Visually Sealed and Digitally Signed Documents

Vicky Liu, William Caelli, Ernest Foo, Selwyn Russell

Information Security Research Centre
Queensland University of Technology Australia

v.liu@qut.edu.au, w.caelli@qut.edu.au, e.foo@qut.edu.au, s.russell@qut.edu.au

Abstract

One of the primary flaws with current digital signature technology is that a digital signature does not "feel" or resemble a traditional seal or personal signature to the human observer; lacking a sense of visualisation and changing each time it is applied. This paper reviews the historical value of seals in Eastern and Western cultures to provide a basis to enhance global acceptability of existing digital signatures. The functionality of traditional seals is investigated in broad terms, encompassing newly established applications to accommodate digital signature technology, and traditional seal principles. Traditional seal certificates are employed to prevent the fraudulent use of the seal and serve to bind a particular identity with a particular seal in some Eastern countries, for instance, Taiwan, Japan and Korea. This usage is analogous to the purpose of current digital certificates.

This proposal develops the concept of integrating a seal certificate into an overall digital certificate. Verification of a document by visualisation is done by affixing a visual seal within a document and then digitally signing the document. Incorporating the seal images into digital certificates ensures the integrity of the seal images applied to digital signatures. This paper defines new private extensions to the X.509 v3 certificate structure and explains the new digital signing and verifying process. The purpose of this proposed solution is to fulfil the cultural gap between traditional seals and digital signatures through the integration of culturally relevant built-in features for increasing the acceptability of digital signatures in global e-commerce, while maintaining the security features of current digital signature schemes.

Keywords: seals, seal certificate, e-commerce, digital signatures, visualisation, security, verification.

1 Introduction

Seals are universal and play significant roles in both Western and Eastern cultures. In the Bible, seals and signets were used for integrity, identification, ratification, and authority purposes. For example, in the Old Testament, Jeremiah bought the field of Hanameel from his uncle's son. Jeremiah signed the land title deed and sealed it. (Jeremiah 32:9-15) Not only does the seal represent the identity of the parties, but also evidence of consent between the parties and a legal binding to a deed. Even though the West no longer uses individual seals to the same degree, some contracts and official documentation still require and bear seals. For instance, the on-line legal dictionary, FindLaw (1996), gives a definition of "contract under seal" such as:

> ***"a contract that does not require consideration in order to be binding but that must be sealed, delivered, and show a clear intention of the parties to create a contract under seal"***

Moreover, an agreement made by deed, as opposed to a contract, requires a seal. Though seals no longer play a role in many modern individual and business situations, the principles of their function remain in all aspects of society; seals having been replaced by handwritten signatures. However, signatures and tangible ink seals are highly impractical within the e-commerce environment, so the new digital signature must reflect the individuality inherent in the signing processes they have rendered obsolete.

In Imperial Chinese history, the importance of seals is summarised in an ancient saying, "authority exists only when a seal is present; once a seal is revoked, authority perishes as well". Within the Chinese community, business and personal seals are commonly used in daily life and for business transactions. Keating (1995) reveals that a person is not required to be present to sign official documents as long as the correct seal is present. Moreover, if the individual is present but their seal is absent, the signing process cannot be carried out. Thus it is the seal that is more important. He also points out that, for business practices, the seal serves as a person's signature and when affixed in red ink is legally binding in all business issues. Both works highlight the importance of seals within Western and Chinese cultures.

Nowadays, the shift towards e-commerce is an inevitable trend. Digital signatures (Rivest et al. 1978) are designed in e-commerce to fulfil the functions of traditional seals or signatures for authentication, data integrity, and non-repudiation purposes. Historically, documents always relied on a recognisable visual stimulus for verification. However, one of the primary problems with current digital signatures is that a digital signature does not "feel" like or resemble a traditional seal to the human observer, as it does not have the same sense of visualisation. Currently, digital signatures such as the PGP (Pretty Good Privacy) digital signatures (Callas et al. 1998) are attached to the

Figure 1 an example of seal certificate

end of a computer document as a stream of binary data. These are then displayed in hexadecimal nature form which appears to the average user as a long incomprehensible string of random characters offering no sense of identity or ownership. Additionally, digital signatures change each time they are applied, unlike traditional seals that are constant personal identifiers associated with individual signatories to facilitate verification. Moreover, the image of the seal, in paper transactions, is indelibly attached to the document.

