Electronic Signatures: Perspective of the CA profession

Ricky Lai
7/13/2010
# Table of Contents

- **Introduction** .......................................................................................................................... 1
  - Legal status of electronic signatures .................................................................................. 1
  - Types of electronic signatures ......................................................................................... 2
  - Purpose of this investigation ......................................................................................... 2

- **Current use of electronic signatures in businesses** .......................................................... 3

- **Risks of using electronic signatures** .................................................................................. 4
  - Authentication .................................................................................................................. 4
  - Repudiation ..................................................................................................................... 5
  - User acceptance ............................................................................................................... 5
  - Effects of the identified risks ......................................................................................... 5

- **Current state of electronic signatures as audit evidence** .................................................. 6

- **Impact of electronic signatures on auditors and the CA profession** ............................... 7
  - Overall effects of electronic evidence to auditing standards ........................................ 7
  - Evaluating the reliability of electronic signatures ......................................................... 7
  - Potential use of electronic signatures within the audit process ..................................... 9
  - Expanded role of the CA profession ............................................................................. 9

- **Conclusion** ........................................................................................................................... 10

- **Annotated Bibliography** ..................................................................................................... 11
**Introduction**

A signature represents an identification tool that enables the authentication of the signer.\(^1\) It should also be able to leave an audit trail, making the document signed non-repudiable.\(^2\) An electronic signature is essentially any representation of the signer made in electronic form.\(^3\)

**Legal status of electronic signatures**

In 2000, the Congress of the United States passed the Electronic Signatures in Global and National Commerce Act ("E-SIGN").\(^4\) This act states that electronic signatures have similar legal effects to handwritten signatures, with several noted exceptions such as evictions, foreclosures, divorce, and prenuptial agreements. The Uniform Electronic Transaction Act ("UETA") was also passed by the Virginia General Assembly in 2000, providing similar legal status to the electronic signature. Since 2000, 48 states have adopted the UETA into their respective state laws. The passing of E-SIGN and UETA suggested that the government began to identify the significance and prevalence of electronic signatures in the business environments, as well as the need to lay down laws and regulations surrounding this issue. In Canada, provincial legislature, such as the Electronic Commerce Act in Ontario, also establishes the legally binding nature of electronic signatures.\(^5\) The United Kingdom passed a law to establish the legality of electronic signatures in 2000, known as the Electronic Communications Act.\(^6\) In a review of electronic signature legislation status of 70 different countries published by Baker and Mackenzie, approximately 84% of the surveyed countries have enacted laws that equate the legal statuses of electronic signatures and handwritten signatures.\(^7\) The worldwide increase in use of electronic signatures in the business environment has led to the increased recognition and legal changes within the past decade.

---


\(^2\) Ibid.


**Types of electronic signatures**

Electronic signatures can take many forms and is a general term used to describe a signature generated electronically. They can be further classified into three different types. The first type of electronic signature is created without any control. For example, the name of the sender of an electronic mail typed at the end of the message would be created with no control to authenticate the sender. This type of signature offers no evidential value as it is very easy to duplicate without consent. An electronic signature can also be created with non-cryptographic security control. Some examples of non-cryptographic controls are the personal identification number, password, or authentication token. In a business setting involving short-term contracts, these signatures may not be effective due to the need to exchange the confidential control element in an occasion prior to the actual transaction. The third type of electronic signatures involves those created using cryptographic security techniques. These electronic signatures are also known as digital signatures. However, the terms digital signatures and electronic signatures are sometimes used interchangeably in literatures to suggest those signatures created with cryptographic security. Such a signature is commonly established using a public key infrastructure (“PKI”). The PKI consists of two asymmetric keys, where the private key is used by the sender to encrypt a message and the public key is used by the receiver to decrypt the message. This authenticates the identity of the sender of the message as the public key can only decrypt those messages encrypted using the private key, which is held only by the sender. As well, a trusted and independent third party, known as a certificate authority, would be responsible for issuance of the keys and the digital certificate on behalf of the message sender. The certificate authority acts to provide assurance over the identity of the private key owner, as well as verification of key validity.

