

Graphical and Digital signature Combination for fulfilling the cultural gap between traditional signature and current smart card digital certificate/signature

Nazar Elfadil

College of Engineering, Sultan Qaboos University, Oman

nazar@squ.edu.om

Abstract

This proposal develops the concept of combining a handwritten signature, digital signature, and a smart card into an overall Public Key Infrastructure (PKI). The purpose of this proposed solution is to fulfill the cultural gap between traditional digital signatures and current smart card digital certificate/signature. It is achieved through the integration of culturally relevant built-in features for increasing the acceptability of digital signatures and smart cards in global e-government/e-commerce, while maintaining the security features of current digital signature/certificate schemes.

1. Introduction

Nowadays, the shift towards e-commerce is an inevitable trend. Digital signatures [1] are designed in e-commerce to fulfill the functions of traditional signatures for authentication, data integrity, and non repudiation purposes. Historically, documents have always relied on a recognizable 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 signature to the human observer, as it doesn't have the same sense of visualization. This is because digital signatures are attached to the end of a computer document as a stream of binary data. These binary data are then displayed in a hexadecimal nature form which appears to the average user as a long incomprehensible string of random characters offering no sense of identity or ownership.

The current digital signature overlooks the importance of visualization and sense of personal identity and ownership in many cultures. To overcome the cultural gap between the traditional signatures and digital signatures, this work investigates signature cultures in the context of digital signatures, identifying the need to develop a new culturally friendly, visual digital signature that can be imbedded into a smart card.

1.1 Digital Signatures with Cultural Issues

There are many reasons, why signatures are the best and most popular means of authentication. Signature is an active biometric characteristic that is never given by accident. A signature is characterized by personal physiological and biomechanical capabilities and individual learning processes. That is what significantly differentiates a signature from passive biometrics in body characteristics such as finger, hand, face or even iris. Every signature is unique. The comparison automatically takes into account the natural variations in the characteristics of a signer

Fillingham [2] believes that traditional signatures (handwritten 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. Lutterbeck [3] states digital signatures fail to meet high expectations for their success due to the simple flaw that they overlook cultural factors.

1.2 Digital signature/Certificate

Digital signature/certificates and their associated keys are predominantly used by Web browsers and e-mail clients for security functions such as user authentication and digital signatures. Therefore, they need to be stored where they can be conveniently retrieved to be used for these functions.

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 [4] and SPKI (Simple Public Key Infrastructure) certificates [5].

Certificates are digitally signed by the issuing certification authority (CA), and they can be issued

for a user, a computer, or a service, (which provides authentication) or a Smart Card User certificate (which provides authentication plus other uses of the smart card cryptography) unless a system administrator has granted the user access rights to the certificate template certificate template.

1.5 Digital and Handwritten Signatures Comparison

1.5.1 Digital and Handwritten Signatures Similarities

Handwritten and digital signatures share some similarities:

- Both provide the security services of authentication, data integrity, and non-repudiation.
- Both handwritten and digital signatures have legal standing, and the legal standing of digital signatures is increasing with the passage of various state and national laws to become the equal (or more) of handwritten signatures.

1.5.2 Digital and Handwritten Signatures Differences

Differences between digital and handwritten signatures include:

- ✚ A handwritten signature is biologically linked to a specific individual, whereas a digital signature relies on the protection afforded a private signature key by the signer, and the procedures implemented by a Certification Authority.
- ✚ Handwritten signatures are under the direct control of the signer, whereas digital signatures must be applied by a computer commanded by the signer.
- ✚ The data integrity service provided by digital signatures is much stronger than that provided by handwritten signatures.
- ✚ A fundamental difference, then, between digital signatures and handwritten signatures is that digital signatures require the intervention of a computer to be applied and computers are subject to both accidental errors and malicious subversion. Handwritten signatures, by virtue of their simplicity, are not subject to these vulnerabilities.