The current digital signature overlooks the importance of visualisation and sense of personal identity and ownership in many cultures. To overcome the cultural gap between the traditional seals/signatures and digital signatures, this work investigates seal cultures in the context of digital signatures, identifying the need to develop a new culturally friendly, visual digital signature. This proposal makes the currently intangible digital signature virtually tangible; i.e., it incorporates visualisation into the current digital signature practice. The purpose of this work is to increase the acceptability of digital signatures in global e-commerce while maintaining the security features of the current digital signature.

In section 2, previous related works are examined. These include a discussion of the cultural issues associated with existing digital signature schemes, in section 2.1; an analysis of the related work based on pre-existing principles of traditional seals, altered to serve contemporary functions within the digital signing environment, in section 2.2; and then an illustration of traditional seal certificates in relation to public key certificate X.509 (ITU-T 2000) is given in section 2.3. Section 3 consists of the proposed extensions to the X.509 certificate and offers an explanation of the new signing and verifying process. The analysis of this work is incorporated in section 4. Finally, the conclusion is drawn and future direction for work is discussed in section 5.

2 Related Work

2.1 Digital Signatures with Cultural Issues

Fillingham (1997) believes traditional signatures will not be completely replaced by digital signatures, given the limitations of digital signatures. These limitations include for instance, long-standing retention issues in terms of the deterioration of the associated storage media, obsolescence of the data format and the evolution of cryptographic algorithms, related standards and certificate validation. He also maintains that digital signatures will never be used in ceremonial or historical events, although this may be accepted. Lutterbeck (2000) states digital signatures fail to meet high expectations for their success due to the simple flaw that they overlook cultural factors. He advocates that before digital signatures can prevail, an appropriate sense of culture must be incorporated into digital signatures in terms of user acceptance and long-term stability and reliability. Lutterbeck believes that the culture of seals in Japan is well suited for the implementation of digital signatures, since the concept of seal certificates and electronic certificates are comparable. Both Fillingham and Lutterbeck investigate the use of traditional seals/signatures and expose the flaws in current digital signatures. However, their work fails to exploit the concept of traditional seals/signatures to innovate a culturally friendly digital signature regime.

2.2 Digital Signing within Existing Trust Based Environments

There is at least one major form of attack on current digital signature schemes; i.e., the document displayed to the signer may be different from the actual one signed. This has been called the “What you see is what you signed” or WYSIWYS problem (Spalka et al. 2001). Researchers at Hewlett-Packard (HP) Laboratories, Balacheff et al. (2001), answer this type of attack by deploying an additional piece of tamper resistant hardware, the Trusted Displayed Controller (TDC), with its own display circuitry and cryptographic functions in a computer system. A TDC

controls the platform's screen, preventing software from learning the specifics of displayed data. Once the TDC is authenticated by the signer's smart card, the signer can trust the platform to perform digital signing.

HP employs a trusted image, which they call a "seal", stored in the smart card that the TDC will display as a background or a border. Under normal circumstances, one computer has only one display screen, hence this seal is used to indicate to the signer that the TDC is controlling the display that users are signing with their smart cards. Microsoft's NGSCB (Next Generation Secure Computing Base) (Carroll et al. 2002) proposes a similar solution to resist Trojan Horse Viruses. NGSCB provides the regular Windows environment as well as a trusted processing environment that enables users to perform confidential tasks while protecting data from being read or written by non-trusted applications. To allow the user to distinguish between a secure window and an unsecured window, the secure window will include a recognisable image or information displayed within a border.

Both HP's (Balacheff et al. 2001), and Microsoft's (Carroll et al. 2002) proposals use a recognisable symbol only known to the signer, referred to as a "seal", for verification of a secured environment on the screen display. This seal is displayed on the screen along with the data that is to be signed, so that the signer can be confident that he/she is working in a highly trusted environment. HP's solution also suggests that the signer needs to change the seal image periodically to prevent the image from being compromised. Their idea of a seal is not a constant token associated with the signer; they use the principles of traditional seals but for a different purpose. The private image is purely a security verification scheme and takes no place in an actual document or transaction. Our proposed seal images are permanent fixtures of digital signatures; functioning as a constant visual token associated with the signer and a document, just like a traditional seal for signing and verification. The Certificate Authority (CA) digitally verifies the integrity of the seal as discussed below in section 4.1; therefore the signer is not required to periodically update their seal images.

