Graphical handwritten and digital signature Integration for secure PKI

Nazar Elfadil, Ali Al Shidhani, Ahmed Al Naamany

College of Engineering, Sultan Qaboos University, Muscat, Sultanate of Oman.
Tel: +968-99523864, Fax: +968-24413454, Email: gazoli@mailcity.com or nazar@squ.edu.om

Abstract:
This paper discusses a concept of integrating a smart card and visual digital signature into an overall PKI in Oman. The purpose of this proposed solution is to fulfill the cultural gap between traditional digital signatures and current smart card digital certificate/signature through the integration of culturally relevant built-in features for increasing the acceptability of digital signatures and smart cards in global e-government, while maintaining the security features of current digital signature/certificate schemes. The paper contribution will be mainly in two areas; namely: modified X.509 authentication information extension and added the visual digital signature capability.

Keywords: *E-commerce, digital signatures, digital certificates, security, verification, and smart card.*

1. INTRODUCTION

Importance and viability of digital signatures for e-commerce and internet user identity verification has recently been significantly emphasized [1, 2, 3, 9, 10, and 11]. However, current digital signatures tend to overlook the importance of visualization, sense of personal identity and ownership. This is seen as essential in many cultures and historically documents verification has always depended on recognizable visual stimulus. This however, is one of the primary problems with current digital signatures they do not have same characteristics of a traditional signature to a user as it does not have the same sense of visualization.

To cater for the cultural requirements and user acceptance between the traditional and digital signatures, this work studies signature cultures in the framework of digital signatures, identifying the need to develop a culturally friendly, visual digital signature that could be imbedded into smart cards. The need of such visual digital signature is increasing due to two main reasons. Firstly, nations have used traditional signatures for a long time, particularly in 3rd world countries, any transaction or legal document have to be tailed with the signature of all individuals concerned. The process of signing transactions or documents spreads a sense of trust among all individuals, this has been the practice for so many years and keeping this practice will for sure keep the trust factor high. Secondly, digital signatures are the signatures of the future, they are more secure and efficient and soon all nations will be involved in the process of digitally signing documents, furthermore, this technology will soon be integrated in e-commerce and e-government transactions and by that time all citizens will come across using this technology once in a while. When digital signatures become a must, citizens of all ages will have to digitally sign their documents and transactions, normally the young generations are more into the digital world and digital signatures shouldn't be a problem to them, old generations might find it a bit awkward to digitally sign documents but when this practice takes place nation wide, age issues can't stop deployment. Looking at the two reasons above, clearly there is a need to compromise one for the other, either stop traditional signatures and depend completely on digital signatures or the other way round. This paper introduces a better solution to this dilemma, a combination of digital and traditional signature to achieve both goals, namely, trust and efficiency.

This work is attempt to identify means to allow acceptability of digital signatures and give a culturally known trust of a normal user signatures when using global e-commerce while maintaining the security features of the current digital signature. This is to be achieved by using new biometrics features that are embedded in smart card.

2. Functions & Syntax of Signatures

Signing of written documents and other formalistic legal processes serve a number of purposes. Among them, when an individual signs a document, it serves as evidence and makes the contents attributable to him/her in case of dispute (i.e. an authenticator). A signature also expresses the signer's approval or authorization of the writing, or the signer's intention that the document should have legal effect. Generally speaking, signatures can be divided into two categories: handwritten signatures and electronic signatures. Electronic signatures, however, exist in a variety of forms, such as, Digital signatures, and Digital certificate.

Traditional Handwritten Signatures

Formal documents are signed by handwritten signatures. The handwritten signatures are used to be the integrity mechanism that employed for prevention of fraudulent. Dispute they were widely used and have culture impacts, they are vulnerable for several reasons. First, there is no "standard method" for a handwritten signature, so they can vary and change from one to the next. This makes signature verification a difficult and uncertain activity. Second, handwritten signatures can be easily forged or copied. Finally, on multiple page documents, it can be difficult to determine whether the signature applies to all pages or whether pages have been added/deleted since the signing. Apart from the above mentioned shortcomings, still handwritten signatures have a role and impact among the various personal authentication techniques.[12]

Cultural Issues for modern Digital Signatures

Researchers of modern digital signatures [2,3, 9] appreciate the shortcomings and acknowledge that digital signatures fail to be widely implemented due to simple reason that they overlook cultural factors. Some tend to believe traditional signatures will not be replaced by digital signatures, due to these limitations [2]. Among the concerns is the issue that storage media utilized to store verifiable digital signatures tend to deteriorate and technological developments tend to make present storage formats redundant [9]. Further concerns are related to the document presentation which in most cases the document presented to the signer may be different from the actual one i.e. "What you see is what you signed" or WYSIWYS problem [4]. This problem is solved by Researchers at Hewlett-Packard (HP) Laboratories, by adding a piece of tamper resistant hardware, the Trusted Displayed Controller (TDC). The TDC display circuitry and cryptographic functions is based in a computer system. When the TDC has been authenticated by the signer's smart card then signer can depend on the platform to perform digital signing.

