Digital Signature Realities in Modern Businesses

P.U. Chine
Head ICT section,
UNICEF Field Office,
Enugu State, Nigeria.
Email: pchine@unicef.org

M.E. Ezema
Department of Computer Science
University of Nigeria, Nsukka
Enugu State, Nigeria
Email: modesta.ezema@unn.edu.ng

ABSTRACT

Digital signatures are a technology that allows two parties to validate the authenticity of electronically transmitted information and documents. When added to a document, it provides some assurance that the document’s sender is the person purports to be. Digital signatures allow companies to share data without the fear of disclosing sensitive information to people for whom it is not intended. The effect of Information Technology on the Auditor’s Consideration of Internal Controls in a Financial Statement Audit, highlights the professional importance of understanding and managing new technologies such as digital signatures. “Digital signatures which represent one of the most explosive modern technologies adoption will undoubtedly help the rapid growth of e-commerce, online assurance procedures, intrusion testing, and other dynamic technology-enabling processes that can better protect online data. This paper considers how effective the promotion, certainty in the use of and reliance on digital signatures. Attempt will be made to set the framework for the maximum acceptance and usage of electronic signatures, and hence electronic commerce. Digital signatures utilizing the public key cryptography system have every potential to achieve the same level of legal recognition as handwritten signatures, however assistance is required from the judiciary to help attain the functional element of non-rejection. This paper deals only with the privacy implications arising in relation to digital signatures. Significant additional and different privacy issues arise in relation to message encryption keys.

Key words: digital, public key, cryptography, private key, decryption

African Journal of Computing & ICT Reference Format:

1. INTRODUCTION:

Digital signature technology grew out of a form of public key cryptography commonly known as public key infrastructure (PKI). In public key cryptography, there are two keys: a private key and a public key. When you send a document to someone, you use a private key, kept secret and known only to the sender, to digitally sign the document. When recipients receive the signed document, they use the sender’s public key, which is available to all recipients, to authenticate the document. “A digital signature is superior to a traditional handwritten signature in many ways. A skilled forger can alter the contents of a document with a handwritten signature or move a signature from one document to another [1].

With digital signature technology, any change in a “signed” document causes the verification process to fail. A third party, usually called a certificate authority (CA), is usually involved in the exchange of keys and enables the entire process. CAs certify public keys by issuing users a digital certificate that contains the user’s identity, public key, and key expiration date.” [2]. Enormous care must be invested in the development of digital signature infrastructure, and the parallel development of privacy protections.

One basic requirement of an accounting system is a reliable method to identify and validate each transaction. The cost of inadequate validation control can be staggering. For example, many businesses has
witnessed cheque fraud running into billions yearly. Internal control procedures must validate the proper authorization of transactions. In addition, adequate documentation supporting transactions needs to be maintained. Online transactions add new complexity to the accountant’s task of ensuring that only individuals with proper authorization are recording such transactions.

2. RELATED ISSUES

Traditional transactions are managed using manually written, preprinted, or electronic forms. This information is then manually transferred to other forms before the information is further processed and finally fed into the company’s general ledger. This transcription is expensive and error prone, and diverts limited resources from services to routine administration. Transcription is not necessary with paperless technology.

Nevertheless, the savings from reduced paperwork and more responsive systems come with increased audit concerns. Accountants must be especially concerned about the accuracy of information when changes to files, transactions, and temporary alterations to recurring processes are regularly made in digital form. The proper use of digital signatures satisfies the internal control needs raised by these new technologies.

Fig1 illustrates the five typical financial transactions in the purchase, payment cycle. Before Step 5 of the transaction, an accounts payable clerk needs to process the payment and verify that supporting documents related to Steps 1 through 4 have been generated and authorized by appropriate personnel. Getting approval from various individuals and verifying their signatures creates costly paperwork. It also increases the costs and time needed to process the transaction. This time directly affects productivity. Digital signatures dramatically reduce the time needed to process transactions. For example, let’s look at company A and company B, which both use digital signatures. company A wants to place an order for goods from company B. company A first sends company B an encrypted (private) purchase order (PO) and its digital signature over the Internet. company B must then be able to verify the following in order to process the purchase order:

- company A sent the purchase order.
- The purchase order was sent without error or tampering.
- company A cannot deny having sent the purchase order.

Company B can perform the validation by simply downloading company A’s public key. Just being able to locate a current certificate for company A from a trusted certificate authority (CA) tells company B that company A is a valid entity with which it can enter into a binding business agreement. After verifying the purchase order, company B proceeds to fulfill the order and ship the merchandise. B can also then transmit the packing list, proof of shipment, and invoice all signed with company B’s digital signature to company A.