1.5.3 Consequences of the differences between Digital and Handwritten Signatures.

The differences between handwritten and digital signatures will likely have some practical consequences:

- ✚ The use of digital signatures for high-value financial transactions outside the protection of trading partner agreements is likely to proceed relatively slowly, until experience with the risks associated with use of digital signatures is accrued.
- ✚ Initial use of digital signatures is likely to be limited to applications where long-term archival is not very important, such as purchase orders, electronic funds transfers, authentication to on-line services, and the like. [6].
- ✚ Applications requiring high levels of non-repudiation assurance will likely require the use of digital time-stamping (or notary) services. These services may be provided by commercial or Government entities.

It seems unlikely that digital signatures will fully replace handwritten signatures in the foreseeable future. Handwritten signatures have a lot going for them - they are fast, cheap, easily understood, and last forever. Digital signatures will probably never be used for treaty authentication, signing bills into law, or other ceremonial or historical occasions.

2. System design & Analysis

2.1 Proposed System Background

The paper proposal defines two data structures, including the subject's signature and issuer's signature in X.509 v3 private extensions, to support the proposed visualized digital signature scheme. Thus visualized digital signature applications will be able to accept visualized digital certificates for use. The visualized digital certificate is defined in accordance with X.509. The X.509 v3 certificate allows communities to define private extensions to carry distinctive information. In X.509 there are some well defined attributes, like: name, address, phone, email address, company name, and role clearance [5].

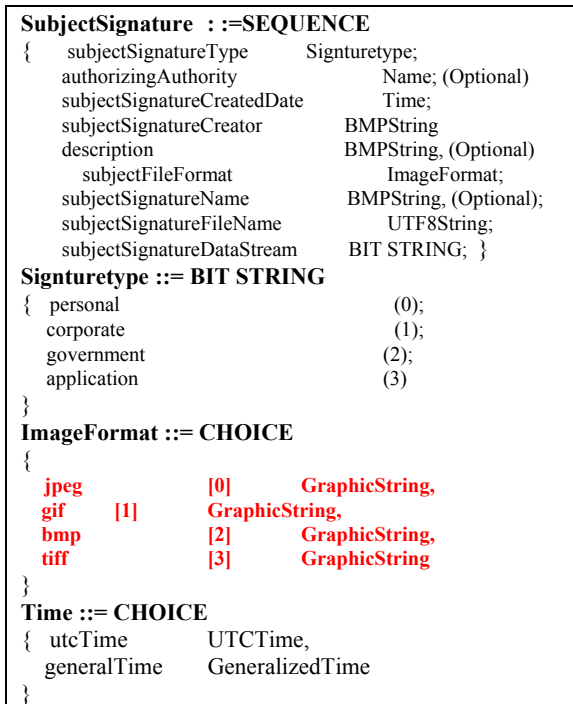


Figure 4: X.509 subject's signature contents

This sub-section specifies the format and content of a subject's signature as one of the proposed private extensions to X.509 v3. The structure of a subject's signature contains the sign type, authorizing authority, creation date, signature creator, description, file format, sign name, file name and the contents of the image file. The contents of a subject's signature are given in Figure 4.

2.2 Proposed System Signing Process

A signature image can be generated by any image-editing program or through a scanner. The contents of a signature image can include an impression bearing a mark or a name, like the inscriptions used to generate traditional signatures, which is a distinctive and recognizable constant token to the signer. The signature image and its related information containing signature type, signature authorizing authority, signature creator, relevant description, signature image format, signature size. Figure 5 shows the signing process. The structure of the issuer's signature is given in Figure 5.

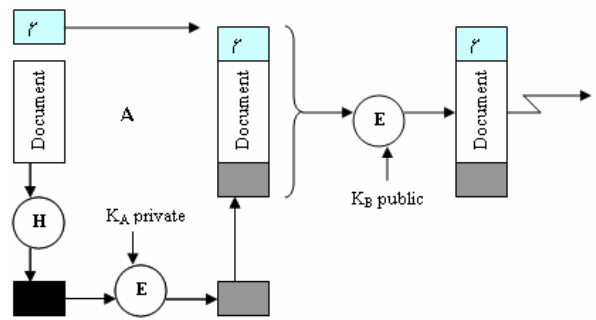


Figure 5: Signing process

2.3 Defining a New Attribute

To utilize the authentication information in an X.509 or related certificate, the authentication information would have to be defined as an attribute. If the authentication information construct, as defined in ECMA.219, is given the attribute syntax, the following attribute is the result as shown in Figure 6.

