ASPECTS OF INFORMATION SECURITY IN THE ELECTRONIC DOCUMENT MANAGEMENT SYSTEM (EDMS) FOR BANK SYSTEM

Sunbula Muminova
Nurafshon branch of Tashkent University of Information Technologies named after Muhammad al-Khwarizmi
Tashkent, Uzbekistan

Nafisa Yuldasheva
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi
Tashkent, Uzbekistan

Nuriddin Safoev
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi
Tashkent, Uzbekistan

Abstract. *This article provides an overview of current document security issues and technologies, and presents a suite of document security solutions. This article also summarizes implementations of document control and digital signatures for protecting electronic documents. As organizations move more and more business processes online, protecting the confidentiality and security of the information used in these processes, as well as ensuring the authenticity and integrity, is essential. Since many automated processes rely on electronic documents containing sensitive information, organizations must properly protect these documents. Many information security solutions attempt to protect electronic documents only when they are stored or in transit. However, these solutions do not provide protection for the entire life cycle of an electronic document. When the document reaches the recipient, the protection is lost and the document can be intentionally or unintentionally forwarded and viewed by unauthorized recipients. A much more efficient solution is to secure the document by assigning security parameters that are passed along with it. To ensure more effective protection of an electronic document throughout its life cycle, six criteria must be met: confidentiality, authorization, accountability, integrity, authenticity and non-repudiation. The two main security methods used to establish these six document security criteria are document management and digital signatures. The Electronic Security Suite provides document control and digital signature services that simplify*

the process of securing sensitive electronic documents and forms. Organizations can easily integrate electronic document security solutions into their current business processes and corporate infrastructure to support a wide range of simple and complex processes. The solutions dynamically protect electronic documents both on and off the network, online and offline, providing end-to-end security throughout the entire lifecycle of an electronic document.

Keywords: *confidentiality; authorization; accountability; integrity; authenticity; reliability*

INTRODUCTION

As organizations move more and more business processes online, protecting the privacy and security of the information used in these processes is essential. Since many automated processes are based on electronic documents containing critical, personal and confidential information, organizations must invest heavily to properly protect these documents [4]. There are three main reasons why organizations need to ensure the security of electronic documents:

A. Regulatory requirements

Many companies are directly or indirectly subject to government regulations and consumer privacy regulations. These include:

- Health Insurance Portability and Accountability Act (HIPAA) - protecting health-related data.
- Gramm-Leach-Bliley Law - Financial Privacy.
- European Union Directive on Privacy and Electronic Communications.
- Japanese and Australian privacy laws.
- California SB 1368 - Privacy Notice.
- California AB 1950 - Protection of customer data [3].

B. Return on Investment (ROI)

Organizations can achieve a significant return on investment by moving to electronic business processes. Automated workflows allow potential customers, consumers, partners and suppliers to participate, allowing organizations to realize significant cost savings while increasing customer satisfaction and loyalty. However, many work processes cannot be automated until adequate security measures are in place for information transmitted electronically. For example, how can you be sure that

the bank statement you receive is really from your bank (authenticity), that it has not been altered in transit (integrity), and that it has not been viewed by anyone other than the intended recipient (confidentiality)?

C. Information Security

The number of thefts of confidential information is on the rise, which can jeopardize revenues, competitive advantages and customer relationships; create negative advertising; and lead to significant sanctions and fines for non-compliance with privacy laws. Many information security solutions attempt to protect electronic documents only when they are stored or in transit. For example, organizations rely on document management systems and virtual private networks (VPNs) to secure documents. With this approach, document security remains a concern because these solutions only protect the communication line or storage location; they do not protect the actual content of an electronic document throughout its entire life cycle. When the document reaches the recipient, the protection is lost and the document can be intentionally or unintentionally forwarded and viewed by unauthorized recipients. Consequently, many organizations are forced to use an inconsistent mix of online and paper-based processes in which sensitive documents must be printed and physically delivered to ensure proper security. As a result, the potential benefits of online processing may not be fully realized.

