Visually & digitally signed Smart card

Nazar Elfadil
College of Engineering, Sultan Qaboos University
Muscat, Sultanate of Oman.
Tel: +968-9523864, Fax: +968-513454.Email: gazoli@mailcity.com or nazar@squ.edu.om

Abstract
This proposal develops the concept of integrating a smart card and visual and 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 egovernment, while maintaining the security features of current digital signature/certificate schemes. The paper contribution will be mainly in two areas; namely: modified the X.509 authentication information extension, and added the visual and digital signature capability.

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

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 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 does not have the same sense of visualization. Because digital signatures are appended to a 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. Moreover, digital signatures change each time they are applied, unlike traditional signature that are constant personal identifiers associated with individual signatories to facilitate verification.

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 could be imbedded into smart cards.

The purpose of this work is to increase the acceptability of digital signatures and give a sense of trust to a normal user using the system in global e-commerce while maintaining the security features of the current digital signature by using extra biometrics features that embedded into smart card.

1.1 Digital Signatures with Cultural Issues

Fillingham [2] 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 [3] states digital signatures fail to meet high expectations for their success due to the simple flaw that they overlook cultural factors. However, Fillingham [2] and Lutterbeck [3] investigate the use of traditional signatures, their work fails to exploit the concept of traditional signatures/signatures to innovate a culturally friendly digital signature regime.

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 [4]. Researchers at Hewlett-Packard (HP) Laboratories, [5] 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.

1.2 Digital Certificate

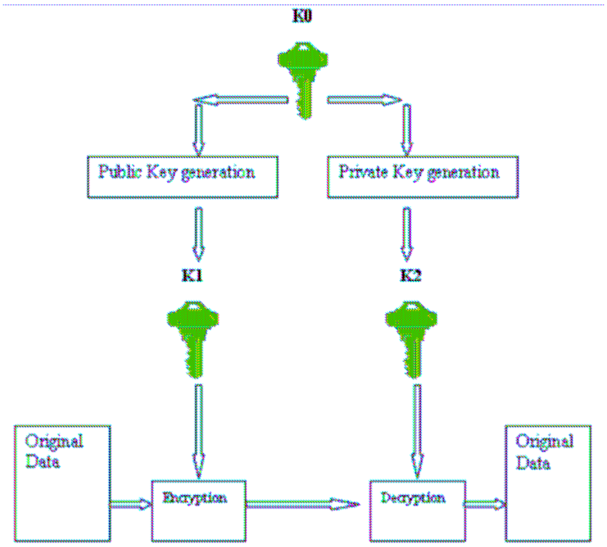
Digital certificates and their associated keys are predominantly used by Web browsers and e-mail clients for security functions such as user authentication and digital signatures. Therefore, they need to be stored where they can be conveniently retrieved to be used for these functions. While there are 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 (Callas et al. 1998) and SPKI (Simple Public Key Infrastructure) certificates (Ellison et al. 1999).

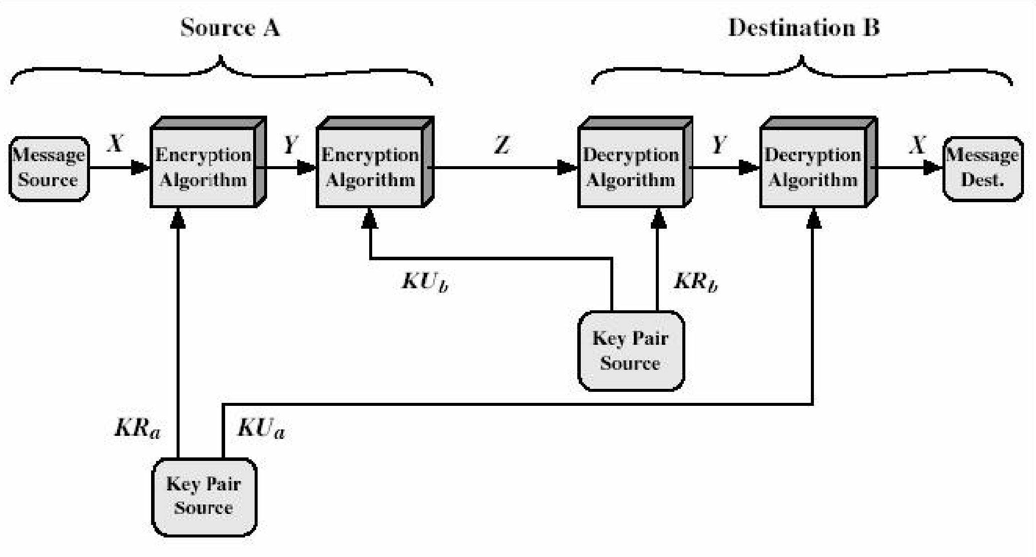
Certificates are digitally signed by the issuing certification authority (CA), and they can be issued for a user, a computer, or a service, (which provides authentication) or a Smart Card User certificate (which provides authentication plus other uses of the smart card cryptography) unless a system administrator has granted the user access rights to the certificate template certificate template