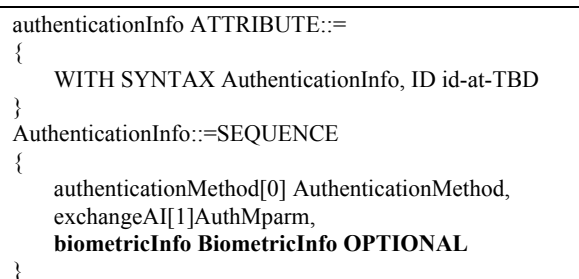


Figure 6: Signing process

2.4 Signature Verification Process

The object entity represents the processes that are involved in basically turning the requisition form into a complete digital certificate. The first of these is the hashing process, which uses the MD5 hash algorithm to hash the form and produce a digital fingerprint. The next process is the signing process, which uses the CA's Private Key to encrypt the fingerprint, and then this signature is attached to the certificate. Figure 8 illustrates the signature verification process.

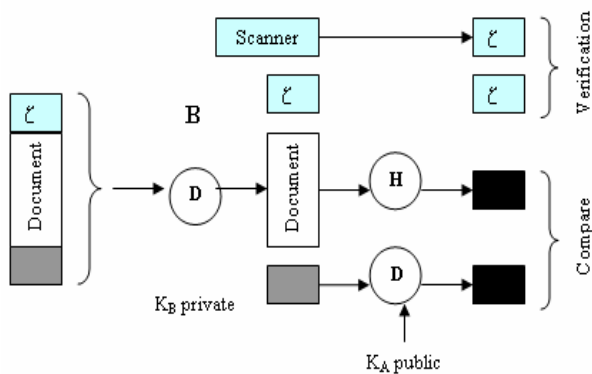


Figure 8: Signature Verification Process

4 Conclusions

Previous works have addressed the cultural gap between digital signatures and traditional handwritten signatures/signatures. However unsolved cultural issues still remain with regards to the use of modern digital signatures within the societies. These works are referred to a visual “signature” 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 signatures but for different purposes. This work bridges the cultural gap between traditional signatures/signatures and modern digital signatures and allows the signer to embrace the consistency of the digital signature. This research examines the historical values and applications of signatures in various 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 visualized digital signature, but also that a new public key digital certificate contain the issuer’s and signatory’s signature images to facilitate verification.

The proposed system enables the graphic image of the handwritten signature to be instantly embedded in documents/ smart cards. The combination of graphical and digital signatures provides a visual signature that the user is accustomed to seeing. Furthermore, the system allows several individuals to digitally and visually sign the same document.

5 References

- [1] Rivest, R., A. Shamir and L. Adleman (1978): A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. 21: 2120-126, Communications of the ACM.
- [2] Fillingham, D. (1997): A Comparison of Digital and Handwritten Signatures. Ethics and Law on the Electronic Frontier 6.805/STS085: Student Papers, Fall 1997.
- [3] Lutterbeck, B. (2000): Governing Legal Identities Lessons from the History of Signatures and Signatures. The Information Security Solutions Europe Conference, Barcelona Informatics and Society, Technical University Berlin.
- [4] Faisal Nabi, " Secure business application logic for e-commerce systems" Elsevier Journal of Computers & Security (2004), Article in press, pages: 1-10
- [5] R. Villarroela, E. Fernánde, and Mario P. "Secure information systems development e a survey and comparison". Elsevier Journal of Computers & Security (2004), Article in press, pages: 1-14
- [6] T. Tsiakis, and G. Sthephanides, "The concept of security and trust in electronic payments" Elsevier Journal of Computers & Security (2005), vol. 24, pages: 10-15.