2.3 Traditional Seal Certificate

Formal documents are sealed in lieu of being signed as part of Chinese custom and culture. Seal certificates are the integrity mechanism employed for prevention of fraudulent seal use. Seal certificates are adopted in Asian countries, such as Taiwan, Japan and Korea, functioning as a notarisation or witnessing activity in the signing process to provide reasonable evidence of authenticity to the general public. Prior to Taiwan abolished the seal certificate system in July 2003 (Chinesetimes 2003), execution of some legal documents required the presentation of the registered seal and the seal certificate, such as in stock assignments and real estate transactions. Figure 1 shows a seal certificate that proves the binding of the seal owner's identity to the registered seal through endorsement by the seal of the Registration Authority and the seal of the Registration Authority executive. The elements of the seal certificate in Figure 1 include: (1) the name of the jurisdictional household registration authority, in this case the Ling-Ya Judicial Area Household Authority, (2) seal owner information including name, date of birth, ID number and address, (3) the owner's seal, (4) seal registration date, (5) the seal of the issuing authority, namely the seal of Ling-Ya Household Authority, (6) the seal of the relevant executive of the Authority, and (7) certificate issue date. The function of a seal certificate is to authenticate the signer through a trustworthy third party similar to the CA within a Public Key Infrastructure (PKI).

2.4 Digital Certificate

A digital certificate consists of a data structure for binding subjects to public key values and is digitally signed by a trusted third party. There are various types of digital certificates (also known as public key certificates), such as, PKIX X.509 (ITU-T 2000), PGP certificates (Callas et al. 1998) and SPKI (Simple Public Key Infrastructure) certificates (Ellison et al. 1999). The X.509 v3 certificate is the most prevalent type in the marketplace, boasting comparable features to a seal certificate. Thus, this paper concentrates on the proposal for new extensions to the X.509 v3 certificate. The extensions of X.509 v3 are used to convey additional attributes associated with users or public keys and for certificate hierarchy management. Each extension in a certificate is attributed as critical or non-critical. When an extension is assigned as critical, it must be recognized by the relying party, otherwise the certificate is rejected. A non-critical extension may, however, be ignored if it is not recognized. Extensions to X.509 v3 include standard and private extensions that can be defined for specific use by communities. This proposal aims to define a specification for a visualised X.509 certificate by use of these private extensions, which are compatible with PKIX requirements.

3 Solution

Existing digital signature schemes overlook the impact provided through visualisation as a force for detection and communication. In particular, when the seal itself is visually recognisable on a global scale, for example, the trademarks of Coca Cola and McDonalds, the verifier can accept the signatory's seal in a confident and expedient manner. This paper exploits the concept of traditional seals and seal certificates prevalent in some seal-culture countries, like Taiwan, to develop the visualisation of digital signatures. Explicitly, the primary purposes of this work are to visualise current digital signatures and digital certificates. The X.509 v3 certificate allows communities to define private extensions to carry distinctive information. This paper defines two data structures, including the subject's seal and issuer's seal in X.509 v3 private extensions, to support the proposed visualised digital signature scheme. Thus visualised digital signature applications will be able to accept visualised digital certificates for use. The visualised digital certificate is defined in accordance with X.509. As stated by RFC3280, the extension specifications of X.509 v3 each include an OID (Object Identifier) and an ASN.1 (Abstract Syntax Notation One) structure. The OIDs of the extensions proposed in this work could be registered with a

registration authority and lead in to the following. In the next section, we will define these ANS.1 structures for the seal of the subject and the seal of the issuer, and then show the new signing and verifying processes using these innovations.

3.1 Structure of Subject's Seal

This sub-section specifies the format and content of a subject's seal as one of the proposed private extensions to X.509 v3 in relation to RFC3280. The concepts are based upon standard legal practice in Taiwan as these seem to have universal applicability. The structure of a subject's seal contains the seal type, authorising authority, creation date, seal creator, description, file format, seal name, file name and the contents of the image file. When the image and its related information are presented to the issuing CA for verification, the subject's seal type identifies whether the subject's seal is a personal, corporate, governmental or application seal. If the seal type is not personal, the authorising authority must be present to reveal who authorised the creation of the seal as a record of accountability. The seal creator's identity is also included for liability purposes should a challenge arise. Since the seal owner may apply different seals for various purposes; the name of the subject seal allows the specification of the of each seal's identity. Other relevant comments can be placed into the description field. There are various graphic formats available to present a seal, thus file format is a critical attribute to specify the image format used in the data structure of the subject's seal. The data stream of the seal image is the essence of the subject's seal. The file name forms part of the seal image of the integrity needs for the seal image, making their verification by the issuing CA essential. The contents of a subject's seal are given in Figure2.

```
 SubjectSeal              ::=  SEQUENCE
{
  subjectSealType           Sealtype,
  authorisingAuthority      Name       OPTIONAL,
  subjectSealCreatedDate    Time,
  subjectSealCreator        BMPString,
  description               BMPString OPTIONAL,
  subjectFileFormat         Imageformat
  subjectSealName           BMPString OPTIONAL,
  subjectSealFileName       UTF8String,
  subjectSealDataStream     BIT STRING,
}
Subjectsealtype       ::= BIT STRING
{
   personal                 (0),
   corporate                (1),
   governmental             (2),
   application              (3)
}
Imageformat           ::=  CHOICE
{
   jpeg            [0]     GraphicString,
   gif             [1]     GraphicString,
   bmp             [2]     GraphicString,
   tiff            [3]     GraphicString
}
Time                  ::=  CHOICE
{
   utcTime                  UTCTime,
   generalTime              GeneralizedTime
}
```