The success of Digital Signature is not expected to completely replace the traditional signature. In cases of ceremonial or historical events digital signatures are not expected to replace handwritten signature will never be used in, although this may be accepted [2].

Digital Certificate

Digital 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. While there are minimum-security issues with storing digital certificates themselves (since they are made publicly available), stringent security measures should be exercised to protect their associated private keys.

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 and SPKI (Simple Public Key Infrastructure) certificates.

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.[5]

3. Smart Card & PKI

Various business and government bodies are using PKI to provide high level of confidence when exchanging information, especially over the Internet. PKI achieves privacy through an architecture that operates using public/ private key pairs; as shown in Figure 1.

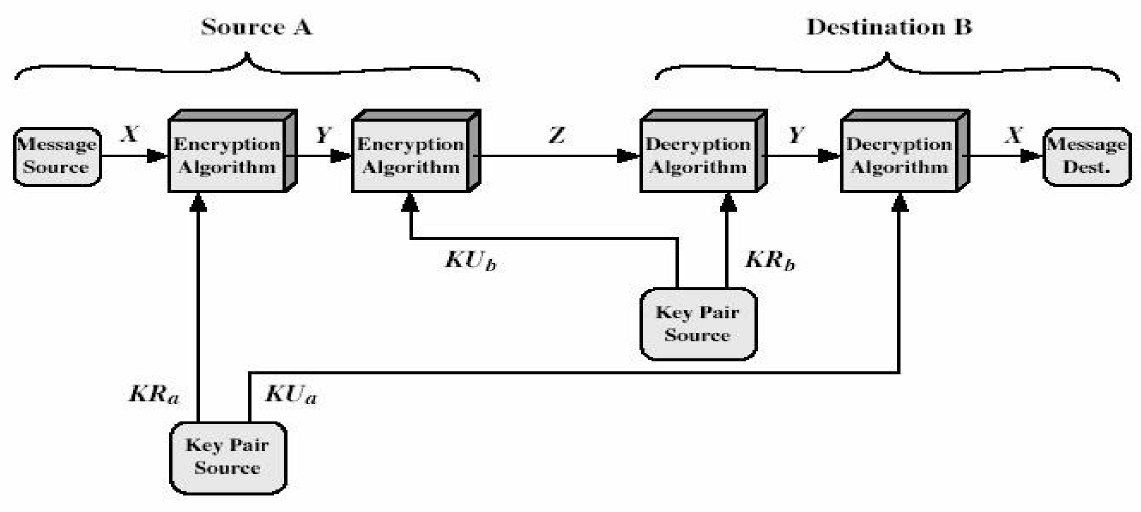

Figure 1: Secrecy & Authentication PKI system

The system works extremely well, but like any security system there are drawbacks. Smart cards could be used to rectify these drawbacks in several areas; among them:

a. **Vulnerability of hard drives**: without smart cards, hard drives can become the repositories of key pairs and digital certificates. Hard drives can crash, be lost, and susceptible to hacking. Despite they are protected with a password, but these are sometimes too easy to be cracked. Smart cards, on the other hand, provide a long term, tamper resistant, secure storage for highly valuable data.

b. **Portability:** Smart cards are highly portable. Moreover, they provide a safe and convenient method of storing and transporting credentials that allow people to access networks, sign and decrypt email and authenticate themselves any where and at any time. Without smart cards, it is necessary to carry a specific laptop or PC around, since the keys are stored on the laptop's or PC's hard drive.

c. **Smart cards and other digital certificate storage devices:** these contain a microprocessor and memory and provide the most secure solution; it has the following features (1) Keys are generated on the card or device, (2) Certificates and private keys are stored in an encrypted file on the card, token, or fingerprint-protected device, and (3) Encryption/decryption and data signing is performed on the card or device. The private keys are never exposed outside the device.