**Purpose of this investigation**

The purpose of this report is to summarize and to analyze the current issues surrounding electronic signatures as they apply to Chartered Accountants (“CA”). The investigation will begin with an analysis on the current uses of electronic signatures by different industries, as well as the major risks faced by management in using electronic signatures. Upon understanding the business perspective to electronic signature, the current state of electronic signatures used as a source of audit evidence will be reviewed. Furthermore, the impact of electronic signatures on auditors and the CA profession will be investigated, such as the potential need for changes in audit procedures and methodologies, as well as potential roles that CAs can assume.

---

9 Ibid.
10 Ibid.
11 Ibid.
Current use of electronic signatures in businesses

Electronic signatures in the business environments have become increasingly popular. This is mainly due to the increased frequency of business communications and transactions occurring over the Internet.\(^\text{13}\) Examples of various businesses implementing electronic signatures into their workflow processes are published in different industry-specific journals.

The mortgage industry has experienced a high amount of electronic disclosure and closing documents as of early 2009.\(^\text{14}\) Ellie Mae, a company which specializes in mortgage and loan origination softwares, incorporated Wave Systems’ eSign Transaction Management Suite, an electronic signature solution, into its Encompass Mortgage Automation System.\(^\text{15}\) The result leads to the elimination of handwritten signatures and delivery costs related to mortgage documentations. As well, Wave’s system allows the transactions originated by Ellie Mae to meet the technical requirement set out in E-SIGN, UETA, and similar laws relevant to the mortgage business. Another mortgage vendor, A la mode, also recognizes the benefits of electronically signing documents for faster document review and turnaround, as well as cost-savings through the reduction in shipping bills, faxes, and paper.\(^\text{16}\) International Document Services (“IDS”), who acts as a preparation vendor for mortgage closing and disclosure documents, also recently implemented electronic signatures into their system.\(^\text{17}\) As described by IDS president Curt Doman, the use of electronic signature “gets the job done with speed and precision”, indicating that companies are adopting this technology due to the improved efficiency it can bring to transaction processes.

ClinPhone, a provider of clinical technology services, has implemented the use of electronic signatures for their offices throughout Europe and the U.S. A signature retrieval process that would have taken approximately a month can now be completed in ten minutes due to the use of electronic signatures.\(^\text{18}\) As a research direct at Gartner has also pointed out, electronic signatures can streamline workflow and


\(^{15}\) Ibid.

\(^{16}\) Ibid.


reduce costs associated with the delay and traditional handling of paper documents.\textsuperscript{19} Another clinical use example of electronic signatures is the incorporation of the CoSign electronic signature solution by GlobalVetLink (“GVL”), a web-based service provider for veterinarians.\textsuperscript{20} Veterinarians can then electronically sign forms and documents prior to sending them to the feedmills and other customers of GVL. In turn, electronic signatures decrease the paper-handling costs associated with the different documents and also increases the efficiency in passing authenticated information to GVL’s customers.

Electronic signatures are gaining an increasing importance in the documentation processes of many companies as they can be obtained much faster than traditional handwritten signature. However, most of the industries that have experienced growth in the use of electronic signatures are often related to those where signed documentations are part of the core business or workflow processes. This is understandable since the use of electronic signatures depends, from a business perspective, highly on the cost-savings it can bring to a company. Therefore, it is likely that more companies will slowly look to adopt electronic signature systems as the cost of these systems starts to decrease. In addition to the benefits and values created by electronic signatures, there is a wide variety of risks involved with implementing this technology into any business process.

**Risks of using electronic signatures**

As with any new technology, electronic signatures pose various significant risks for businesses implementing them.

**Authentication**

One of the greatest risks that can be identified is authentication.\textsuperscript{21} Authentication refers to establishing the fact that a document is sent by the apparent sender and contains information that it is supposed to contain.\textsuperscript{22} In businesses where authenticity of a document is of utmost significance, a document that is not authentic can lead to false information being passed on to its users. For example, if an electronic signature is attached to a financial statement audit report with an unqualified opinion that does not

\textsuperscript{19} lbld.
represent that of the auditor, then the users of those financial statements will face the risks of being misguided by financial statements with possible material misstatements. Therefore, businesses must ensure that the electronic signatures implemented into their business process can provide evidence to the authentication of the signed document.