When company A decrypts the message using company B’s public key, company A can be certain that the information originated with company B, has not been tampered with during transmission, and is authentic. A may then choose to make an electronic payment to B, using documents authorized with a digital signature. Since the records of all these transactions are electronic, documents can be transmitted within seconds. In addition, international transactions requiring customs documents and clearances can be processed rapidly using digital signatures.

3. METHODOLOGIES FOR SIGNATURE CAPTURE

Signature capture is a rapidly growing and mission-critical component of any business application and transaction [3]. In terms of technology, raw digital signatures are made up of a stream of five byte packets. Depending on the use of normal or enhanced mode, each packet contains a specific set of information.
Normal Mode

7 6 5 4 3 2 1 0

SYNC BYTE *0* *1*

To assist you in your decision-making process, this article details several recommended and supported digital signature processing services and file formats for signature capture. Details on compression type and level, image quality, average compression ratio and average file size are provided in addition to storage requirements for data capture services. The goal is to provide you with a guide to choosing the most effective digital signature processing services and file formats to meet your needs.

3.1 Recommended and Supported Electronic Signature Capture Formats

There are a wide variety of signature capture formats available to accommodate the heterogeneity of signature capture systems currently on the market. Many of these devices already support the capture of raw data or five byte packet (FBP) file formats, but this format is unable to store digital signatures. To provide acceptable storage capabilities, several highly recommended formats include SIG, VBC and CMP. The SIG, or signature, format is the simplest and one of the oldest signature capture and storage formats. It requires no complex compression/decompression algorithms for use. Its very light, built-in compression scheme is extremely simple to implement.

The variable bit compression (VBC) format is the most advanced compression format. This is a highly flexible format, supporting lossless and lossy compression features as well as features for storing both user-defined information and signature data. CMP, or compressed signature, is the most compact format in use today. It produces higher compression than the VBC format, but is considerably lossier. The CMP format should only be used in instances where the need for a very high compression ratio dominates the need for very high quality signature rendering.

3.2 SIG Signature Image Format

The SIG format is the most popular, portable format used today. It uses minimal compression and retains the original signature image exactly, without loss in quality. Dots-per-inch (DPI) and image size information are stored in the header for rendering purposes. However, the new VBC format is technically superior to the SIG format and should be used in most cases where the SIG format is not required. The only advantage to using the SIG format is backward compatibility with older software and systems that do not support the newer VBC format.

SIG File Object Header
BYTE ID[2]; // Inforite signature file identifier 'MP'.
WORDSigOffset; // Offset to start of signature data.
WORDSigSize; // Number of bytes in signature data.
BYTE Version; // Version number of file. Currently 2
BYTE Flags; // Status flags.
WORDWidth; // Maximum range of X values.
WORDHeight; // Maximum range of Y values.
WORDHorzDPI; // Horizontal DPI.
WORDVertDPI; // Vertical DPI.

3.3 Point Array for the Signature Data Follows the Header

WORD // Horizontal(0x4000 == new x: coordinate stroke)
WORD // Vertical coordinate (0x4000 == new y: stroke)

Each point in the array is made up of two words (32-bits in total). The point array contains the total elements specified by the "SigSize" field in the SIG file header.

3.4 VBC Image Format

VBC is a relatively new image format that works well for storing signature images. It uses an advanced image compression algorithm called Variable Bit Compression. This format compresses well and retains the exact original image, without loss in quality when the default compression level of 0 is used. DPI and image dimension information is stored in the header for rendering purposes. For applications that require the highest compression ratio with no loss in signature quality, this is the preferred signature format to use. The VBC format
also allows compression levels to be specified. The default is 0, which compresses image data without any loss. Compression levels 1-7 offer higher compression ratios, but will introduce loss to the image data and should only be used when high compression is desired over image quality. Compression level 1 offers good compression with minimal loss to image data, while compression level 7 offers the highest VBC compression but also has a corresponding higher loss of image data [4].

The VBC format is currently the only image format that supports optional encryption of the image data using 64-bit DES. Encryption of signature data is useful when security requirements restrict access to signature images. The VBC format also supports embedded user variables, which are useful when images need additional information attached to them, such as account numbers, dates, copyrights and more. Embedded user variables may be encrypted along with image data, as described above.