There are several approaches for user authentication are based on human biometry are being developed, e.g., fingerprint sensor, face recognition, hand geometry, and retinal scans. One of the primary advantages of biometrics authentication methods over other methods of user authentication is that they use real human physiological/ behavior characteristics to authenticate users.

Generally, a smart card is a relatively secure device compared to bar code and magnetic stripe cards. It is a safe place to store valuable information, such as private keys, account numbers, passwords, or valuable personal information such as medical records. It is also a secure platform for performing processes that you do not want to be exposed to the world, for example, performing an encryption using a public key, or a signature using a private key. Nonetheless, smart cards themselves have inherent drawbacks and risks. These include:

- Cost of readers, readers are an essential part of smart card infrastructure as they provide interface between the token and the network. It is important to consider the cost of readers
- Lack of standards, the lack of accepted standards within the smart card industry is another drawback. Although smart card readers are standardizing on the ISO 7816 based interface standards, that does not guarantee interoperability with all smart card vendors because various smart cards standards exists.
- Loss or theft, a primary risk that users face is physical loss or theft of the token. A more dangerous risk is theft of keys and discovery of the associated PIN or password used to unlock the keys, without damaging or removing the smart card and the fact that smart cards are susceptible to many kinds of attacks.

4. Proposed System

Overall Architecture

This 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 [4, 7]. While Authentication Information (AI), and including Biometrics attribute are not clearly defined; as shown in Figure 2, so the proposed system will modified the X.509 extension to accommodate the visual signature. When the user first registers with the CA, a visual signature will be needed, this is going to be digitized into X.509 v3 private extensions. Visual signature can be achieved using digital pen and can be signed in a tablet PC or smart card reader of the CA. The new digital certificate now contains user information, public key and visual digital signature. This digital certificate can be stored in the user's smart card.

```
SubjectSignature    : :=SEQUENCE
{      subjectSignatureType     Signturetype;
       authorizingAuthority                Name; (Optional)
       subjectSignatureCreatedDate       Time;
       subjectSignatureCreator             BMPString
       description                          BMPString, (Optional)

       subjectFileFormat                   ImageFormat;
       subjectSignatureName               BMPString, (Optional);
       subjectSignatureFileName          UTF8String;
       subjectSignatureDataStream        BIT STRING;
}
Signturetype ::= BIT STRING
{   personal                               (0);
    corporate                              (1);
    government                             (2);
    application                            (3)
}
ImageFormat ::= CHOICE
{  jpeg              [0]        GraphicString,
   gif               [1]        GraphicString,
   bmp               [2]        GraphicString,
   tiff              [3]        GraphicString
}
Time ::= CHOICE
{
```

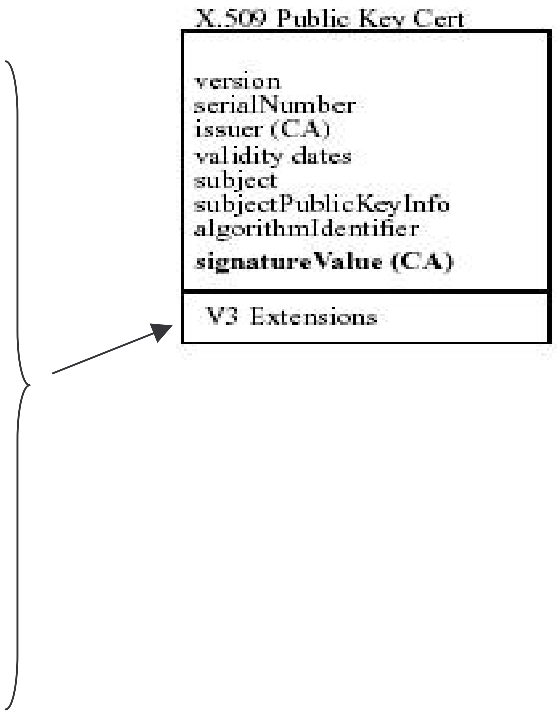

Figure 2: X.509 V3 Public key certificate attributes & contents [4]

This sub-section specifies the format and content of a subject’s signature as one of the proposed private extensions to X.509 v3 in relation to RFC3280. The concepts are based upon standard legal practice in Oman as these seem to have universal applicability. 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 3.

