Editorial

The articles in this issue of the Journal expresses the underlying tension between the forms of electronic signature that people use in their daily lives, and the early attempts to introduce the widespread use of cryptography in the form of digital signatures as a standard form of electronic signature. When using technology, people prefer something that is both easy to use and straightforward to understand. This is why, when it comes to the form an electronic signature can take, the three most popular types of electronic signature in use are:

- Typing a name into a document, such as an e-mail.
- Using a password or a personal identification number (PIN).
- Clicking the 'I accept' icon to accept the terms of a software licence or to agree to enter a contract on-line.

These forms of electronic signature are popular because of their attributes and simplicity of use. For instance, the act of typing a name into a document in electronic format replicates the meaning of a manuscript signature. Of course, the typed version of a name is clearly not capable of replicating the unique manifestation of a manuscript signature. However, the act of typing a name into a document, or the inclusion of the name in an automatic signature block at the end of an e-mail, acts as a symbolic link to the physical world. A person's name is capable of representing their unique identity. As a result, the use of a name typed into a document in electronic format is capable of serving a number of purposes, one of which is to identify the sender of the communication, another of which is to indicate the sender adopts the content.

However, there is a perceived problem with the use of the three types of electronic signature set out above. That is, it cannot be certain that the person whose name is typed in the e-mail, the password or the PIN number used, or the icon that is clicked, is that of the person that it claims to represent. In this respect, the claim made for digital signatures is that the use of a signature based on cryptography provides a greater assurance in providing the link between the owner of the digital signature and the use of the signature. Politicians across the world have accepted this assertion, and have passed laws to this effect, including legal presumptions regarding the use of digital signatures in particular. To give one example, the provisions of article 7 of the *Ley De Firma Digital N° 25.506* of Argentina sets out a presumption that where a digital signature is used, it belongs to the holder of the certificate:

> "ARTICULO 7°. – Presunción de autoría. Se presume, salvo prueba en contrario, que toda firma digital pertenece al titular del certificado digital que permite la verificación de dicha firma."

> "ARTICLE 7. – Authorship presumption. Unless it is otherwise proved, every digital signature is presumed to belong to the holder of the digital certificate that permits the verification of the digital signature in question."

The presumption is further enhanced by the provisions of article 10. This provides that where a person uses a digital signature, they will be presumed to have sent it, even where it is sent automatically:

> "ARTICULO 10. – Remitente. Presunción. Cuando un documento digital sea enviado en forma automática por un dispositivo programado y lleve la firma digital del remitente se presumirá, salvo prueba en contrario, que el documento firmado proviene del remitente."

> "ARTICLE 10. – Sender presumption. When a digital document is sent automatically by a programmed device and bears the sender's digital signature it shall be presumed, unless otherwise specified, that the signed document was originated by the sender."

Unfortunately, both the technology and the infrastructure supporting digital signatures is opaque and difficult to understand. The vast majority of people fail to appreciate the need to secure their computers from hackers and other threats, as the number of zombie computers used by hackers testifies. This means a digital signature can be used by a malicious person, either by obtaining remote access to a computer, or where the computer is used by a person other than the owner of the digital certificate. Naturally, the other forms of electronic signatures set out above are just as capable of being misused in the same way.

As a result, the recipient of an electronic communication or document must determine for themselves whether they trust the source of the communication. It is for this reason that a name typed into an e-mail is easier to deal with. People are beginning to become more familiar with the features to look out for when an e-mail is received that does not appear to be genuine. Even if a person is not aware of the header information that is available to test the source of the e-mail (although this may be forged), there are a number of features that a recipient can assess, including the authenticity of the sender's e-mail address, the linguistic structure of the text of the e-mail, and whether there are references to physical attributes, such as a postal address or a telephone number. It is inevitable that new users of the networked world will make mistakes, such as responding to phishing attacks. However, a combination of intuition and education will help resolve, although not eradicate, reliance on forged or unwanted electronic communications. Digital signatures do have a part to play, but within the context of a closed system, by which all the parties are contractually bound to provide for the security of their systems, thus reducing the risks that an electronic signature can be used without authority or inappropriately.

It is inevitable that new users of the networked world will make mistakes, such as responding to phishing attacks

Editorial

Of future interest will be how human beings cope with the demands to retain passwords and PIN numbers in their memory

The digital environment has caused us to more fully comprehend the complexities of the assumptions we take for granted in the physical world.

One example is buying goods and services over the internet. Previously, buying at a distance was mainly by mail order catalogue, a means of selling that began in the nineteenth century. Catalogues are not immune from schemes to defraud buyers. However, because it takes time, trouble and expense to display merchandise in a catalogue, the buyer feels a degree of reassurance that the catalogue is trustworthy because it is a physical object, which in turn provides a high level of comfort. The catalogue confirms the existence of the supplier, and acts to reassure the buyer that the goods they order will be supplied.

The physical item of a catalogue should not, necessarily, act to reassure the buyer. The catalogue could be an elaborate swindle to defraud buyers by purporting to offer goods, and once sufficient money has been cashed, the thieves disappear without supplying the goods ordered. To be worthwhile, the cost of setting up the deception has to be low enough to provide an adequate return.

Attempts to defraud mail order catalogues are relatively rare, because the set-up costs are disproportionate to the return. The reverse applies in the digital world. The outlay in setting up a similar operation in the digital domain is minimal, and the returns can be significant. Mass education has helped budding crooks, because schools across the world not only teach children how to read and write, but they provide sufficient knowledge about computers to encourage the fraudsters whilst young. However, the majority of children receive such a rudimentary understanding of the digital world, that they fail to understand the risks when participating in the digital world.

Until the emergence of the digital environment, we relied on our perceptions, based on experience, about the physical materials we handled in everyday life. A person will trust a physical object by considering its intrinsic properties. Items that are not trustworthy may be manifest because a letterhead does not quite look genuine, or a manuscript signature on a cheque differs a little too much from that which is usually observed. In essence, we all authenticate the provenance of physical objects every day: just as we are learning to verify our perceptions in the digital world.

In responding to the risks associated with the digital realm, attempts have been made to provide sufficient assurance that the person we are dealing with is the person we should be dealing with. This is often described incorrectly as ‘security’ by people at the end of a telephone in a call centre. Authenticating the identity of the other party certainly forms part of the security process, but in itself, the aim of authentication is to validate the person’s identity: it is necessary to exchange sufficient information to reassure one or both parties that the person they are communicating with is the person whom they claim to be.

For this purpose, government agencies and banks in particular have taken great strides to resolve this problem. In responding to this quandary, the digital world has moved us away from dependence on a signature, to reliance on the use of multiple items of information that, taken together, validate the identity of the user to an acceptable degree of trustworthiness.

Of future interest will be how human beings cope with the demands to retain passwords and PIN numbers in their memory. A person has little difficulty in replicating their manuscript signature, but may have significant problems in recalling passwords and PIN numbers to obtain access to their bank account and other services. To this end, it will be significant to know what work has been undertaken in the medical profession on memory. For instance, consider the liability of a bank that insists a person must use a PIN number to obtain access to their bank account. The question might be, what is the likelihood that the bank is liable for failing to deliver up the customer’s property, even though the customer cannot remember their PIN number, yet they are perfectly capable of signing their name.