Figure2 data structure of subject's seal

A description of each field is given below:

- **subjectSealType:**

  This field identifies the particular seal from a list of alternative types of seal including personal, corporate, governmental and application.

- **authorisingAuthority:**

  When the value of subjectSealType is "personal", then the authorisingAuthority field is not required; since normally the creation of a personal seal does not require the approval of authorities. The authorisingAuthority field must be present if the subjectSealType field is not set to "personal", to specify who authorises the creation of the seal as a method of accountability. Corresponding to RFC3280, the two basic certificate fields of X.509 v3, issuer and subject, are defined as the X.501 type Name, which is identical to this authorisingAuthority field.

- **subjectSealCreatedDate**

  This field specifies when the seal image was created. It is defined as a Time type that has a choice of UTCTime or GeneralizedTime as the ASN.1 standard for dates and time.

- **subjectSealCreator**

  This field is a string identifying the seal's creator as a record for any accountability needs. It is classified as a BMPString type. In fact, BMP (Basic Multilingual Plane), defined in (ISO/IEC 1993), is designed to convey special characters in all scripts, for instance, Latin, Cyrillic, Greek, Arabic, and Han. RFC 3280 states that BMPString is one of the subtypes of the UNIVERSAL types of strings in 1988 ASN.1.

- **description**

  The description field is an optional string that contains specific comments on the subject's seal.

- **subjectFileFormat**

  The seal image types that this work proposes are the current major image types available and compatible with most computer platforms, applications, and common Web browsers; including GIF, JPEG, BMP and TIFF (CDL 2003). The image sizes of GIFs and JPEG type data records are more compact than TIFFs and BMPs, making them well-suited to be candidates for onscreen seal images while minimising transmission latency. However, while JPEG compression provides a larger compression ratio for images than other types of compression, the original detail of an image is unrecoverable once the image has been compressed. Generally, a seal image can be a monochrome impression bearing the user's mark or the name and thus does not require the provision for millions of colours. Thus the size of seal images is usually relatively small. TIFF and BMP formats are also included among the choices for seal image types and are provided the conforming applications can recognise these image data type.

- **subjectSealName**

  This field is an optional string that allows specifying the identity of the seal, particularly when the seal owner may possess multiple seals.