1.3 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.



(a) Secrecy of PKI



(b) Secrecy & Authentication of PKI system
Figure 1: 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:

1.3.1 **Vulnerability of hard drives**: without smart cards, hard drives can become the repositories of key pairs and digital certificates. Hard drives can be crash, 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.

1.3.2 **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.

1.3.3 **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.

1.4 RISKS OF SMART CARDS

A smart card is a relatively secure device compared to bar code and magnetic stripe cards [Maybe this sentence should come when you first started talking about smart cards in 1.3]. 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 the high cost of readers, algorithm replacement, lack of standards, loss or theft, and the fact that smart cards are susceptible to many kinds of attacks.

1.4.1 Cost of Readers

One challenge is planning for the cost of card readers. Readers are an essential part of smart card infrastructure as they provide interface between the token and the network.

Smart cards can be the basis of trust for secure interaction in PKI for many agencies and their customers. For this to be achieved, a cost effective and acceptable level of risk must be achieved for all who depend on the associated certificates and keys. Achieving an efficiency of scale between volume of shared PKI-enabled services that use certificates and keys stored on a common token is the desired trade-off. An important element to consider is the high cost of readers.

1.4.2 Algorithm Replacement

Algorithm replacement is inevitable and as such these replacements and the associated costs will have to be considered at the outset. Algorithm replacement costs and operational impacts to applications and associated smart cards that generate keys should be accommodated through a modular design of algorithm related functions. Every algorithm will inevitably require replacement due to the increasing computer processing capacity (although algorithm useful life can be extended through the use of larger keys. For example, an RSA modulus of 1024 bits is considered secure today; but if it can be attacked within the next 10 years, one solution is to convert to longer key lengths, such as a modulus of 2048 bits). The careful planning for replacement before the anticipated time when an algorithm cannot protect data satisfactorily should be planned into smart card maintenance schemes.

1.4.3 Lack of Standards

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. Numerous standards exist, and many of them target certain verticals or a certain layer of communications. This leaves out many players. This problem is being mitigated as PKI-enabled Web browsers and other mainstream applications gain the capacity to accept the smart cards and a consensus on basic PKIbased service requests to the smart card. The development of smart card standards, however, is trailing the demands for greater processing and storage capacity on smart cards. By the time standards are developed, the next generation of smart cards is being fielded.

1.4.4 Loss or Theft

Irrespective of the use of the smart card, a primary risk that users face is physical loss or theft of the token. This risk is countered with the inevitable acknowledgement of a missing token and associated revocation procedures to prevent further misrepresentations of the individual’s certificate-based trust among associated PKI enabled applications. 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. This risk poses a far greater threat to the associated trusting PKI-enabled applications and breaches are usually discovered and mitigated only after serious harm occurs, or the certificate is revoked or expires. Regardless of the protections that are built into the system, if the card is not physically protected, laws and security measures will not be effective. This protection is evolving into a combination of user responsibility for physical possession/compliance with associated policies for use and card protection of the keys during generation and/or use.

1.4.5 Attacks on Smart Cards

Smart cards are susceptible to attack by bad actors. An attack is defined simply as an attempt to steal or compromise data on the smart card. There are two classes of attackers—those who are parties to the system, and those who are interlopers. Attacks by participants could be a cardholder trying to cheat a terminal owner, a card issuer trying to cheat a cardholder, or similar behavior. Attacks by outsiders could be mounted via card theft, card misuse, or replacement of terminal software or hardware. Attacks by outsiders are often similar to attacks on protocols involving general-purpose computers; however, they may take advantage of various properties of the system created by the separation of roles. Four kinds of attacks can be made on smart cards: logical, physical, Trojan horse, and social engineering.

