Securing e-business

By Mr. Ted Humphreys [1], *Dr. Marijke De Soete* [2] *and Prof. Chris Mitchell* [3]

There are many risks that may happen in an e-business world, including fraudulent transactions, user accounting and validation errors, and deliberate or accidental mistakes in identifying citizens, customers and business partners. These and other risks can have a significant financial impact on citizens using the Internet for on-line shopping, and on businesses exchanging legally binding documents or making payments and transactions electronically.

We previously wrote about some of the security issues arising in the conduct of e-business, and the technologies that exist to address these issues. That article [4] discussed a management framework for establishing trust for e-business. This current article takes this a stage further by looking at some of the security standards being implemented in various e-business technologies to help ensure business confidence in the e-business world. These standards are designed to help counter the risks mentioned above and thereby engender long-term success and trust in e-business.

Enter the world of cryptographic techniques

Cryptographic methods and techniques can be used in a range of different ways, such as protecting the integrity and guaranteeing the origin of an electronic document, preventing the originator of an electronic document from repudiating it (*non-repudiation*), or verifying the identity of a communicating party. These are all key issues in e-business, and it is vitally important for all parties involved in e-business to have trusted and interoperable techniques that can secure and protect e-business services. Therefore having access to standardized security techniques should be of considerable significance to businesses worldwide. In recent years, ISO/IEC JTC 1/SC 27, *IT Security techniques*, have developed standards which cover a wide range of cryptographic techniques designed specifically to address e-business concerns, and this article focuses on two fundamental security mechanisms, namely authentication and digital signatures.

Authenticating users and devices

Entity authentication mechanisms are fundamental to the establishment of secure communications between two parties; for example the industry protocols SSL/TLS, used by many Web browser applications, are based on an entity authentication mechanism. Also, NIST (National Institute of Standards and Technology), which produces standards for US Government use, has recently produced a Federal Information Processing Standard (FIPS Pub 195) based on ISO/IEC 9798-3, containing two entity authentication mechanisms based on the use of digital signatures.

"New standards provide vital building blocks for signing e-business transactions."

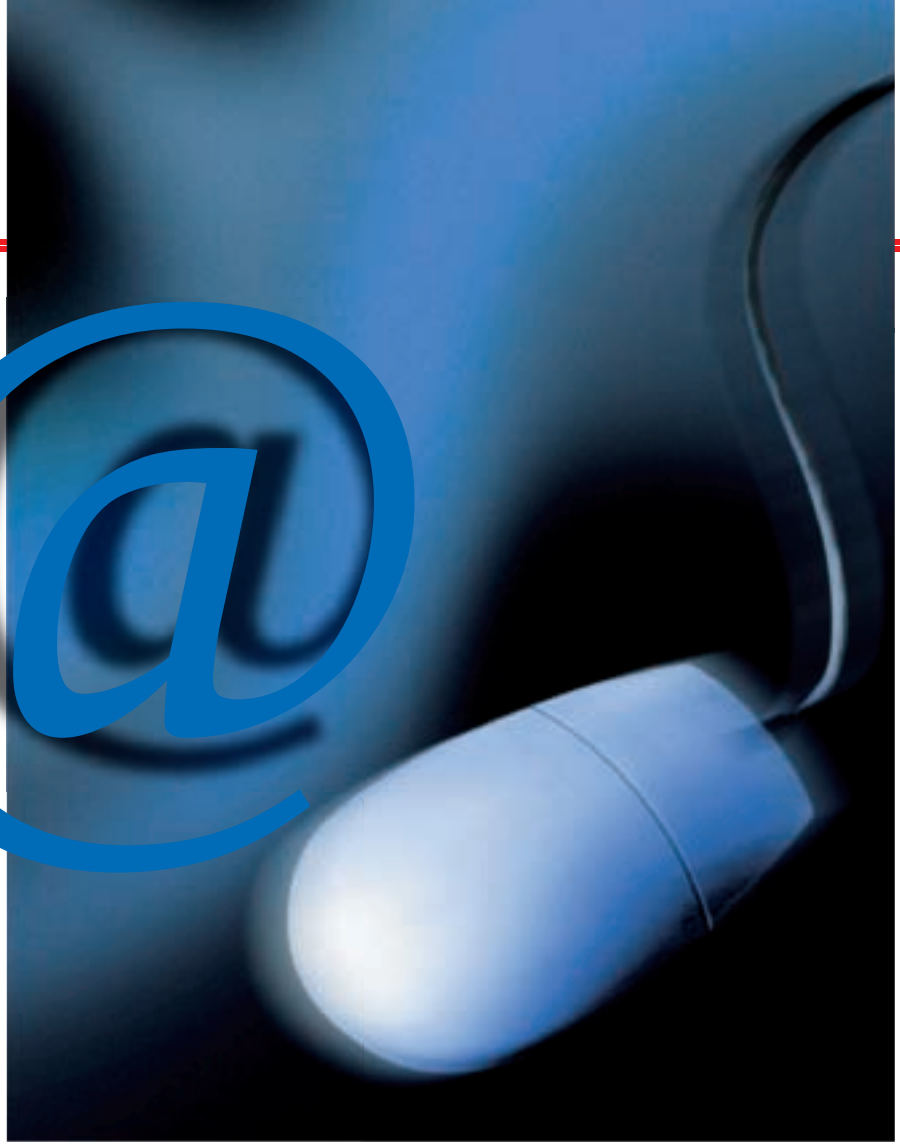
ISO/IEC 9798, *Entity authentication*, is a five-part standard that specifies mechanisms that can be used to corroborate that an entity is the one that is claimed. An entity to be authenticated proves its identity by demonstrating its knowledge of a secret. The mechanisms involve exchanges of information between entities (e.g., users, computers or communications devices) and, where required, exchanges with a trusted third party. The individual messages exchanged between parties are protected using cryptographic techniques, but successful authentication also requires proof of the timeliness of messages, to prevent a malicious party simply replaying old messages to impersonate a user. Thus the messages also incorporate techniques for establishing message freshness, e.g., timestamps or random challenges and responses.