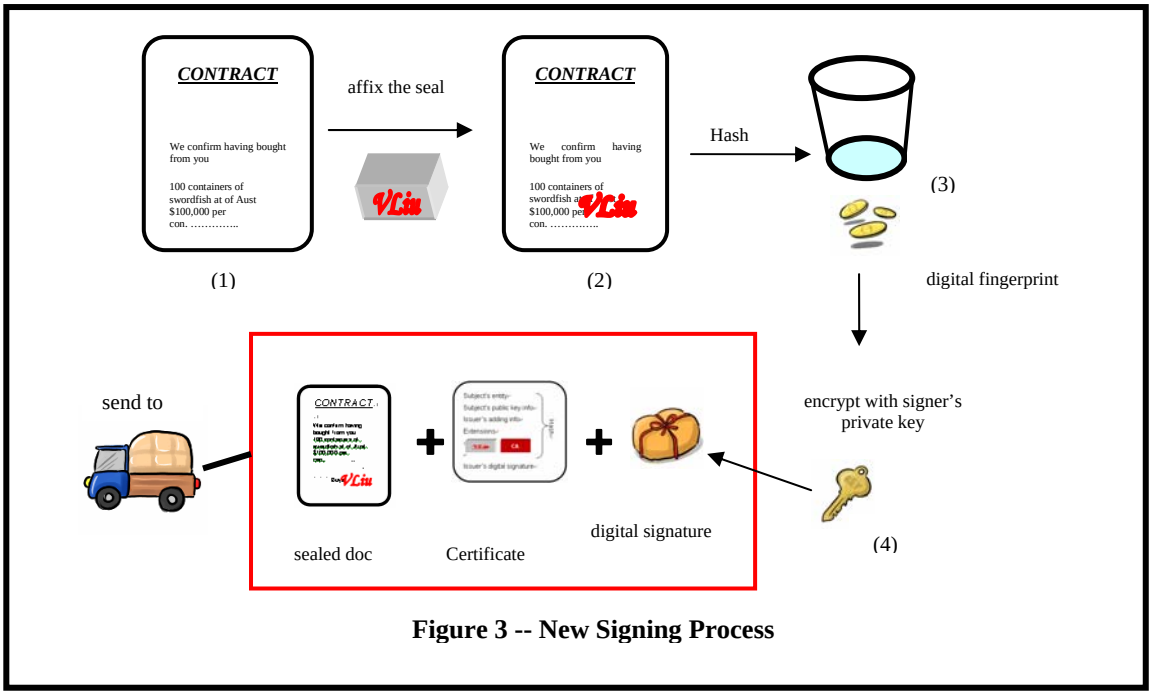

Figure 3 -- New Signing Process

- **subjectSealFileName**

  Corresponding to RFC 3280, all certificates issued after December 31, 2003 MUST use the UTF8String encoding of DirectoryString. Thus, this field is an UTF8String that specifies the file name of the subject's seal.

- **subjectSealdDataStream**

  This field contains the data content of the subject's seal image.

3.2 Structure of Issuer's Seal

The issuer's seal is displayed on the visualised digital certificate with the subject's seal for testimony, which is comparable with the traditional seal certificate that the issuing authority's seal is applied to as a testament to the owner's seal. This sub-section denotes the data structure of the issuer's seal as another proposed private extension to X.509 v3 (RFC3280), including seal creation date, seal creator, description, file format, seal name, file name and the contents of the image file. The creator and created date of the issuer's seal are retained as a record of liability. The certificate issuer may have various seals for use; therefore the identity of the seal can be given in the name of the issuer's seal field. A number of different types of graphic formats exist; hence it is important to indicate the image format in the specification. The data stream of the seal image is the principle element of this data structure. The file name is part of the integrity needs for the issuer's seal. The issuer itself digitally signs them. The structure of the issuer's seal is given in Figure4.

```
Issuserseal              ::=  SEQUENCE
{
  issuerSealCreatedDate     Time,
  issuerSealCreator         BMPString,
  description               BMPString OPTIONAL,
  issuerSealFileFormat      Imageformat,
  issuerSealName            BMPString OPTIONAL,
  issuerSealFileName        UTF8String,
  issuerSealDatastream      BIT STRING
}
```

Figure4 Data structure of issuer's seal

A description of each field is given below:

- **issuerSealCreatedDate**

  The description of this field is similar to the subjectSealCreatedDate field described above.

- **issuerSealCreator**

  This field corresponds to the subjectSealCreator field of the subject's seal structure.

- **description**

  This field is an optional string that contains specific comments regarding the issuer's seal.

- **issuerSealFileFormat**

  This field corresponds to the subjectSealFileFormat field of the subject's seal structure.

- **issuerSealName**

  This field is an optional string that specifies the identity of the issuer's seal when the issuer may own multiple seals for various reasons.

- **issuerSealFileName**

  This field is an UTF8String that specifies the issuer's seal name .

- **issuerSealDatastream**

  This field contains the data content of the issuer's seal image.

3.3 A New Digital Signing Process

A seal image can be generated by any image-editing program or through a scanner. The contents of a seal image can include an impression bearing a mark or a name, like the inscriptions used to generate traditional seals, which is a distinctive and recognisable constant token to the signer. The seal image and its related information containing seal type, seal authorising authority, seal creator, relevant description, seal image format, seal size