### 3.2 VBC Format & Features

<table>
<thead>
<tr>
<th>Predefined Variable</th>
<th>Variable Name</th>
<th>Value Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>'©'</td>
<td>Copyright</td>
<td>no rules</td>
</tr>
<tr>
<td>'a'</td>
<td>Acct No</td>
<td>no rules</td>
</tr>
<tr>
<td>'d'</td>
<td>Date</td>
<td>must be MMDDYY, where MM is the month, DD is the day and YY is the year</td>
</tr>
<tr>
<td>'e'</td>
<td>Encryption</td>
<td>type of encryption used 1 = 64-bit DES - if not specified, 64-bit DES is used</td>
</tr>
<tr>
<td>'f'</td>
<td>First Name</td>
<td>no rules</td>
</tr>
<tr>
<td>'k'</td>
<td>Encryption</td>
<td>key used to Encrypt/Decrypt a signature</td>
</tr>
<tr>
<td>'l'</td>
<td>Last Name</td>
<td>no rules</td>
</tr>
<tr>
<td>'m'</td>
<td>Middle Name</td>
<td>no rules</td>
</tr>
<tr>
<td>'n'</td>
<td>Full Name</td>
<td>no rules</td>
</tr>
<tr>
<td>'p'</td>
<td>PIN number</td>
<td>no rules</td>
</tr>
<tr>
<td>'t'</td>
<td>Time</td>
<td>no rules</td>
</tr>
<tr>
<td>'v'</td>
<td>Verification</td>
<td>reserved code**</td>
</tr>
<tr>
<td>'x'</td>
<td>Extra Small</td>
<td>reserved ***</td>
</tr>
</tbody>
</table>

* Not supported in VBC1.0. Supported only in VBC1.1 and greater.
** Reserved/not implemented in current version.

When setting the extended information of a VBC object, the variable "k" is used to set a key to lock the VBC object. For example, setting the extended information to "k87029837:a13124:location=23" will cause the VBC object to be locked using the key "87029837". If the locked VBC is then viewed, only the variable "k" will be viewable until the data is unlocked.

When reading the extended information of a VBC object, the presence of the predefined variable "k" indicates that the image and its data was locked using a key. This means that the image data and any variables contained in the VBC object cannot be viewed until the object is unlocked using the unique key that locked it. Without having the unique key that was used to lock the data, it is not possible to unlock the data.

### 3.6 CMP Signature Image Format

The CMP format compresses better than both the SIG and VBC formats. However, its header does not contain the DPI information of the signature image. The net result is that the signature's shape is altered slightly to increase the signature compression ratio. However, this makes this format a poor choice where loss of image quality is an issue. The CMP format compresses both high-resolution images and low-resolution images well.

### 3.7 FBP Format: Important Considerations

Many signature capture hardware devices support the capture of data in a five-byte-per-point format. Storage formats are transformations and extensions to the captured data. The internal format is not compressed and contains no information about the DPI or dimension of the signature image. This format should not be used for the storage of signature data.
Adding electronic signature capture to your day-to-day business applications facilitates the creation of a superior transaction-based environment, and the most important considerations to make among the recommended and supported formats are easily summarized by comparing several variables.

4. SIGNATURE, IMAGE FORMATS COMPARISON

<table>
<thead>
<tr>
<th>Format</th>
<th>Comprn Type</th>
<th>Comprn Image Level</th>
<th>Quality</th>
<th>Avg Comprn Size Ratio</th>
<th>Avg Size (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>FBP</td>
<td>None</td>
<td>N/A</td>
<td>excellent</td>
<td>1:1</td>
<td>2000</td>
</tr>
<tr>
<td>SIG</td>
<td>Lossless</td>
<td>N/A</td>
<td>excellent</td>
<td>5:4</td>
<td>1600</td>
</tr>
<tr>
<td>VBC</td>
<td>Lossless 0</td>
<td>excellent</td>
<td>4:1</td>
<td>500</td>
<td></td>
</tr>
<tr>
<td>VBC</td>
<td>Lossy 5</td>
<td>good</td>
<td>5:1</td>
<td>400</td>
<td></td>
</tr>
<tr>
<td>VBC</td>
<td>Lossy 7</td>
<td>poor</td>
<td>8:8:1</td>
<td>225</td>
<td></td>
</tr>
<tr>
<td>VBC</td>
<td>Lossy 10</td>
<td>poor</td>
<td>11:1</td>
<td>180</td>
<td></td>
</tr>
<tr>
<td>VBC</td>
<td>Lossy 14</td>
<td>poor</td>
<td>16:11</td>
<td>25</td>
<td></td>
</tr>
<tr>
<td>CMP</td>
<td>Lossy N/A</td>
<td>poor</td>
<td>10:1</td>
<td>200</td>
<td></td>
</tr>
</tbody>
</table>

Keep in mind that a comprehensive checklist of capabilities for selecting the appropriate digital signature processing services and file formats includes additional in-depth considerations. These may include analyzing software coding support requirements or even a comparison of compression algorithms.

4.1 Innovative Transaction Systems from Symbol Technologies

Symbol Technologies manufactures a range of with advanced signature capture technology and IP-enabled features for traditional and advanced payment capabilities at the retail point of sale (POS). [5] These terminals enable enhanced customer interaction and order processing. Each device offers flexible integration and is magnetic stripe, smart card and/or biometric capable. Available for a variety of retail environments, Symbol transaction systems also enable you to deliver effective targeted marketing and advertising, obtain valuable customer information, promote store loyalty, and strengthen your branding and customer relationships while increasing efficiency at the point of sale.