**Repudiation**

Furthermore, repudiation is a significant risk for electronically signed documents. An electronically signed document is non-repudiable when there is proof that party who signed the document confirmed the content of the document. If an electronic signature cannot provide non-repudiation, it limits the validity of the transaction in question. For example, a party who sent an electronically signed contract may be able to repudiate such a contract when he/she violates the contract, if the party is able to deny having signed that specific contract. This scenario poses significant business risks for those who are looking to accept electronic signatures, as they have no protection from the violation of signed agreements.

**User acceptance**

User acceptance is another risk area that businesses face upon implementation of electronic signatures. The users involved in core business processes may include employees, suppliers, and customers. It is important that the electronic process is well established so that parties involved understand and accept the meaning of their electronic signatures. For example, customers need to understand that by clicking the check box next to the statement of “I agree” indicates that they have electronically signed an agreement. The risk involved in this case is if the users feel uncomfortable or non-accepting towards the use of electronic signatures. This may lead to potential loss of sales or bad supplier relationships. It is important for businesses to establish protocols such as exception procedures to handle specific user requests during the implementation of electronic signatures.

**Effects of the identified risks**

The significant risks associated with electronic signatures form the basis of the reliability of electronic signatures as a source of audit evidence. In order for electronic signatures to be considered effective

---


audit evidence, the risks associated with them must be assessed to determine whether they can be relied upon. First, however, the current use of electronic signatures as a source of audit evidence is analyzed.

**Current state of electronic signatures as audit evidence**

Auditors face an increasing amount of electronic documents in the current financial reporting environment, ranging from invoices sent over the internet to financial statements published electronically on regulator websites. Electronic signatures are used to assist in the electronic auditing process. When electronic signatures created with encryption technology, they can be used to ensure that documents retrieved over an electronic data processing system are non-repudiable.

In the audit of Mortgage Strategies Group, the auditor accepted electronic signatures as the original and legally binding signature on disclosure agreements after initial doubt on accepting them as audit evidence. Had the auditors insist to accept only handwritten signatures, the results of the test in question would likely fail as Mortgage Strategies only use electronic signatures for their initial disclosure agreements. The audit opinion on Mortgage Strategies’ financial statements may have been different.

Published stories of auditor’s use of electronic signature as audit evidence, such as that of Mortgage Strategies, do not appear often. This is likely due to the limited use of electronic signatures in current audits. As a result, it often represents a challenge for auditors to encounter electronic signatures presented to them as audit evidence. This is highly likely as part of a financial statement audit’s control testing, where the electronic signatures are obtained as evidence of the controls being in operation. A second factor that leads to the infrequent use of electronic signatures as audit evidence is that electronic signatures, from aforementioned analysis, are being implemented in mostly document-intensive industries such as the insurance industry and the mortgage industry. Other businesses, such as those whose core businesses depend on manufacturing or production of goods, may not be able to realize the same cost-savings benefit as the businesses previously studied. Therefore, many businesses have very little incentives currently to implement electronic signature solutions into their systems. Despite the current low usage frequency of electronic signatures as audit evidence, electronic signatures can, in the near future, have great potential impacts on the auditing process, as well as the CA profession overall.

---


Impact of electronic signatures on auditors and the CA profession

Before an attempt to evaluate the impact of electronic signatures, the overall effects that electronic evidence has on the underlying audit framework should be investigated.

Overall effects of electronic evidence to auditing standards

Technological changes in the audit environment have led to increasing auditing guidance in the U.S. In particular, SAS 80 was introduced as an amendment to SAS 31, Evidential Matter. As well, SAS 94 deals with the effect of technology on the auditor’s consideration of internal control. SAS 106, Audit Evidence, also came into effect as of February 2006 to address electronic evidence.\(^\text{28}\) In the Canadian environment, most of the standards remain technology-neutral to place emphasis on professional judgment. However, AuG-32, Electronic Commerce – Effect on the Audit of Financial Statements, was established to provide further guidance on financial statement audits for businesses where electronic evidence may be critical to the auditing process. Specifically, the guidance suggests that auditors “may test automated controls, such as record integrity checks, electronic date stamps, digital signatures, and version controls when considering the integrity of electronic evidence.”\(^\text{29}\) The changes to these standards form the backbone for the use of electronic signatures by auditors.