II. HOW TO ENSURE PERMANENT DOCUMENT PROTECTION

A much more effective solution for protecting an electronic document is to assign security parameters that are an integral part of the document itself. The following criteria determine the continued security of a document [2]:

- Confidentiality - who should have access to the document?
- Authorization - what rights does the user have to work with the document?
- Accountability - what did the recipient do with the document?
- Integrity - how do you know if a document has been modified?
- Authenticity - how to find out where the document was taken from?
- Non-repudiation - can the person who signed the document refuse to sign the document?

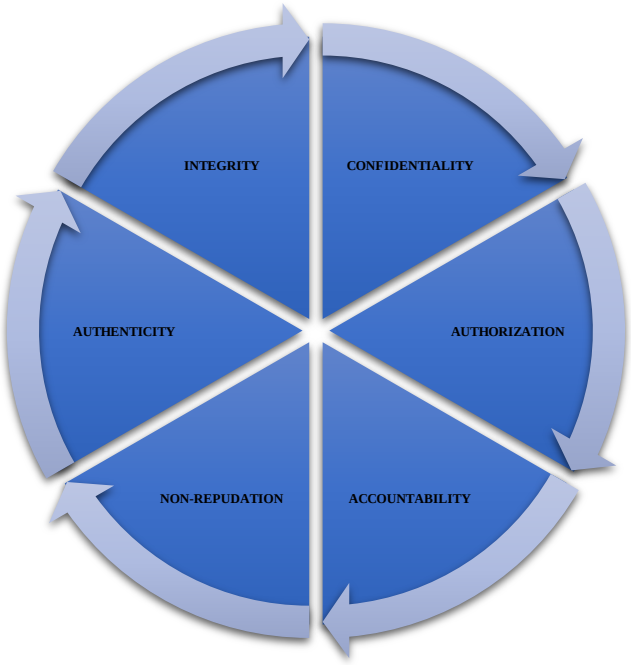

Fig.1. Six Key Criteria for Keeping Documents Secure at All Times

The following sections review the main technologies used to provide document and digital signature verification and identify the technologies that have been implemented in document security solutions.

III. DOCUMENT CONTROL

A. Privacy - Encryption

Encryption is the process of converting information (plaintext) into an incomprehensible form (ciphertext). Encryption is an effective method for controlling access to documents. Decryption is the reverse process that converts the ciphertext back to the original plaintext. Cryptography refers to the two processes of encryption and decryption, and its implementation is called a cryptosystem. Popular encryption systems use the concept of keys. The encryption key is the data that, when combined with the encryption algorithm, creates the ciphertext from the plaintext and reconstructs the plaintext from the ciphertext. Today, security experts agree that the Kerckhoff principle is the foundation of an efficient cryptosystem. The Kerckhoff Principle states that the key is the only part of a cryptosystem that must remain secret for the entire system to be secure. If the strength of a cryptosystem depends on the fact that an attacker does not know how the algorithm works, then it is only a matter of time before it can be reverse engineered and cracked. The two main types of encryption keys include symmetric and asymmetric.

1. *Symmetric keys.* Symmetric key cryptography uses the same key for both encryption and decryption, and is very fast and difficult to break with large keys. However, since both parties need the same key to communicate effectively, key distribution becomes a problem. Common symmetric key encryption algorithms today are AES, DES, 3DES, and RC4. Electronic products use AES (128-bit and 256-bit) and RC4 (128-bit) as they have become very strict standards.

2. *Asymmetric keys.* Asymmetric key cryptography, also called public key cryptography, uses pairs of keys to encrypt and decrypt. For example, if the first key encrypts the content, then the second key of the pair decrypts the content. Similarly, if the second key is used to encrypt information, then the first key must be used to decrypt the content. Typically, one key in a pair is marked as the public key and the other as the private key. The individual keeps the private key secret, while the public key is freely distributed to others who wish to communicate with that individual. When someone wants to send a confidential message to a person, he or she can encrypt it with a freely available public key and send the encrypted text to the person. Since only the person has the private key, he or she is the only one who can decrypt the content. Asymmetric keys help solve the key distribution problem, but the algorithms tend to be slower at equivalent powers. Some common asymmetric algorithms are RSA, DSA and El Gamal.