SIG, VBC and CMP formats are used by Symbol in its family of signature capture transaction systems. These formats were originally created by @pos, a wholly-owned subsidiary that Symbol acquired in 2002. In addition, Symbol transactions systems also support the FBP signature capture file format. Our complete line of electronic signature capture management solutions includes signature capture, compression and storage as well as signature biometric verification.

4.2 Nature of digital signatures

Asymmetric (or public key) cryptography involves two related keys, one of which only the owner knows (the 'private key') and the other which anyone can know (the 'public key'). The advantages this technology has provided are that only one party needs to know the private key; and that knowledge of the public key by a third party does not compromise security.

A digital signature is a 'message digest' (created by processing the message contents using a special algorithm) encrypted using the sender's private key. The recipient can, by re-creating the message digest from the message that they receive, using the sender's public key to decrypt the digital signature, and comparing the two results, satisfy themselves not only that the contents of the message received must be the same as that which was sent (data integrity), but also that the message can only have been sent by the purported sender (sender authentication), and that the sender cannot credibly deny that they sent it (non-repudiation).

Digital signatures are subject to a form of 'spoofing' by creation of a bogus public key that purports to be that of a particular person, but is not. In order to address that risk, 'certification authorities' (CAs) are envisaged, that will certify that a public key is that of a particular person.

5. STANDARDS AND POLICIES

In the United States, the National Institute of Standards and Technology (NIST) established a federal digital signature standard (DSS) during the period 1991-94. Many U.S. States are in the process of establishing legal frameworks for digital signatures, most of them based on Utah's legislation (1995).

The Public Key Authentication Framework Task(PKAF) Group which produced the PKAF Report contained no-one representing an institutional commitment to privacy protection (the only contender, the Commonwealth Attorney-General's Department, has complex conflicts of interests). It is therefore not surprising that its Report, while not hostile to privacy protection and recommending some valuable protections, provides inadequate consideration of the issues involved.

The following discussion will identify those strengths and weaknesses. On the closely related issue of encryption policy, no overall Australian policy has yet been released, but the OECD's encryption policy guidelines will soon be released and are likely to be influential, particularly as an Australian representative is the chairman of the Committee developing them.

5.1 Private Keys - Direct Privacy Implications

The practice is emerging of using separate key-pairs for encryption of message-content and for digital
signatures, as the PKAF Report notes [6] The draft OECD encryption guidelines insist that this distinction should be taken into account in development of national policies on access to keys (Greenleaf 1996b at 70). This separation is crucial for the protection of privacy in digital signatures, because the public interest in obtaining access to private keys used for message encryption is likely to be stronger than the public interest in obtaining access to private keys used for digital signatures.

5.2 Private key generation
A first concern relates to the manner in which private keys are generated. From a security viewpoint, it is essential that key-generation is undertaken entirely under the control of the individual concerned, and that the private key never leave the possession of that person without strong security precautions being taken. If any other approach is taken (such as generation by a service organisation, or by a government authority), serious security and privacy issues arise, because the scope exists for the individual to be convincingly impersonated.

The PKAF Report only recommends that it should require key pairs to be generated by a 'trusted process and is silent on whether individuals should be allowed to generate their own [6]. It says that any user-generated pairs would have to comply with guidelines set up by the relevant CA, 'otherwise, the key pair might not be secure'. Of course, it might also be too secure for the liking of governments. For privacy protection, individuals need a right to generate their own keys, and to not be restricted in the strength of the keys they generate.

5.3 Private key storage and backup
A further concern relates to the manner in which private keys are stored, and are backed-up, and in which backup copies are stored. Where other individuals or organizations are involved, the private key must be the subject of strong cryptography-based security precautions; otherwise impersonation risks arise from this source.

Cryptographic measures exist, or may be invented, which may make it feasible for a person to store and backup their private key with multiple individuals or organisations, in such a way that the collusion of multiple parties is necessary in order to gain access to the key. This may represent a sufficiently secure means of secondary storage.

5.4 Private key escrow
'Escrow' is an arrangement whereby something is placed on deposit with a trusted party, but may be accessed by third parties under certain conditions. It was originally used for title deeds for real property, and is used for source-code for software packages. Escrow can also be used for private keys, in which case it is referred to as 'private key escrow', which is commonly shortened to 'key escrow'.

5.5 Private key access
National security and law enforcement agencies may claim an interest in gaining access to private keys, in the sense of knowing what the key is. Since access to private keys used for digital signatures does not provide access to content of messages, or provide the only source of identification details of the holder, the reasons which would support such access seem limited. The danger of such access is, that it enables surveillance agencies to convincingly impersonate the holder of the key. It is clear from recent Australian history that there is a risk of our police and security agencies abusing such access.