1.4.5.1 Logical Attacks.

One type of attack is logical attack. A logical attack does no physical harm to smart card; rather, some sensitive information on the card is obtained by examining the bytes being transmitted to or from the card. If successful, this attack creates one of the greatest threats (i.e., potential undetected use increases until substantial damage occurs and is noticed). This attack is difficult to achieve because it involves capturing both the private key and associated PIN to perform private key operations. If the byte level I/O operations are monitored, and processing of PKI functions is not performed on the card, both the keys and PIN are exposed.

1.4.5.2 Physical Attacks.

Physical attacks are carried out, usually using special equipment, by varying temperature, voltage, or clock frequency, etc., to gain access to sensitive information on the card, or by monitoring card parameters (such as power consumption or the timing of certain card processor operations). Most smart card operating systems write sensitive data to the EEPROM area in a proprietary, encrypted manner so that it is difficult to obtain clear-text keys by directly hacking into the EEPROM. Other physical attacks that have proven to be successful involve an intense physical fluctuation at the precise time and location where the PIN verification takes place. When this happens, sensitive card functions can be performed even though the PIN is unknown to the perpetrator of the attack. A combination of a physical attack with a logical attack will reveal the private key.

1.4.5.3 Trojan Horse Attacks.

A Trojan horse attack involves planting malicious code on a user’s workstation without the user's knowledge. When the user submits a valid PIN, the Trojan horse presents rogue data to be signed using the private key. The user is never aware that the rogue data has been signed. There are two ways of counterattacking the Trojan horse. The first is to use “single-access device driver” architecture.

The operating system allows only one “trusted” application to have access to the smart card (if that one application can be compromised, of course, then even this approach can be circumvented). Not using a multiapplication smart card both reduces the number of parties involved and creates a simpler operating environment with less complexity and potential for bugs. Although this reduces the possibility of attack, the benefits to be derived from multi-functionality are, of course, lost. Another way to prevent this type of attack is to require one private key entry per PIN entry; the user must then use the PIN every time the private key is to be used, thereby disallowing the Trojan horse access to the key.

1.4.5.4 Social Engineering Attacks.

This kind of attack exploits the vulnerabilities inherent in human beings. For example, a hacker could pose as a network technician and request PIN and passwords in order to hack the system. This attack is not as effective when smart cards are involved because people are less likely (or even able) to share their smart card than a PIN or password. When a decision to proceed with smart cards is made, it is essential to understand that “eternal vigilance” is not only expensive, but impossible. The risks associated with smart card tokens must be understood and bound and balanced against associated benefits. The benefit of cost savings from increased efficiency or compliance should be weighed against the associated threats resulting from the fact that data will be exposed to remote access by users who hold the appropriate PKI credentials. Incremental steps to cost effectively control and leverage the demand for smart cards should be undertaken. [Since the objective is to use smart cards to rectify PKI drawbacks, I guess mentioning all these drawbacks and risks of smart card is against your objective]

1.5 Authentication Information (Biometrics)

Users’ identities are verified using one or more of three generic methods (types): something they know (PINs, passwords, memory phrases, etc.), something they have (a physical token such as a magnetic stripe card, a physical key, a smartcard, etc.), or something they are (biometric verification). If this information is gathered by a trusted process, verified, and then signed by a trusted authority, it can be considered as trusted authentication information (AI). Biometrics are methods of measuring the inherent physical attributes of an individual. This is usually performed in order to identify an individual or to verify a claimed identity. In the first case, a “livescan” is provided, and a database of templates is searched to determine who the scan is associated with. In the second case, a template is provided with the livescan for a direct comparison. There is exists many different types of biometric attributes to identify users. They may be based upon fingerprints, hand or facial geometry, retinal or iris patterns, or even speech recognition. Each of these technologies can be obtained from multiple sources, with different algorithms and techniques for storing an individual’s features and/or comparing“livescan” of an individual’s features to the previously stored record. The stored record is typically referred to as the “Biometric Template”. Biometrics can be best characterized as an emerging technology.

2. System design & Analysis

2.1 proposed system

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 will defined attributes; like: Name, Address, Phone, Email address, Company Name, and Role Clearance [5]. 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. Figure 3 illustrates the overall proposed system architecture.