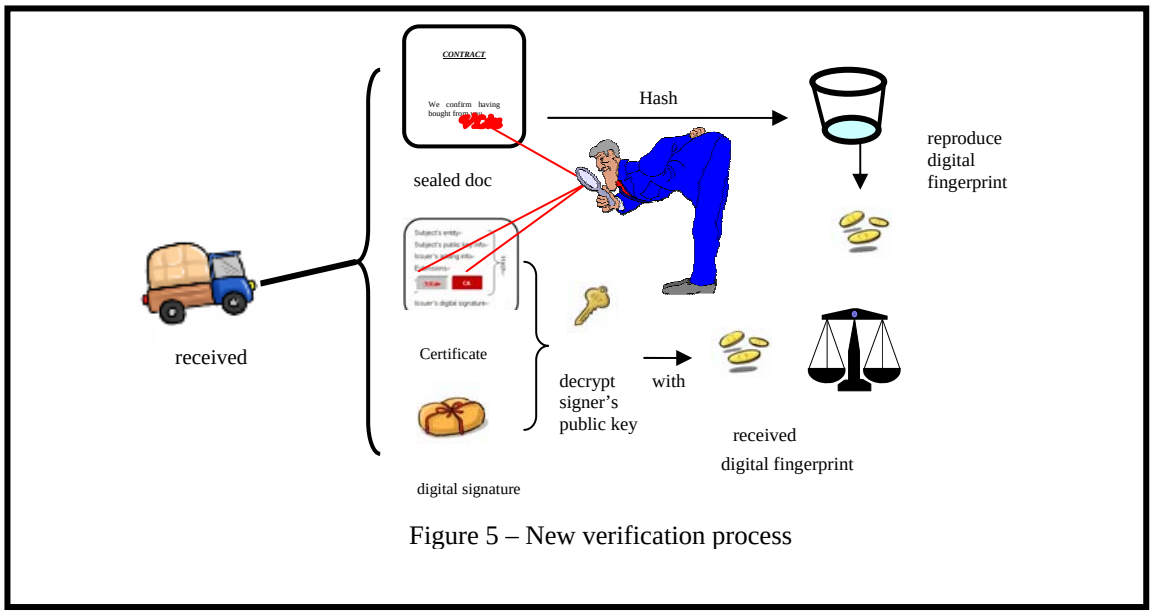

Figure 5 – New verification process

and seal file name are presented to the issuing CA for registration. After the CA certifies the seal image, the new public key certificate is issued, and the seal image can be incorporated into the digital signature. As figure3 illustrates, the process of creating a visually sealed and digitally signed document consists of:

Step 1: create a document in a word processing program, for example;

Step 2: importing the registered signer's seal image into the text to affix the seal to the document;

Step 3: placing the visually sealed document into the hash function to produce the message digest code, that is, its "digital fingerprint";

Step 4: encrypting the digital fingerprint with the signer's private key to generate the digital signature

This is analogous to the traditional paper-based signing process; in which a seal is affixed upon a document, and thus it's content, that is obvious to the signer. This new signing process is designed to simulate traditional signing techniques incorporating visualisation into digital signing. In seal-culture societies, when parties want to formalise a contract, the seals are affixed and the seal certificates are also attached to the contract for authentication, data integrity and non-repudiation purposes. By the same token, with the new digital signing process, the public key certificate is transmitted with a visually sealed and digitally signed document for the same purposes.

3.4 A New Digital Signature Verification Process

Figure 5 depicts the new signature verification process. The new signature verification process is analogous to the traditional, sealed paper–based document with the seal certificate for verification attached. When the recipient receives a visually sealed and digitally signed document with an associated digital certificate, the recipient immediately perceives the claimed signer's seal on the document, particularly when the signer's seal is recognisable to the verifier. This would be the case, in particular, where regular business transactions between parties occur. Importantly, the signatory's digital certificate, signed by the CA, should be displayed on the screen along with the received sealed and signed document to facilitate verification. The recipient then verifies the document in the same way as a digital signature, which is to place the received signed document into a hash function regenerating the digital fingerprint. The digital signature is decrypted with the signer's public key to restore the digital fingerprint generated by the signer. If two digital fingerprints are equivalent then the document is authenticated, otherwise the document has been altered during the transmission.

The signer's seal image on the signed document greatly increases the verifier's confidence that the signed document is from the originator. Furthermore, both the issuing CA's and the signer's seal images on the public key certificate instill confidence that the signer's public key is attested to by the CA, unlike the current digital signature's verification process of presentation of long meaningless hexadecimal strings to the verifier.

4 Analysis

This section evaluates the quality of service of this proposed visualised digital signature and visualised digital certificate scheme with respects to integrity, security, interoperability, and performance.

4.1 Integrity

Public key certificates provide assurance that the public key is associated with a particular entity. By the same token, the strategy of ensuring the integrity and authenticity of seal images is to employ public key certificates. This is the mechanism binding the visualised seal image and other related seal information in addition to the public key and other associated information to the declared entity, before it is digitally signed with the private key of the issuing CA. Figure 6 compares the structures of a current certificate and the new proposed certificate. The