Access without a warrant is inimical to privacy protection. The Telecommunications Bills 1996 at present before Parliament are allowing surveillance, agencies to issue their own public interest certificates concerning call data, and this is a bad precedent for encryption policies [7]. Warrants should be issued by a high level of judicial authority. A case should have to be made why the digital signature should not be revoked simultaneously with it being compromised through access. Otherwise, there is need for a mechanism whereby the access should be known at some later point in time, to enable the individual concerned to revoke the now-compromised key, and generate and publish a new one.

5.6 Private key revocation
When grounds exist for believing that a private key may have been compromised, the key pair must be withdrawn, or 'revoked'. This involves identification of the party who is requesting the revocation. This identification is necessarily intrusive, because the risk exists of an impersonator requesting revocation, and certification of a replacement key. This would only need to be achieved during a few key minutes in order for a fraud to be perpetrated, e.g. in relation to the purchase or sale of shares, or the transfer of funds from a bank account. The consequences for individuals of wrongful key revocation are sufficiently important that there should be legal right to compensation if a key is wrongfully revoked. Further issues surrounding revocation and Certificate Revocation Lists (CRLs) are discussed below.
6. PUBLIC & PRIVACY KEY ISSUES

It may seem strange to some that something which is intended to be a ‘public’ key, and the utility of which depends on it being known, should raise privacy issues. However, it is a commonplace of privacy policy that some of the most privacy-intrusive practices arise from the existence and/or misuse of ‘public registers’ of various types, such as the Electoral Roll, telephone books, motor vehicle registers, and council registers of building approvals. No one is yet proposing that possession of a digital signature be compulsory, and some might think its establishment of identities with one or more certification authorities than they have received to date.

Public keys are designed to be widely available, and so privacy issues will be the exception, rather than the rule. However, the privacy issues that may arise are complex and important, and deserve more consideration than they have received to date.

6.1 Certification identification requirements

There are also some potential problems that may arise in relation to the identification requirements for public keys. This is intrusive, because it requires people to expose data about themselves that they may wish to keep private. For some people (e.g. those who are stateless, or whose birth details are uncertain), it may be acutely embarrassing. The level of identification required is a significant privacy issue. The PKAF Report proposes ‘a points based scheme to establish an entity’s true (unique) identity (similar to the procedure for obtaining a passport or a bank account) based on at least two pieces of independent evidence’. It properly proposes that these details should be protected by legislative privacy principles. The PKAF Report does not seem to envisage that these details will be passed ‘up the chain’ to the PARRA, but it is considerable importnace that this be prevented.

Registers of public keys, or certificates - or both. If any central public register(s) of all public keys is maintained, then in order to sufficiently describe the person who holds each digital signature (because names are inadequate), personal information such as addresses, date-of-birth etc may be included, leading to problems of secondary uses for other purposes. We can describe such a register as a ‘positive’ register, as it contains identification information about every holder of a digital signature.

The PKAF Report does not propose any such central ‘positive’ register, but is based on a certificate system. This reduces one of the main privacy dangers, as the owner of the digital signature chooses who to send it to (accompanied by its certification). However, there is still a need for the certificate which is issued to include sufficient identification details of the holder for the receiver to be sure which person is identified by the digital signature they have received. A three way identification is needed: person - digital signature - message. The certification must therefore contain some identifying particulars of the person, and since names are ambiguous, there are privacy issues of how much other personal information (address, d-o-b etc) certification will have to contain.

An ambiguous aspect of the PKAF Report is its mention of ‘procedures for "unlisted" certificates (similar to unlisted telephone numbers in concept’ and ‘procedures for distribution of certificates to directories’. The Report says that CAs ‘may distribute certificates to a publicly available facility such as a Directory’. The extent to which ‘listing’ certificates will genuinely be optional is crucial, if there is to be no central ‘positive’ register.

6.2 Certificate Revocation Lists (CRLs) -

The PKAF Report proposes that the PARRA (Policy and Root Registration Authority) ‘[g]enerates and publishes the national and international Certificate Revocation Lists (CRLs) for and from all subordinate and peer authorities’.

This appears to anticipate a national public register of revoked digital signatures. It will be to some extent unsafe to rely on any digital signature because of the possibility it has been revoked. The only way to remove this uncertainty is to check that it has not been revoked, and the PKAF Report proposes the most ‘efficient’ method of conducting such a check: one central public register of revocations. It is possible to have no such central register, but then the recipient would have to identify the relevant ICA or OCA and check with it concerning revocation.