Part 1 of ISO/IEC 9798 provides a general model for entity authentication and Parts 2-5 of this standard specify mechanisms based on different types of cryptographic techniques, including digital signatures, encryption and Message Authentication Codes (MACs). Separate standards exist for each of these types of techniques, and the standards for signatures, of particular relevance to e-business, are discussed later in this article.

Digitally signed information

A digital signature in the electronic world (e.g., in an exchange of payment information) provides the same kind of characteristics that are expected from a handwritten signature in the paper-based world. It is applicable to providing authentication of the signer, integrity of the information being signed and non-repudiation of the transaction. Digital signatures are being used for the protection of patient records in healthcare systems, for electronic payments, exchange of information via Web browser, filing tax records and other legal documents, on-line shopping and card transactions.

Digital signature capabilities are being embedded in mobile phones, mobile computing devices, smart cards and other IC cards, Web browsers and many other technologies and applications. Therefore several digital signature schemes have been developed and standardized to offer a range of implementation options to take account of application and technology variants and constraints: length/size of message/document to be signed, storage and transmission limitations/capacity, speed of signing and verification, and performance.



ISO/IEC 9796, *Digital signature schemes giving message recovery*, is a three-part standard, which specifies digital signature mechanisms giving partial or total message recovery, aiming at reducing storage and transmission overhead. The second part of this standard (covering schemes based on the difficulty of the integer factorization problem) specifies three digital signature techniques for messages of any length. The third part (covering schemes based on the difficulty of the discrete logarithm problem) specifies a further two signature methods. Schemes from this standard are specifically designed to minimize the data overhead of using signatures, and hence are designed for application in constrained environments, where storage space and/or communications bandwidth may be very limited. Examples of application domains include smart cards and personal mobile devices.

ISO/IEC 14888, *Digital signatures with appendix*, is a three-part standard: a general model which provides a description of the signature and verification processes of a digital signature with appendix, and two further parts each based on a specific type of digital signature mechanisms with respect to the distribution of verification keys. In Part 2: *Identity-based signature mechanisms*, the verification key is a public function of the signer's identity, while in Part 3: *Certificate-based signature mechanisms* the verification key cannot be computed from the signer's identity but the verifier obtains it by some other means, e.g., by retrieving it from a certificate. In summary ISO/IEC 14888 offers a complete range of signature mechanisms designed for general application.

At this point it is also important to mention hash-functions, i.e. functions mapping messages to short fixed-length blocks of bits called hash-codes.These functions are a vital component in almost every practical digital signature scheme, including all those standardized in ISO/IEC 9796, *Digital signature schemes giving message recovery*, and ISO/IEC 14888, and therefore developers of applications and software must also choose a hash-function for the signature scheme they are implementing. ISO/IEC 10118, *Hash-functions*, is a four-part standard specifying cryptographic hash-functions designed to efficiently compute short hash-codes, e.g. of 20 bytes, as a function of arbitrary length messages. These hash-functions have the one-way property, i.e. given a possible short hash-code it is computationally infeasible to find a message that, when input to the hash-function, gives this hash-code as output. ISO/IEC 10118 provides a wide range of hash-functions, using a variety of different computational techniques.