Evaluating the reliability of electronic signatures

In order for an audit team to rely on electronic signatures as audit evidence, several criteria needs to be established with regards to the reliability of these electronic signatures. As noted by the CICA, the main reliability criteria are authentication, authorization, integrity, and non–repudiation.

As previously mentioned, authentication is present if the signature is able uniquely identify the signer of the document.\(^\text{30}\) Auditors need to identify whether the electronic signatures in question contain mechanism that can verify authenticity. An example of such mechanism is the use of PKI.\(^\text{31}\) A properly implemented PKI is able to provide assurance over the identities of document signers. If the audit client does not have proper cryptographic controls over the authenticity of the electronic signatures, the auditors should consider whether they can further rely on the documents involved. As part of its Staff Audit Practice Alert issued in November of 2009, the International Auditing and Assurance Standards Board (“IAASB”) recommended the use of digital signatures with appropriate data encryption for audits utilizing electronic confirmation procedures, in order to provide proof of authenticity of the sender of the


\(^{30}\) Canadian Institute of Chartered Accountants. (2003). Electronic audit evidence. Toronto: Canadian Institute of Chartered Accountants.

\(^{31}\) Ibld.
confirmations.\textsuperscript{32} A recommended procedure as noted in the CPA Journal is for the auditors to select a sample of documents containing electronic signatures, and to contact the signers personally to verify that they have signed and agreed to the specific documents.\textsuperscript{33}

Authorization relates to verifying that the electronic signatures are signed by individuals who are empowered or responsible to do so.\textsuperscript{34} This has been the traditional requirement even for handwritten signatures in the audit process, and should not create significant changes to the audit procedures. For example, in an accounts receivable confirmation process, it is the auditor's responsibility to verify that the confirmation has been signed by the appropriate personnel, such as the accounts receivable clerk of the company. Authorization requires then the confirmation of consent from the entities represented by the signer, which has been a criterion for reliance on any signatures reviewed during the audit process.\textsuperscript{35}

Integrity refers to the fact that the electronically signed document has not been altered. Even though an electronic signature is not sufficient in preventing further manipulations to the documents, it should provide a clear indication as to whether manipulations occurred subsequent to the electronic signing.\textsuperscript{36} An electronic signature is only reliable if it can be added as a seal to an electronic document. Any tampering of the signed document should invalidate the signature in place, thus voiding the integrity seal. Auditors should perform testing to ensure that electronic signatures used in significant controls of business processes are capable of indicating the integrity of documents.

Non-repudiation can be tested through the confirmation between the document and the signature.\textsuperscript{37} PKI, which is able to ensure the authentication of a signature, should be sufficient in ensuring the non-repudiation of the document as well. As a signature is essentially encrypted using the same private key as the document on which it is signed, the encryption of a document with an attached signature can

\textsuperscript{32} Emerging practice issues regarding the use of external confirmations in an audit of financial statements. (November 2009). \textit{International Auditing and Assurance Standards Board – Staff Audit Practice Alert}. Retrieved from \url{http://web.ifac.org/download/IAASB_Staff_Audit_Practice_Alert_External_Confirmations.pdf} on June 9, 2010
\textsuperscript{35} Canadian Institute of Chartered Accountants. (2003). \textit{Electronic audit evidence}. Toronto: Canadian Institute of Chartered Accountants.
\textsuperscript{37} Canadian Institute of Chartered Accountants. (2003). \textit{Electronic audit evidence}. Toronto: Canadian Institute of Chartered Accountants.
confirm that the signature is acknowledged as part of the document.\textsuperscript{38} Along with the authenticity of the signature, the validity of the document would not be deniable by its signer.

The reliability of electronic signature is the pre-requisite condition for it to be used as appropriate audit evidence. Therefore, auditors will likely need to apply additional tests of controls when they are relying on electronic signatures to verify the various assertions of a transaction involving electronic documentations.