The PARRA revocation register is the digital signature equivalent of the Credit Reference Association of Australia's national 'negative reporting' database, or perhaps closer to the old ‘Australia Card register’ - the place you have to check before you can rely on the information you have been given. The great dangers of a central register arise from its potentials for political abuse and for surveillance. A ‘negative’ register such as is proposed for PARRA poses somewhat less dangers than a ‘positive’ register, simply because it need contain no identification details, ‘merely’ a list of revoked digital signatures.
However, it does pose two significant privacy dangers:

1. If a digital signature (or all digital signatures held by a person) could be revoked on the central ‘negative’ PARRA register (perhaps irrespective of revocation by the issuing ICA/OCA) for reasons unrelated to compromise of the signature then a person could become incapable of participation in cyberspace. The PKAF Report compares issue of a digital signature to issue of a passport, and indeed the capacity to hold non-revoked digital signature(s) will become the cyberspace equivalent of a passport, and a domestic one at that.

2. If it becomes routine for signature recipients to check PARRA for non-revocation of digital signatures, then PARRA logs will be a centralised surveillance facility, capable of indicating which cyberspace entities a person is transacting with over a period of time. To some extent the surveillance could be real-time, but more often would provide logs over time. Either way, police and other investigative agencies are likely to show a keen interest, as they already do with telephone call data held by carriers.

7. CONSEQUENTIAL PRIVACY IMPLICATIONS EXPECTATIONS OF IDENTIFICATION

There are strong pressures towards increasing expectations that members of the public should identify themselves when they conduct transactions. These pressures include:

- the technological imperative, i.e. ‘it can be done, so it should be done’;
- the marketing imperative, i.e. ‘the more that marketers know about consumers, the more efficient marketing communications will be, and the better-informed the consumer is’; and
- the social control imperative, i.e. ‘the public is not to be trusted, and data about their behaviour is essential in order to deter non-compliance and detect and prosecute offenders’.

Digital signature technology adds a new dimension to the technological armoury, because it provides apparently high-reliability identification of the individual who conducts a transaction. An early application is likely to be electronic commerce, where whichever party delivers first is interested in assurances that the other party will keep their part of the bargain. Knowing the identity of the other party is one way of gaining that assurance. It is, however, only one way; and there are ways of designing transactions such that neither party is at risk of default by the other. A particular form of electronic commerce, electronic publishing, may be another area in which identification may become mainstream. This is because period-subscriptions and multiple-issue subscriptions to digital versions of documents need to be the subject of controls. User-names and passwords are adequate in most circumstances, but high-cost and limited-distribution subscriptions may be seen to justify the requirement for digital signatures.

There are many other potential cyberspace applications. For example, bogus postings to newsgroups and e-lists, and bogus private mail, could be overcome if everyone signed their mail - although only to the extent that recipients actually used the signature to check the authenticity of the message. Chip-storage as a means of carriage of the private key Keys used for digital signatures are very long series of bits, which can be represented as long series of alphanumeric characters. Unlike Personal Identification Numbers (PINs), it is simply not feasible for individuals to remember them. They must therefore be stored in a manner which is convenient, portable, but secure.

The most likely current technology to support such storage is a chip. The chip could be embedded in a variety of carriage-mechanisms, such as a ring, watch or brooch. At present, the main form used is a plastic card. Any such device gives rise to security and privacy issues.

A fundamental concern is the means whereby the private key within the card is authorised for use. A PIN is feasible, but easily compromised. The possibility exists to store an individual’s biometric in the card, and unlock the use of the private key only if a new measurement of this matches to that stored on the chip. People are very wary of biometrics, and many of them are highly intrusive in one sense or another.

7.1 Central storage of biometrics

Even if the individual’s biometric measure remains solely on the card carried by the individual, a considerable level of security and privacy concern exists. If the measure were to be stored by a third party, even if only for the purposes of backup, then a much higher level of security and privacy concern exists. A central repository for such biometric identifiers would present opportunities for social control that are the stuff of anti-utopian novels.

7.2 Legislative Controls
The PKAF Report recommends (Appendix C: Legal Issues) implementation of the PKAF scheme via legislative standards rather than a ‘bureaucratic’ 'purpose created statutory body'. It suggests that the PARRA (to be approved by Standards Australia) would have 'some form of corporate structure ... with a widely-based membership' representing major interest groups in use of digital signatures. The only privacy protection proposed is that digital signature participants (CAs etc) would not be accredited unless they complied with the Standards Australia standard. The legislation would require the standard to provide that use of digital signatures would be voluntary, and that 'information about the holders of key pairs should be protected in accordance with privacy principles'.

This meagre consideration of privacy is inadequate on a number of counts:

1. The standards/accreditation approach, while it obviously has its uses in improving corporate behaviour, is completely inadequate as a means of creating or protection civil rights (or any other individual rights). Standards give individuals no right to obtain remedies for breaches, and threats of loss of accreditation are no substitute. There needs to be legislation providing for rights, investigation, and remedies.

2. The privacy issues, and the individual rights that are needed, go beyond the protection of personal information in accordance with existing privacy principles, as will be illustrated below.