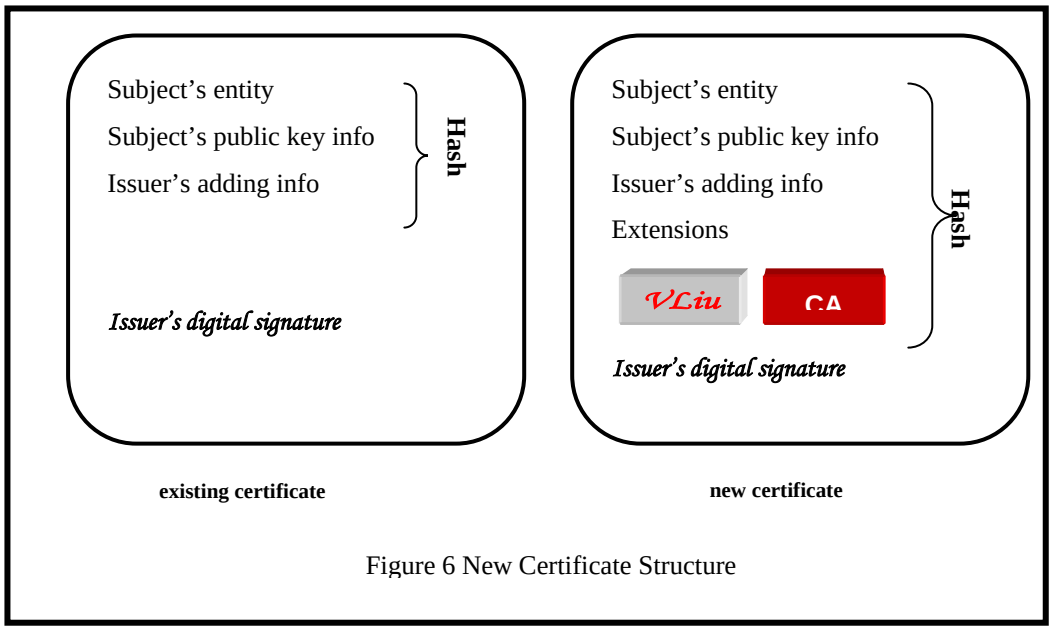

Figure 6 New Certificate Structure

newly designed public key certificate comprises the original three components together with the subject's identity, subject's public key, and issuer's added information as well as the extensions including:

- the subject's seal image and the seal related details containing seal type, seal authorising authority, seal creator, relevant description, seal image format, seal size and seal file name, and
- the issuer's image and its seal related information.

The four components are hashed and then signed by the private key of the issuer to ensure the integrity of the subject's public key with the designed visualised seal images.

4.2 Security

This proposal still requires the verifier to execute the digital signature verification process to validate the received visualised digital signature instead of only relying on the visual tokens for verification. Moreover, this proposal maintains the security features of current digital signature schemes, hence potential form of attacks on digital signature applications may still arise, such as, the WYSIWYS problem (Spalka et al. 2001) and a Signature Stripping attack (McCullagh et al. 2001), (i.e., a digital signature can be removed without leaving a trace and replaced with a new one by a fraud). Actually, our solution does not prevent the occurrence of Signature Stripping attack. However, the visualisation of digital signatures makes a Signature Stripping Attack harder to deploy, since people are much better at identifying a visual symbol on a signed document. Likewise it is easier to use a certificate with the issuer's and signatory's seal images for verification than attempting to verify an existing digital signature without any tangible visual stimulus.

4.3 Interoperability

According to RFC 3280, each extension in a X.509 v3 certificate is attributed as critical or non-critical. When an extension is assigned as critical, the relying party, as a result of rejecting the certificate, may not recognize it. The proposed visualised seal images are integrated into the private extensions of X.509 v3. Hence, to prevent loss of interoperability, the assignments of the proposed visualised seal data fields in the extensions are marked "non-critical".

4.4 Performance

Two proposed private extensions containing subject's and issuer's seal images are incorporated into theX509 v3 certificate, which may cause slightly more transmission latency than the current transmission of the existing public key certificate. In order to minimise the transmission latency, a compact size for image formats is desirable. However, high compression ratio of some image formats that result in a loss of the fidelity of the original image should be carefully evaluated when selecting the seal image format. Generally a seal bears a mark or a name, which does not require the provision of millions of colours; thus the sizes of seal images should generally be relatively small, e.g., the digitised form of a manual signature made in black ink. In addition, transmission bandwidth is increasing with evolving technology, effectively nullifying this small increase in latency. Therefore, the integration of visualised seal images into digital signatures and digital certificates should not be a major issue for transmission.

5 Conclusion and future work

Previous work addressed the cultural gap between digital signatures and traditional signatures/seals. However unsolved cultural issues still remain with regards to the use of modern digital signatures within these societies. Other work has referred to a visual "seal" or image as a verification of the trustworthy nature of a screen display, not as a constant token associated with the signer. These schemes do use the principle of traditional seals but for different purposes. This work bridges the cultural gap between traditional seals/signatures and modern digital

signatures and allows the signer to embrace the consistency of the digital seal. This research examines the historical values and applications of seals in Western and Eastern cultures and resolves the cultural issues by emulating the traditional signing and verification techniques within the digital signing process. Not only do we propose a visualised digital signature, but also that a new public key digital certificate contain the issuer's and signatory's seal images to facilitate verification. This work makes existing intangible digital signatures and digital certificates virtually tangible, which will greatly increase user acceptability of digital signatures among the global populace.