\textbf{Potential use of electronic signatures within the audit process}

Electronic signature embedded on documents of audit clients have been used as potential audit evidence. On the contrary, most auditors have yet to incorporate the use of electronic signatures into their audit methodologies and procedures. The CPA Journal suggests that electronic signatures can be used to automate the confirmation procedures often used in financial statement audits.\textsuperscript{39} The implementation of digital signatures on electronic confirmations can increase the effectiveness of the procedures, reducing the risk of forged signatures on confirmations. In addition, the efficiency of the process is improved since the response to electronic confirmations may be received much quicker than traditional paper confirmations. As audit firms implement paperless audit tools, electronic signatures can be incorporated to allow convenient preparer and reviewer signoffs as some of the larger audit firms have already implemented. In addition, engagement letters, management representation letters, and other important communications between the audit client and the auditors can also incorporate electronic signatures to validate the integrity of these documents.

\textbf{Expanded role of the CA profession}

The Big Four accounting firms have already begun issuing digital signatures as certificate authorities, in partnership with other private vendors such as VeriSign.\textsuperscript{40} This direction is certainly a potential expansion path for the CA profession. As well, the AICPA and CICA have also established WebTrust to endorse organizations with appropriate controls over their e-commerce processes.\textsuperscript{41} As electronic signatures introduce new risks into the financial reporting process, the CA profession can grasp the opportunities to help clients not only in identifying potential threats to the financial audit process, but also in exploring electronic signature solutions to improve the efficiencies of their core business and financial reporting processes. However, CA must recognize the potential competition with IT professionals who have great understandings in the technical aspect of these new technologies. CAs must differentiate themselves by


\textsuperscript{41} Ibid.
offering values achieved through the integration of these technologies for both business and financial reporting purposes.

**Conclusion**

Electronic signatures are slowly integrating into many business processes. As a result, laws and regulations have been passed to provide electronic signatures with the appropriate legally-binding status. Implementation of electronic signatures, however, depends highly on whether significant cost savings can be achieved. As such, there has been limited use of electronic signatures outside of industries where signed and legally binding documentations are integral to the business’ core processes. The risks in using electronic signatures relate mainly to the reliability of them as a replacement of the traditional handwritten signatures. Another concern in their implementation is how quickly users, such as customers, will accept the signing of documents and contracts in electronic form. As a result of the limited applications of electronic signatures in most industries, they have not been a common source of audit evidence used by auditors. The implications of applying electronic signatures into an audit mainly surround the testing of reliability of these signatures. On top of that, there is a potential for greater use of electronic signatures for audit documentations, such as confirmations and communications with management. As electronic commerce and business transactions over the Internet continue to grow in numbers, electronic signatures will likely gain a larger attention from auditors than it current has. It is important for the CA profession to periodically identify changes in standards and practices that target the technological change in the business environment.
### Annotated Bibliography

<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/website</th>
<th>Vol./No./Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, database, website, link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cashell, James D.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Annotation

The automation of the confirmation process performed for various areas during a financial statement audits may be improved through the use of digital signatures. The articles listed various past audit failures due to forged signatures, which are difficult to detect without the use of external signature experts. The use of electronic confirmation by auditors, along with digital signatures used by the respondent to confirmations, can potentially increase the effectiveness and efficiency of the confirmation process. As long as access to the private key of a digital signature encryption is safeguarded, a digital signature offers an advantage over traditional signature as they are much easier to verify. The risk of confirmation fraud can be reduced significantly, along with the legal risk of the auditor on performing the confirmation process with due care.

In the U.K., the “Electronic Communications Act” passed in 2000 establishes the legality of electronic signatures. However, regardless of its legality, the evidential value of digitally signed transactions depends heavily on the adequacy of the security environment in which the signature is applied. Some factors to consider include the identification and authentication of users and the proper generation and management of cryptographic material. As the publication describes, accountability can be strengthened through the use of digital signatures on documents. However, this is not widely used as of yet since companies need to invest in a supporting infrastructure to take advantage of this new technology. Accountability is provided through the identification of the originator of transactions, as well as the indication of the integrity of a transaction.
A signature must be able to:
- authenticate the signer;
- leave an audit trail;
- make a document “non-repudiable”.

This article describes the technology used by DocuSign, a Seattle firm which designed a system of authenticating the users through series of personal information questions. DocuSign uses no software except a web browser, thus has a great chance to overcome the failures experienced by digital signatures in the past in which compatibility of software and encryption algorithm was a key problem.