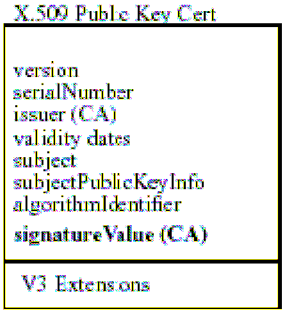


Figure 2: X.509 V3 Public key certificate attributes

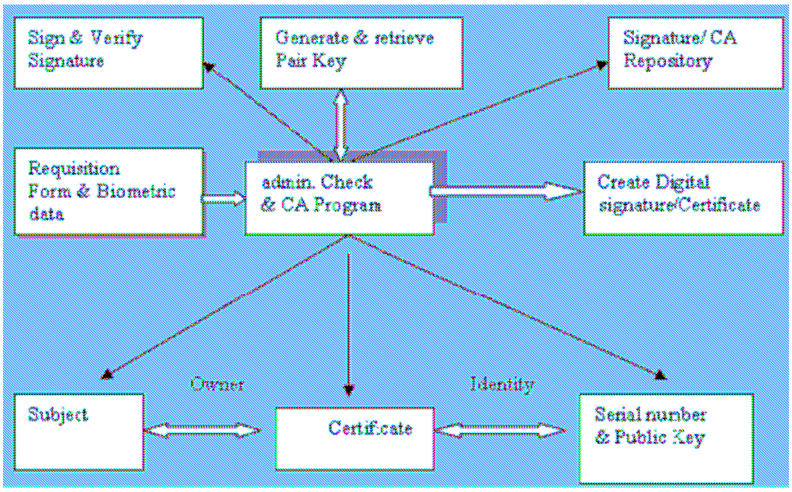

Sign & Verify Signature
Generate & retrieve Pair Key
Signature/ CA Repository
Requisition Form & Biometric data
admin. Check & CA Program
Create Digital signature/Certificate
Owner
Identity
Subject
Certificate
Serial number & Public Key

Figure 3: proposed system architecture

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 4.

```
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
{
    utcTime                 UTCTime,
    generalTime             GeneralizedTime
}
```

Figure 4: X.509 subject's signature contents

Table 1: X.509 subjects' signature contents description

Item	Description
subjectSignatureType	Identifies a particular signature from a list of types; including: personal, corporate, governmental and application
authorizingAuthority	It present if the SsubjectSignatureType is not set to personal.
subjectSignatureCreatedDate	Specifies when the signature image was created
subjectSignatureCreator	String field identifying the signature creator as record.
description	An optional string field that contains specific comments on the subject's signature.
subjectFileFormat	The major signature image types are: JPEG, GIF, BMP, and TIFF
subjectSignatureName	An optional string that allows specifying the identity of the signature, particularly when the signature owner may posses multiple signatures.
subjectSignatureFileName	It is string that specifies the file name of the subject's signature.
subjectSignatureDataStream	It contains the data content of the subject's signature

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. 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

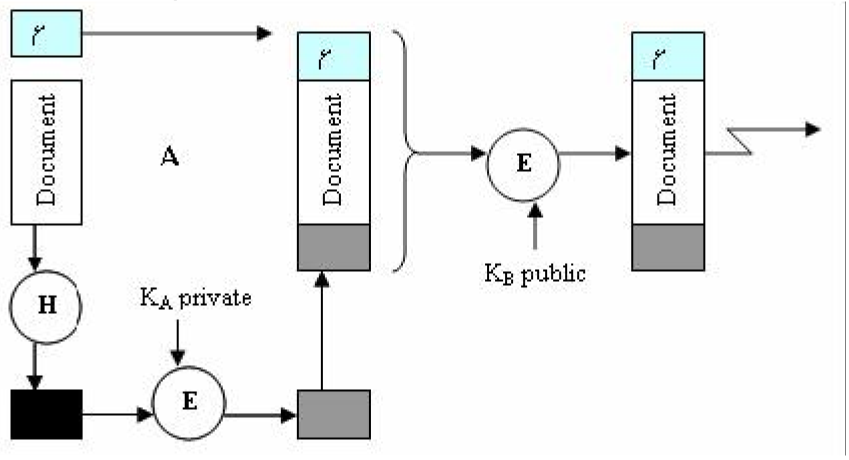


Figure 5: Signing process

The issuer itself digitally signs them. The structure of the issuer’s signature is given in Figure4.