7.3 The Privacy Act 1988's limited role - as it stands, and proposed changes

The Privacy Act 1988 (Cth) only applies to the Commonwealth public sector, with some limited extensions not very relevant here. However, the Commonwealth Attorney-General has proposed to extend its operation to the private sector (see the Discussion Paper, Privacy Protection in the Private Sector (Attorney-General's Department, September 1996), Attorney-General Williams' launch speech in 3 PLPR 81).

Extension of the Privacy Act and its Information Privacy Principles (IPPs) to the private sector will go a little way toward controlling the collection, use and disclosure of personal information used in relation to digital signatures, particularly unauthorised uses, but will have little impact on the main privacy issues as they are outside the scope of the IPPs. One main reason is that the Privacy Act's IPPs (except the collection Principles) do not apply to a 'generally available publication' (see the Act's definition of 'record'), which will exclude any registers of signatures or of revoked signatures from the scope of the Act. The second main reason is that it is not clear that the collection principles in the IPPs provide any guarantees against systems being built which require digital signatures or specific forms of digital signatures. Another reason is that the IPPs, for various definitional reasons, may fail to deal with some cyberspace transactions (see Greenleaf, 1996a). For these reasons, as discussed below, new privacy rights going beyond the IPPs are needed.

Various submissions to the Attorney-General on the Discussion Paper (see various papers in Volume 3 Nos 9 and 10 of PLPR, special issues on submissions on the Discussion Paper) have recommended wholesale revision of the IPPs, to enable them to address these issues more directly. Some of the suggestions below already appear in various submissions, particularly those influenced by the Australian Privacy Charter.

New privacy rights needed - Privacy rights in public registers

The Australian Privacy Charter, Principle 17 (Public registers) provides: 'Where personal information is collected under legislation and public access is allowed, these Principles still apply except to the extent required for the purpose for which public access is allowed' (see 2 PLPR 44 for the text of the Charter). Some such principle is needed to attempt to control the secondary uses which may be made of digital signature certificate and revocation registers. The 'under legislation' restriction may already be too narrow, given that PKAF registers are proposed to operate under standards, not under legislation.

New privacy rights needed - Identification rights

The Australian Privacy Charter, Principle 10 (Anonymous transactions) provides: 'People should have the option of not identifying themselves when entering transactions', and is subject to any justified over-riding public or private interests. This new privacy principle needs to be adopted and applied in legislation and guidelines concerning digital signatures. Some aspects of its application are given below.

7.4 A right to unauthenticated transactions

In order to prevent digital signatures, and the infrastructure that surrounds them, becoming a pervasive surveillance mechanism, it will be necessary to give individuals the right to participate in cyberspace communications without using digital signatures (ie 'unauthenticated transactions') wherever there is no strong social interest supporting the need for authentication. Some commercial transactions will probably always require authentication. Operators of some discussion lists may well justify authentication
of all messages sent to a list, because of the dangers inherent in widespread publication. On the other side of the coin, ISPs and others should never be able to require that private communications between individuals should require digital signatures. The PKAF Report recognises that use of digital signatures should be voluntary, but there needs to be legal guarantees of this, not just ‘voluntariness’ in the sense of ‘no signature, we won’t deal with you’.

7.5 Authenticated anonymity - or pseudonymity?
Even where communications must be authenticated, that does not mean they must necessarily be identified to the recipient. The PKAF Report says that PKAF infrastructure ‘may’ support anonymous certificates, and this is a helpful recognition, but individuals need a right not to be excluded from transactions because of unnecessary demands for identification. One of the central privacy struggles of cyberspace will be between the market (and surveillance agencies) that want identified transactions at all costs, and individuals who wish to resist this. The PKAF Report is really supporting a digital pseudonym, because it means certificates bound to account numbers or other indirect identifiers, but which are ‘capable of indirectly being traced to the actual user’. This recognition of pseudonymity is useful, but the important privacy issue is who will be capable of making such an indirect identification, and under what circumstances?

7.6 Multiple identities - or pseudonymity?
The PKAF Report says that PKAF infrastructure ‘must support multiple certificates or multiple keys for a single user’, referring to another aspect of pseudonymity. It is very important to individual privacy that recipients of digital signatures do not normally have the ability to aggregate profiles of the transactions that a person enters into using multiple digital identities. The obligations on CAs and others to maintain the privacy of the multiple identities a person uses, with appropriate exceptions for fraudulent or other illegal use, must be made clear.

8. RESULTS & DISCUSSIONS
Accounting and Auditing Opportunities
Digital signatures provide specific opportunities to improve internal control and the authenticity of data. It is essential that electronic, legally binding documents and transaction records be subject to a trustworthy process of authentication [8]. Without this, expensive duplication of effort will result from technology deployment, and extensive audit testing will be needed to assess data integrity. Exhibit 2 lists the roles of digital signatures in the authentication process.