International Document Services (IDS) is a mortgage document preparation firm. It is incorporating electronic signatures into its document platform. With this technology, customers will be able to receive documents faster, allowing the process to flow more efficiently. The e-signature service can be accessed anywhere with a computer and Internet access. This results in a mortgage document, compliant with E-SIGN, that provides a full audit trail.
Use of electronic signatures is increasing for the loan closing process. Wave Systems developed an electronic signature management system for Ellie Mae, automating the many transactions without the need for faxes or delivery. The audit trail of this system is a receipt that the lender receives once the document has been signed, being then both legal and binding.

The degree of reliability for electronic signatures varies greatly depending on whether cryptography is involved. Digital signature is a security technique which allows for authentication, integrity, authorization, and nonrepudiation. In order to rely on digital signatures, the entity should have adopted adequate policies and procedures to ensure their effectiveness. The policy should outline the type of information expected to be digitally signed, as well as the choice of encryption algorithms and key management process. There has yet to be a uniform standard on this type of infrastructure on a widely accepted scale.

Electronic signature is a generic term that describes signature generated electronically and in binary form, including:

- signature created without control, e.g. typed name
- signature created with noncryptographic security technique, e.g. PIN, password, smart card, biometric ID
- signature created using cryptographic security technique, e.g. digital signature.

The publication also discusses the key components of a cryptographic electronic signature, including the public key infrastructure, and the process of creating a digital signature.

**Annotation**

As part of its recommendation to improve the security of electronic confirmation procedures, the IAASB recommended the use of data encryption, as well as electronic digital signatures to provide proof of authenticity of the sender. In this staff alert issue, digital signatures refer to the use of encryption by a key which would be uniquely linked to the signer of the document.


**Annotation**

GlobalVetLink (GVL) is a provider of web-based services of veterinarians. They have implemented ARX’s CoSign electronic signature system, which will allow them to be compliant with the U.S. FDA regulations. The employees of GVL sign the document electronically to signify that the data, such as feed directives, sent to customers have not been changed subsequent to the signing. This will reduce the cost of paper and handling of certificates for GVL.
<table>
<thead>
<tr>
<th>Author(s)</th>
<th>Title</th>
<th>Journal</th>
<th>Volume, Issue</th>
<th>Year</th>
<th>Pages</th>
<th>Date</th>
<th>URL</th>
</tr>
</thead>
</table>

**Annotation**

In the U.S., Congress passed the Electronic Signatures in Global and National Commerce Act ("E-SIGN") in 2000. It outlined the type of contracts that would be excluded under the Act, which indicates that electronic signatures have similar legal effect to handwritten signatures. Some of these exceptions are evictions, foreclosures, divorce, and prenuptial agreements. Electronic signatures have gained prevalence for most businesses, allowing paper records to be substituted entirely by electronic records. The Uniform Commercial Code of the U.S. requires signatures for sales contract with value higher than $500. If the vendor wants to obtain e-signatures deemed valid under E-SIGN, he/she must obtain consent from the customer. The article also defined electronic signature as “an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record”. A public key infrastructure allows the verification of digital signatures from a specific individual. For internal auditors, they should be aware of the range of equipment capable of providing e-signatures, as well as ensuring that their companies have the capability of verifying electronic signatures received from trading partners. The article also mentioned WebTrust as a mean of providing assurance to electronic signatures by controls which would prevent hacking and breaches of security.

Asymmetric cryptography and digital signature can be used to proof the authenticity and integrity of electronic records, thus also ensuring the reliability of these records. Authenticity refers to the fact that the document in question is what it purports to be and is sent by the person who claims to have sent it. Integrity refers to the document being complete and unaltered. Authenticity can only be shown if the identity of the document is actually established. For example, a forged document presented as a counterfeit would be considered authentic. One important point of this article is that digital signatures do not prevent manipulations of the documents. Digital signatures are only capable of indicating whether the document was or was not manipulated after signing. As well, digital signatures are time-bound by their nature as they are heavily dependent on technology. They can become obsolete due to technological changes, which may lead to problems with the storage or archival of documents.

**Annotation**

This article gave an example of how digital signatures are commonly used in a corporation.