Application-specific standards

The generic signature techniques defined in ISO/IEC 9796 and ISO/IEC 14888 are of importance in a broad range of application domains, and it is intended that these standardized techniques are used as building blocks in the development of application-specific standards. For example, the ISO/TC 68, *Banking, securities and other financial services*, defines security standards for the financial industry, which are based on the generic security standards,

1) Mr. Ted Humphreys is Convenor of ISO/IEC JTC 1/SC 27/WG 1, Requirements, security services and guidelines.

2) Dr. Marijke De Soete (MasterCard Int.) is Convenor of ISO/IEC JTC 1/SC 27/WG 2, Security techniques and mechanisms.

3) Prof. Chris Mitchell (Royal Holloway, University of London) is editor of ISO/IEC FCD 18033-1, Information technology – Security techniques– Encryption algorithms – Part 1: General and ISO/IEC 9798-6, Information technology -- Security techniques -- Entity authentication -- Part 6: Mechanisms based on manual data transfer.

4) Mr. Ted Humphreys, 'Trust in E-biz'. *ISO Bulletin*, January 2003

5) A joint specification, orginally developed by Europay, MasterCard and Visa, and now administered by EMVCo, LLC, which ensures global interoperability for smart card payments by defining all interactions that take place between a smart card and a chip terminal. These specifications are available from the EMVCo website www.emvco.com

mentioned above. Also ISO/IEC JTC 1/SC 17 refers to these standards for application in smart cards (e.g., within ISO/IEC 7816, *Identification cards –Integrated circuit(s) cards with contacts* – Part 5: *Numbering system and registration procedure for application identifier*). The financial industry standard for chip card-based debit/credit transactions (known as the EMV specifications[5]) uses a digital signature technique taken from ISO/IEC 9796-2 (a scheme optimized to minimize storage requirements in the card and bandwidth in the transmissions) and a hash-function from ISO/IEC 10118-3, *Information technology – Security techniques – Hash-functions* – Part 3: *Dedicated hash-functions.*

Increasing needs for protection

As more business is now being carried out electronically, the need to protect the information a company processes electronically continues to increase. The standards mentioned above provide some of the vital building blocks for signing e-business transactions. The ISO/IEC JTC 1/SC 27 current development programme is set to shape an even better future for protecting e-business worldwide. This includes some newer techniques that can be used for authentication/digital signatures. A multipart standard, ISO/IEC 15964, *Cryptographic techniques based on elliptic curves*, provides further digital signature schemes in parts 2 and 4. Their different performance characteristics make them of particular interest in specific environments using, for instance, contactless technology. Work has also started on the standardization of security requirements for "cryptographic engines" and, indeed, a new standard on *Security requirements for security modules* is underway and will be based on FIPS (Federal Information Processing Standard) 140-2.

Paying for standards has

By Mr. Keith Moyes, International Commercial Policy Manager, BSI (United Kingdom)

Standards are crucial. They support legislation, promote trade, create common understanding, reduce costs, accelerate product development, save money and can even save lives. With so much at stake, we should do everything we can to promote their widest use. Paying for standards restricts their use. Standards should be free!

That is an argument the ISO community has been hearing for years: from governments, academics, companies that have invested heavily in standards development and from many standards users. It has real merit, but I want to argue for retaining the current system in which standards work is largely funded through sales of standards.

We should avoid false alternatives. There are no free standards, just as there are no free laws or regulations. Someone, somewhere, is paying for these documents to be written and disseminated. It might be a small group of companies paying large fees to be members of a consortium, or the taxpayer paying for a parliament and its supporting administration. It is just a question of who is paying and how. In the ISO community, it is the purchasers of standards who pay, but we can all envisage alternative models that would allow standards to be freely accessible. These are not just theoretical; there are successful precedents in existence right now, so why doesn't ISO follow them?

Partly, it is a question of history. ISO has developed according to a different business model and it would be difficult to change now, but that is not a compelling reason for maintaining the status quo. Many necessary changes are difficult, but that is no reason to avoid making them. However, I believe that the ISO model has evolved and persisted because it has real advantages that are often overlooked.

"International Standards have a unique status because they embody core ISO values."

There are many standards that are widely used, but International Standards have a unique status because they embody certain core ISO values. They are consensual, open, transparent, balanced and voluntary. The funding system that has evolved is the one that is most consistent with the preservation of these values.