These security benefits also allow a CFO to capture some cost savings through workflow efficiencies in the accounting department. These savings include:
- Reduced paper and communications costs
- Reduced transaction and administrative costs
- Reduced head count
- Elimination of process steps.

The potential savings in using digital signatures go well beyond the purchase, payable, payment cycle. Some other areas to explore are:
- Paperless contracts
- Regulatory reporting to all levels of government
- Legal documents filed with courts
- Bids on auctions
- Real estate purchases
- Legally binding consent
- Human resources functions, such as approval of vacations
- Payroll
- Supply chain transactions.

8.1 Selection of a Certificate Authority
The widespread availability of digital signatures has led to three concerns for accountants. The first concern is the selection of a reliable CA. Several choices are now available. The Big Four have started issuing digital signatures in partnership with private vendors such as Verisign. The AICPA’s Webtrust seal identifies organizations that follow its availability and control principles and meet its requirements. Companies contemplating the introduction of digital signature technology should look for such endorsements before choosing a CA.

8.2 Keeping Up With the Law
A second concern is the rapidly developing legal environment that bears on technology use. Several laws have been enacted at the state and federal level, as well as in foreign countries, to protect both parties involved in a digital signature transaction. One such law, The Electronic Signatures in Global and National Commerce Act of 2000, renders digital signatures legally binding as long as the consumer or corporate purchaser has affirmatively consented to such use and has not withdrawn such consent. The E-Signature Act does not require “any person to agree to use or accept electronic records or e-signatures.” Moreover, businesses are required to inform consumers and trading partners of the following:
- Their right to withdraw consent to accept electronic transactions
- Procedures for withdrawal of consent
The federal laws, so it is important that businesses process. Many of the state laws are more specific than federal law, and another eight have legislation in process. Many of the state laws are more specific than the federal laws, so it is important that businesses considering a digital signature-based infrastructure study state, federal, and international laws. This is an emerging area of law, and those that do not stay current could make unwitting, serious errors.

8.3 Digital Accounting Business Risk

The third area of concern is managing the new business risks introduced by digital signature usage. Digital signature technology causes a pervasive and fundamental change to business processes. As a result, both the accounting and internal audit functions must take on new tasks to protect businesses from new risks. The following are areas where existing accounting practices and expertise may have to be altered to maintain internal control:

- Regularly review all systems utilizing digital procedures, to eliminate costly duplicate manual processing.
- Conduct a quarterly review of CAs to ensure there have been no changes in policy and business practice.
- Legal counsel should review digital practices for compliance with new regulations and legislation at least once a year.
- CA and business partner agreements should be kept current and reviewed for compliance with current laws.
- Private keys, passwords, and other security information should be reviewed and updated at least quarterly.
- Monitor expenditures on digital training and processes quarterly to ensure adequate resources.
- Update storage procedures of digital files on a monthly or more frequent basis, including a test of off-site backup facilities.
- Conduct a quarterly update of digital authorizations, to avoid leaving inappropriate levels of control in place when not needed.

Developing good risk-management habits for digital signatures is an essential part of this requirement. Companies that take precautions to make sure that their digital signature program follows sound risk-management guidelines can improve their customer satisfaction and relationships with business partners. By capitalizing on the successful use of digital signatures, businesses can appeal to customers attuned to the changing economy.

8.4 Preparing for Success

There are many examples of failed digital signature implementations. Some of this can be blamed on the newness of the technology, but digital signatures mostly experience the same troubles that any systems project does. Some common reasons for failed digital signature implementation include: insufficient planning and preparation; underestimated scope of the implementation requirements; infrastructure and procedural costs; unexpected operational and technical incompatibilities with existing systems; and unclear analysis of the expected cost-benefits. Large corporations and governments have so far been responsible for pushing digital signatures in order to reduce the cost of their paper processing and filing. At the current level of adoption, companies can still obtain significant strategic advantages with a relatively fast implementation of digital signatures. Whether companies move to adopt the technology now, or wait and are forced by customers and suppliers to adopt it later, digital signatures will soon be a reality for every accounting department [10].

9. CONCLUSIONS

Digital signatures and the infrastructure within which they will operate are difficult to understand. Digital signatures will be championed by many players that the public distrusts, including national security agencies, law enforcement agencies, and consumer marketing companies. Digital signatures will be associated with increasingly intrusive expectations that people identify themselves. Digital signatures will inevitably be associated with cards. Digital signatures will inevitably be associated with biometric identifiers.

As a result, the public will be very suspicious about digital signature technologies. They will seek countermeasures and subversion opportunities. They will demand explicit privacy protections, far more substantial than the weak and patchy regime that is presently in place. The protections proposed are also quite inadequate, though promising in some respects.
Successful implementation of digital signatures and infrastructure will require far more attention to privacy issues by policy-makers and business interests.

REFERENCES