1. Message encrypted with corporate office private key, creating digital signature for authentication and nonrepudiation.
2. Message and digital signature are encrypted with factory’s public key, providing confidential transmission.
3. At the factory, message and digital signature are decrypted using the factory’s private key to make the message readable.
4. Then the digital signature is decrypted with the corporate office’s public key, verifying the authentication and nonrepudiation of the message.
5. Any new message or modified message would go through the same series of events.

An example is specifically given for an online stockbroker communication. As part of this process, confidentiality, integrity, authentication, and nonrepudiation are achieved.


**Annotation**

The technological changes in the audit environment have led to increasing guidance under SAS80, SAS94, and SAS106. Electronic signatures are on a rising trend. As such, the Congress passed the Electronic Signatures in Global and National Commerce Act in 2002 to declare electronic signatures legally binding. Electronic signatures create a problem for auditors since there is no “physical evidence” attached to the document to declare the intention of the signer. This article recommends the auditors to corroborate through confirmation or inquiry with the signer before accepting electronic signatures as evidence to significant transactions.
|-------------|------------------------------------------|-------|-------|------|---|--------------|--------------------------------------------------------------------------------------------------|

**Annotation**

This article discusses the public key encryption infrastructure and its application to items such as digital signature, digital certificate, and certificate authority. Digital signatures indicate high authenticity as they are difficult to counterfeit, which is an advantage over traditional ink-on-paper signatures. The document or message under encryption is encrypted using a private key which identifies the creator of the document. The corresponding public key can then be used to decrypt the document, signifying that the document is created by the holder of the private key. Digital signatures are used commonly in e-commerce, with legal binding effect in Ontario, Canada (the Electronic Commerce Act).

The article goes on to identifying the appropriate management assertions impacted from the use of encrypted documents as audit evidence in financial statement audits. As well, the article provides a list of procedures which auditors should consider when assessing the effectiveness of encryption technology in assurance engagements.

|-------------------|----------------------------------|-----------------------|-----------------|------|----|--------------|--------------------------------------------------------------------------------------------------|

**Annotation**

The auditor of Mortgage Strategies Group initially challenged the use of e-signature as binding for disclosure agreements. In the end, however, the auditor accepted the e-signature as legally binding. This is consistent with most of the United States as they have not challenged E-SIGN or UETA. As e-notes and e-mortgages are becoming more common, there is an increased use of e-signatures because it is more convenient than waiting for FedEx to deliver the documents, thus providing funds to borrowers faster. Engaging in electronic processes would also prove to provide cost savings on each transaction for the lenders.
| Kerr, Stephen G. | | | | | | |
| Kuechler, William | | | | | | |
| Patel, Nilesh | | | | | | |

**Annotation**

The authors define digital signatures as the “technology that allows two parties to validate the authenticity of electronically transmitted information and documents”. This technology has been preferred by governments in allowing companies to share confidential data knowing that information will only be viewed by people that the documents were intended for. In terms of audit, digital signatures provide a new development in improving the internal control efficiency and the authenticity of data used as audit evidence. Certificate Authorities (CAs) are needed for the exchange of keys and management of the overall process. The Big Four accounting firms, acting as CAs, began issuing digital signatures in partnership with private vendors such as VeriSign. As well, WebTrust by AICPA also endorses organizations with such control and availability. Despite the advantage, digital signatures also introduce new risks to accounting and audit. Periodic review of CAs should be performed to identify any changes in policy or practice. As well, updates of digital authorization must be done regularly to eliminate inappropriate levels of controls when not needed.

| Pacini, Carl | | | | | | |
| Sinason, David | | | | | | |

**Annotation**

Weaknesses of electronic signature technologies were identified:

- The parties involved must have a prior relationship to establish a shared secret, such as the key to cryptography. However, this is difficult to establish for two parties transacting over the internet.
- The shared secret should only be known to the parties involved, though verifying the validity of the provided secret is difficult without initial face-to-face meeting.
<table>
<thead>
<tr>
<th>Author</th>
<th>Title</th>
<th>Journal</th>
<th>Volume</th>
<th>Issue</th>
<th>Year</th>
<th>Issue Date</th>
<th>URL</th>
</tr>
</thead>
</table>

**Annotation**

This article suggests that for electronic signatures to be considered audit evidence, appropriate technologies are required to ensure the issuance of a reliable electronic signing and reviewing process. In order to confirm the integrity of the signature, the signature should not be independent of the document itself. The two authors went on to identify reliability criteria for an electronic signature to be used as audit evidence, focusing primarily on the area of authentication, authorization, integrity, and nonrepudiation. As well, the controls and technologies involved with electronic signatures also affect their reliability. The federal and provincial legislations in Canada have been amended to recognize signatures on electronic documents, as well as establishing the relevant admissibility criteria for them to be legally binding.