Signing Process

A signature image can be generated by digital pen or any digital input device. The user singes the document using the digital pen; the signature could be similar to the traditional handwritten signature which grants a comforting feeling. 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. At the front-end, the user signs the document using a digital pen. At the back-end, the document is first hashed to produce H(M) then it is encrypted with the private key of user A to produce $SIG_A(H(M))$. The visual signature is actually stored in binary representation by digitally sampling the signature, then it is hashed using a hash function to produce H`(M) which is then encrypted using the private key of user A to produce $VSIG_A(H`(M))$. Next, $SIG_A(H(M))$ and $VSIG_A(H`(M))$ are appended to the document and they are sent as one package along with the digital certificate of the sender. Figure 3 shows the signing process. This object contains the program, which acts as the security, services provider to the administrator operating the server. In addition to creates the actual digital certificate using X509 format

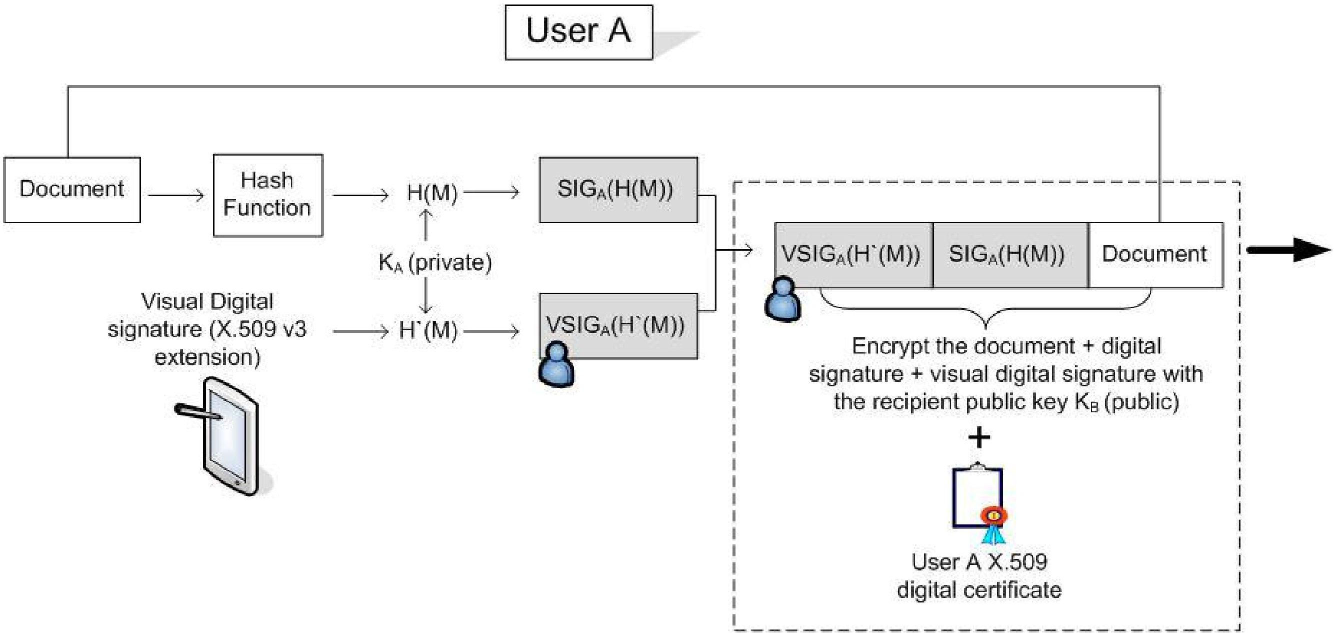
User A
Document
Hash Function
H(M)
SIGA(H(M))
KA (private)
Visual Digital signature (X.509 v3 extension)
H`(M)
VSIGA(H`(M))
VSIGA(H`(M))
SIGA(H(M))
Document
Encrypt the document + digital signature + visual digital signature with the recipient public key KB (public)
+
User A X.509 digital certificate

Figure 3: Signing process

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:

```
authenticationInfo ATTRIBUTE::=
{
      WITH SYNTAX AuthenticationInfo, ID id-at-TBD
}
AuthenticationInfo::=SEQUENCE
{
      authenticationMethod[0] AuthenticationMethod,
      exchangeAI[1]AuthMparm,
      biometricInfo BiometricInfo OPTIONAL
}
```