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:

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

Figure 6: Signing process

Table 2: X.509 Version 3 Fields

Field	Description
version	This identifies which version of the X.509 standard applies to this certificate.
serial Number	The issuer creates a unique serial number and places it here. It is intended to distinguish this certificate from all others created by the issuer.
subject	The name of the entity (usually a human) whose public key the certificate identifies.
subject Unique identifier	The unique id of the subject (optional for version 3 and after).
Subject PublicKeyInfo	This value is used to encrypt information to be sent to the entity.
issuer	The name of the entity that is signing the certificate. The entity is usually a Certificate Authority (CA).
issuer Unique identifier	The unique id of the issuer (optional).
validity	This specifies when a certificate is valid.
extension(s)	Add on fields (Optional-see following section)
signature	The signature field consists of: Identifier of the algorithm used to create the signature and the output of the signing function.

2.4 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.

```
Attribute ::= SEQUENCE {
type ATTRIBUTE.&id ({ SupportedAttributes}),
values SET SIZE (0.. MAX) OF ATTRIBUTE.&TYPE
                    ({ SupportedAttributes}{@ type}),
valuesWithContextSET SIZE (1 .. MAX) OF SEQUENCE
{
    value ATTRIBUTE.&Type
    ({SupportedAttributes}{@type}) OPTIONAL,
    contextListSET SIZE (1 .. MAX) OF Context} OPTIONAL
}
```

Figure 7: Attribute construct utilized by X.509

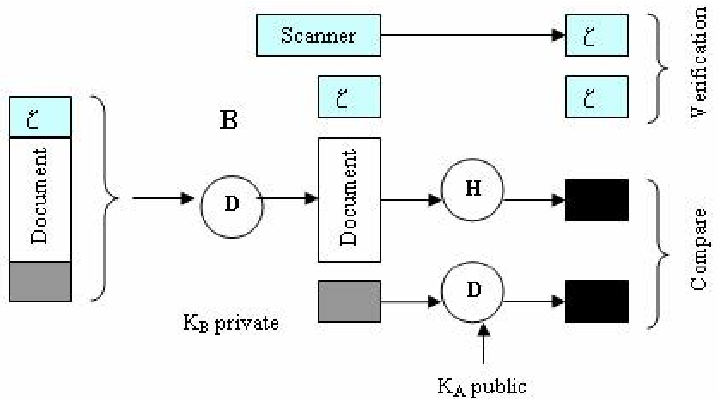


Figure 8: verification process

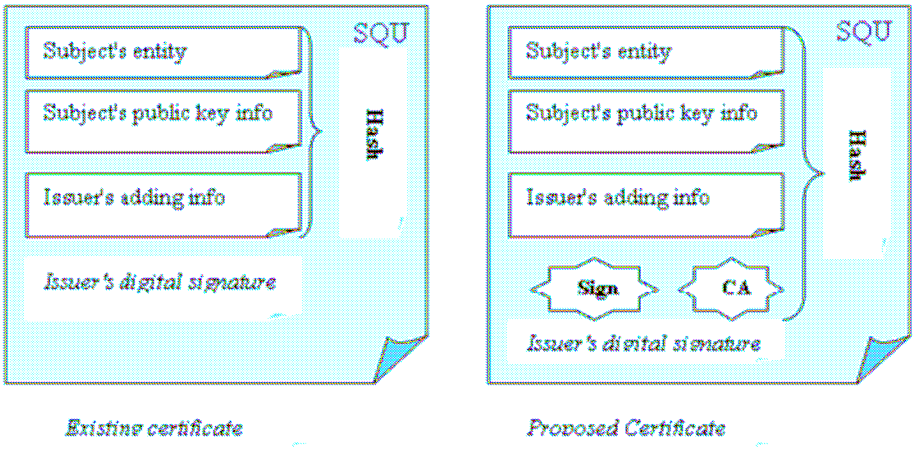


Figure 9: The overall process

3. 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. PKI software is written and developed by a team of students at the department as a final year project. PKI and visual digital signatures are going to be the building blocks of a secure e-government in Oman.

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. Accessed 3 April 2003**.

[4] 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

Received: 2005-02-08