Digital signatures can be added to indicate the integrity and authenticity of transactions recorded in the audit trail. It is used to seal an electronic document so that changes made to the document would invalidate the signature, thus preventing the tampering of signed document. ClinPhone, a provider of clinical technology services in the life sciences industry, implemented a paperless signature process across various offices to improve efficiency. A research director at Gartner also describes e-signatures as a mean to improve workflow and reduce costs. Industry regulations have also noted the trend in technological change to implement requirements which are more technology neutral or which incorporated the use of digital signatures.

An electronic signature is essentially the representation of a name made in electronic form. However, it is vastly different than simply typing out your name onto an electronic document. The article defines that all digital signatures are electronic, but electronic signatures are not necessarily digital. Digital signature offers the proof of authenticity that the document has not been modified after it has been signed. The “Electronic Signatures in Global and National Commerce Act” passed in 2000 indicates that the same legal effect can be applied to signatures made on paper or to electronic documents. The article also mentioned that at the time of writing, the most common system of digital signatures used was the public key cryptosystems.
Digital signatures can assist in the electronic auditing process. Auditors are often faced with documents sent over the internet. Without proper security controls, authentication, encryption, and nonrepudiation cannot be achieved. Nonrepudiation requires incontestable proof that the document in question originated from a specific individual or party. In this regard, electronic signature can be used, with encryption technology such as the public key infrastructure, to ensure that documents such as financial statement retrieved over an electronic data processing system are nonrepudiable.

The following significant items were noted from the survey of electronic signature legislations around the world:
- 84% of the surveyed countries have laws which treat electronic signatures the same as handwritten signatures.
- Archival of electronic signatures is not common in the countries surveyed.
- 95% of the surveyed countries do not have clearly defined laws preventing cross-border recognition of electronic signatures, therefore reducing the geographical limitations on their use.

As handwritten signature is not applicable to electronic commerce, the use of electronic signatures will increase. The major concern of these signatures relate to their authenticity (i.e. whether they actually originated from the identified signers). Potential risks include financial loss due to fraud, theft of confidential information, unauthorized use of resources, and others stated by the author.
Legal status of the digital signatures has been established by E-SIGN, giving the same legal status to e-signatures as handwritten signatures. Implementation of digital signatures is based on two components:

1. **Public key infrastructure**: two asymmetric keys, one private and one public, which is used to encrypt and decrypt the message, respectively.

2. **Certificate authority, CA**: a trusted and independent third party which issues the keys and digital certificate on behalf of the message sender. As well, CA provides assurance to the private key owner’s identity, as well as the verification of the private key’s validity.

Applications of digital certificates for auditors include the source identification of management-prepared documents and third-party confirmations, as well as the documentation of authorization for specific internal controls.

In recognition of the auditor’s expanding responsibility of providing assurance through the use of electronic media and records, the AICPA stated that the “competence of electronic evidence usually depends on the effectiveness of internal control over its validity and completeness”. As e-commerce becomes increasingly popular, legislations such as E-SIGN and the Uniform Electronic Transactions Act (UETA) establishes the legality of electronic signatures in business transactions and contracts. In respect of the due care required for an auditor, evaluation of the impact brought by technological changes and legal statutes must be made in the assessment of the client’s internal controls, as well as the planning phase of a financial statement audit.

Main question in the mind of people is the validity and legal viability of electronic signatures. The “clicking” of a box to signify agreement would fulfill the definition of an e-signature. Biggest risks faced by electronic signatures are authentication and repudiation. There is a growing popularity amongst business due to e-signature’s speed and convenience. Some noteworthy industries include banking, insurance, and online retail. Questions are asked to identify the individuals before they sign, with internal edits checking that all questions are answered accurately.