Signature Verification Process

The object entity which represents the processes that are involved in basically turning the requisition form into a complete digital certificate. The first of them 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 takes uses the CA's Private Key to encrypt the fingerprint just now and finally this signature is attached to the certificate. The receiver uses his/her public key to decrypt the package. Sender's public key is used to decrypt SIG_A(H(M)) and $VSIG_A$(H`(M)) to produce H(M) and H`(M) respectively; as shown in Figure 4. The original message goes through a hash function to produce H``(M). H(M) and H``(M) are compared to prove the integrity and authenticity of the message. Visual signature information stored in the private extensions of user A's X.509 digital certificate goes through a hash function to produce H```(M) which is compared to H`(M) produced from $VSIG_A$(H`(M)). If H`(M) = H```(M) then the visual signature is authenticated otherwise the message is discarded. For the security system to work perfectly, both comparisons should prove positive, if any of them proves negative then the received package can be discarded.

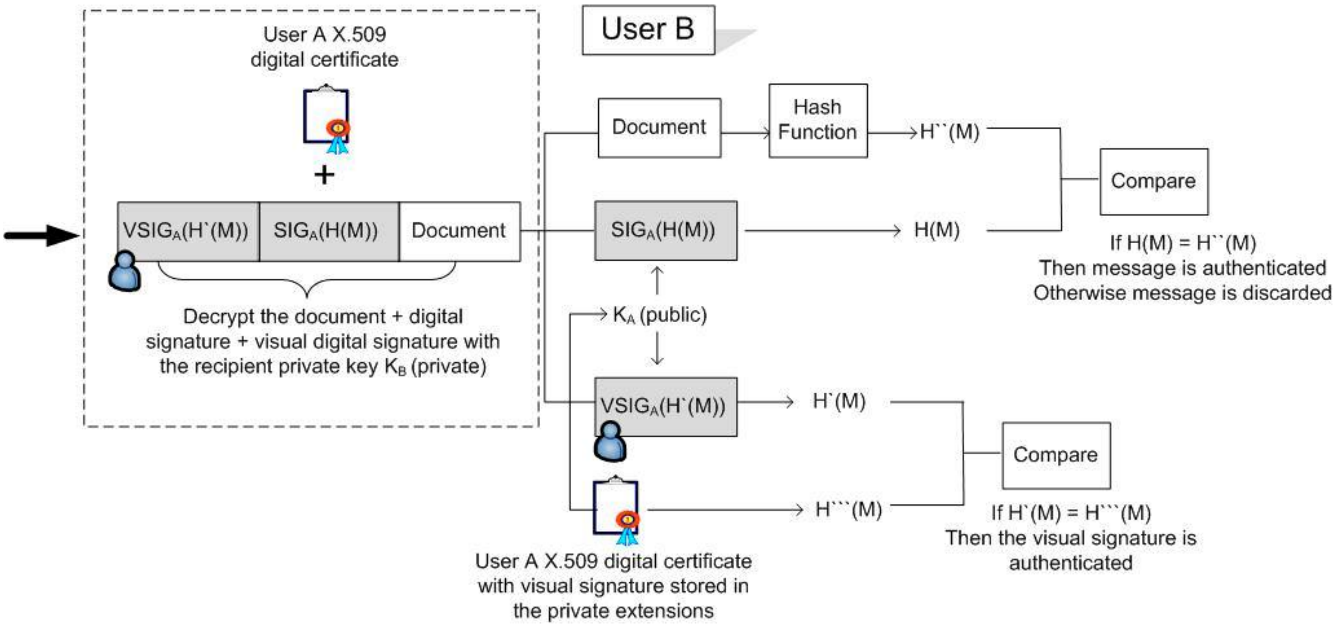
User B
User A X.509 digital certificate
+
VSIGA(H`(M))
SIGA(H(M))
Document
Decrypt the document + digital signature + visual digital signature with the recipient private key KB (private)
Document
Hash Function
H``(M)
Compare
SIGA(H(M))
H(M)
If H(M) = H``(M) Then message is authenticated Otherwise message is discarded
KA (public)
VSIGA(H`(M))
H`(M)
Compare
H```(M)
If H`(M) = H```(M) Then the visual signature is authenticated
User A X.509 digital certificate with visual signature stored in the private extensions

Figure 4: verification process

5. CONCLUSION

Digital signatures, as they are today, give a limited ability to electronically simulate a traditional signature. Extending digital signatures from stream of bytes appended to documents to a visual pattern that could very likely be similar to the traditional signature will make digital signatures more useful. However, the usefulness of digital signatures is maximally achieved when operated under a PKI. PKI is the foundation on which many security schemes can be implemented and many security applications can become reality.