The mechanism of ensuring the integrity and authenticity of seal images is to incorporate the signatory's seal image into the X.509 v3 certificate in relation to RFC3280. Explicitly the public key, the seal image and associated information are digitally signed by the issuing CA. New extensions to the private extensions of X.509 v3 are defined, including the data structures of both the subject's seal and issuer's seal. The proposed private extensions may not be recognised by the verifier's system; hence the assignments of the proposed visualised seals in the extensions are marked "non-critical", to prevent loss of interoperability. It is suggested that the visualised seals be incorporated into X.509 v3 certificates, but not be limited to X.509 v3. With further study, this design may be also be incorporated into other types of certificates, such as, SPKI certificates, PGP certificates, Attribute certificates, and Cross certificates (RFC3280), where appropriate. This work exploits the concept of traditional seals and seal certificates to develop visualisation of digital signatures. Nevertheless, the proposal emanating from this research does not add undue complexity and still maintains the original security features of the existing digital signatures. At present, this paper defines the data structures to X.509 v3 extensions, a prototype system will be developed and be evaluated for future study. Finally, while this paper may appear to target only those communities and business/legal practices where a visual "seal culture" applies, the visualisation of modern digital signatures is also appropriate within cross-culture communities, just as traditional seals are universal.

6 References

Balacheff, B., L. Chen, D. Plaquin and G. Proudler (2001): A Trusted Process to Digitally Sign a Document. *New Security Paradigms Workshop 2001*, Cloudcroft, New Mexico, USA, **NSPW '01:** 78-86, ACM.

Callas, J., L. Donnerhacke, H. Finney and R. Thayer (1998): OpenPGP Message Format. Internet Request for Comments 2440

Carroll, A., M. Juarez, J. Polk and T. Leininger (2002): Microsoft "Palladium": A Business Overview. Microsoft Content Security Business Unit

CDL: California Digital Library Digital Image Format Standards, California Digital Library (CDL) http://www.cdlib.org/about/publications/CDLImageStd-2001.pdf. Accessed 3 April 2003.

Chinesetimes: e-Yam Chinesetimes, Chinese Times Inc. http://forums.chinatimes.com/report/new0101/seal4.htm**.** Accessed 17 January 2003

Ellison, C., B. Frantz, B. Lampson, R. Rivest, B. Thomas and T. Ylonen (1999): SPKI Certificate Theory. Internet Request for Comments 2693

Fillingham, D. (1997): A Comparison of Digital and Handwritten Signatures. *Ethics and Law on the Electronic Frontier* **6.805/STS085:** Student Papers, Fall 1997

FindLaw: Merriam-Webster's Dictionary of Law, Merriam-Webster's Incorporated. http://dictionary.lp.findlaw.com/scripts/results.pl?co=www.findlaw.com&topi... Accessed 15 Jun 2003.

Housley, R., W. Ford, T. Polk and D. Solo (2002): Internet X.509 Pulbic Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile. Internet Request for Comments 3280

ISO/IEC 10646-1: (1993): International Standard Information technology -- Universal Multiple-Octet Coded Character Set (UCS) -- Part 1: Architecture and Basic Multilingual Plane.

ITU-T (2000): Recommendation X.509. Information Technology--Open Systems Interconnection -- The Directory: Public Key and Attribute Certificate Frameworks.

Keating, J. F.: Chinese Seals Business and Art, Vision International Publishing Co. http://sinica.edu.tw/tit/arts/0496_Seals.html. Accessed 5 Jun 2001.

Lutterbeck, B. (2000): Governing Legal Identities Lessons from the History of Seals and Signatures. *the Information Security Solutions Europe Conference*, Barcelona Informatics and Society, Technical University Berlin.

McCullagh, A., W. J. Caelli and P. Little (2001): Signature Stripping: A Digital Dilemma. *Journal of Information, Law and Technology* **2001:** 1

Rivest, R., A. Shamir and L. Adleman (1978): A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. **21: 2**120-126, Communications of the ACM.

Spalka, A., A. B. Cremers and H. Langweg (2001): The Fairy Tale of What You See Is What You Sign - Trojan Horse Attacks on Software for Digital Signatures. *IFIP WG 9.6/11.7 Working Conference*, Bratislava / Slovakia, **SCITS-II: June 2001** Security and Control of IT in Society-II.