An important contribution of this paper is to consider the impact of social, cultural and political factors on the adoption of Digital signature. It also discussed technological, political and cultural implications of the different steps of digital signature. Furthermore, it combined the traditional signature and digital signature in one platform to shrink the culture gap or impacts.

The limitations of one technique, in fact, reflect the strengths of the other which has prompted their integration. In combining the paradigms, handwritten signature can be viewed as mechanisms for providing social and culture acceptance, and digital signature as mechanisms for proving the authentication and confidentiality of the signed documents.

References

1. Balacheff, B., L. Chen, D. Plaquin and G. Proudler (2001): A Trusted Process to Digitally Sign a Document. NewSecurity Paradigms Workshop 2001, Cloudcroft, New Mexico, USA, NSPW '01: 78-86, 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. CDL: California Digital Library Digital Image Format Standards, California Digital Library (CDL) http://www.cdlib.org/about/publications/CDLImageStd-2001.pdf. 2003.
4. Housley, R., W. Ford, T. Polk and D. Solo (2002): Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile. Internet Request for Comments 3280
5. A. Bensefia, T. Paquet, & L. Heutte. "Handwritten Document Analysis for Automatic Writer Recognition" *Electronic Letters on Computer Vision and Image Analysis 5(2):72-86, 2005.*
6. Fabian Monrose, Aviel D. Rubin "Keystroke dynamics as a biometric for authentication" Future Generation Computer Systems 16 (2000) 351–359
7. T. Tsiakis, G. Sthephanides. "The concept of security and trust in electronic payments" Computers & Security (2005) 24, page: 10-15 (www.elsevier.com/locate/cose)
8. Stephen J. Elliott, Development of a Biometric Testing Protocol for Dynamic Signature Verification.
9. Vicky Liu, William Caelli, Ernest Foo, Selwyn Russell, "Visually Sealed and Digitally Signed Documents ". Proceedings of the 27th conference on Australasian computer science - Volume 26, p.p. 287-294.-Dunedin, New Zealand , 2004.
10. JANE K. WINN. ‘The Emperor’s New Clothes: The Shocking Truth about Digital Signatures and Internet Commerce’ http://www-swiss.ai.mit.edu/6.805/articles/signatures/quinn-signatures.html
11. Stapleton, J.; Doyle, P.; Esquire, S.T. ‘The digital signature paradox’ Proceedings from the Sixth Annual IEEE Systems, Man and Cybernetics (SMC) Information Assurance Workshop, 2005, Pages: 456 - 457.
12. Nir Kshetri, Nikhilesh Dholakia. Impact of Cultural and Political Factors on the Adoption of Digital Signatures in Asia. *Proceeding of the Seventh* Americas Conference on Information Systems, Boston, August 3-5, 2001.
13. Hamilton, D. J., Whelan, J., McLaren, A. & MacIntyre, I. (1995). Low Cost Dynamic Signature Verification System. In European Convention on Security and Detention (pp. 202-206). London, UK: IEE.
14. Barcelo, R., Baker, S. & Greenwald, E. (2000, Sept). An Analysis of International Electronic and Digital Signature Implementation Initiatives. In Internet Law and Policy Forum. New York, NY: Internet Law and Policy Forum. Retrieved November 24, 2000 from the World Wide Web: http://www.ilpf.org/digsig/analysis_IEDSII.htm
15. Leclerc, F. & Plamondon, R. (1994). Automatic Signature Verification: The State of the Art - 1989-1993. Progress in Automatic Signature Verification (pp. 3-21). Singapore: World Scientific Publishing Co.
16. Lee, L., Berger, T. & Aviczer, E. (1996). Reliable On-Line Human Signature Verification Systems. IEEE Transactions on Pattern Analysis and Machine Intelligence, 643-647.
17. Li, X., Parizeau, M. & Plamondon, R. (1998). Segmentation and Reconstruction of On-Line Handwritten Scr. Pattern Recognition, 675-684.
18. Mettyear, N. (2000). Error Rates in Biometric User Authentication. Unpublished manuscript Mingming, M. & Wijesoma, W. (2000). Automatic On-Line Signature Verification Based on Multiple Models. In CIFEr'01: Computational Intelligence in Financial Engineering Conference (pp. 30-33).IEEE

Article received: 2005-03-05