3. *Hybrid encryption.* Security systems tend to use a hybrid solution to improve the security and speed of document encryption. One approach is to use asymmetric keys to secure the symmetric keys and then use the symmetric keys to encrypt the information. This technique helps to solve both the key distribution problem of symmetric key cryptography and the performance problem of asymmetric key cryptography. The Electronic Acrobat software uses hybrid approaches so that individual documents can be protected for multiple recipients, each with a unique key pair. With this method, the file size does not increase significantly because it is not necessary to encrypt the entire document for each person. Instead, the document is encrypted with a single symmetric key, and that symmetric key is encrypted for each recipient with their respective public key.

B. Authorization

In addition to controlling who can open a document, organizations gain additional protection through authorization. Authorization specifies what a user can do with a document and is achieved through permissions and dynamic document management.

– Permissions govern the user's actions when working with a protected document. Permissions can specify whether a recipient who has access to the document is allowed to print or copy content, fill in fields, add comments or annotate the document, insert

or delete pages, forward the document, access the document offline, digitally sign the document, and so on. .

– Dynamic Document Control maintains the access rights and permissions assigned to an electronic document after it has been published and distributed. The author of a document can make changes to a released document without having to manually distribute it, because the changes are automatically propagated to all existing versions of the document, no matter where they are. Using Dynamic Document Control, organizations can manage and monitor electronic document usage inside and outside the firewall, online and offline, and across multiple documents.

Dynamic document control includes the following features:

– Document Expiration and Revocation - Control of documents after publication can be maintained by applying expiration dates and the ability to revoke access to a document. For example, an author might send a document that expires in two weeks so that recipients cannot access it after the expiration date, or access to a document can be automatically revoked if the authorized recipient leaves the project or changes department.

– Offline Access Control - Organizations can control how long an authorized recipient can access a document offline. After the specified amount of time has elapsed, the recipient can no longer view the document and must reconnect to the network to gain additional access. Any access or permission changes made by the author to the distributed document will be applied when the recipient comes back online.

– Persistent Version Control - Content and document management systems provide an efficient mechanism for version control as long as a document remains within the system. Persistent version control extends these capabilities by supporting offline and offline versioning. This allows document authors to make changes to document usage policies and prevent access to an outdated version by providing end users with the location of the updated version, no matter where the document is located.

C. Accountability

Document auditing allows organizations to maintain accountability regarding the use of secure documents because they can know for sure:

– How the recipient used the document
– How often did each type of use occur
– When did this use occur

Accountability is achieved when the author can track each recipient's use of the document for each assigned permission (for example, allowing the user to fill in fields

on a form, print, forward, save a copy, etc.). The audit should include automatic notifications about the use of protected documents. For example, a customer service representative sends an urgent electronic statement to a customer that requires action from the customer, such as a response or a digital signature. Once the client receives the electronic document, the representative is automatically notified when the client opens it. If the customer does not open the document, the representative is notified about this after 24 hours. Alternatively, a customer relationship management (CRM) system can use a failure notification to trigger an escalation or a specific follow-up task by a customer service representative.

IV. DIGITAL SIGNATURES

When businesses distribute documents electronically, it is often important that recipients can verify:

- That the content of the document has not been changed (integrity)
- That the document comes from the person who sent it (authenticity)
- The fact that the person who signed the document cannot refuse to sign (non-repudiation)

Digital signatures meet these security requirements by providing higher guarantees of document integrity, authenticity, and non-repudiation [5].

A. Integrity

Digital signatures allow recipients to verify the integrity of an electronic document used in one-way or two-way workflows. For example, when a digital signature is applied to a quarterly financial report, recipients have more confidence that the financial information has not been changed since it was sent. Techniques for maintaining integrity include:

- Parity bits or cyclic redundancy check (CRC) functions - CRC functions work well for unintentional modifications, such as wire noise, but can be bypassed by a cunning attacker.
- One-way hash - A one-way hash creates a fixed length value called a hash value or message digest for a message of any length. A hash is like a unique fingerprint. With the hash attached to the original message, the recipient can determine if the message has been modified by recalculating the hash and comparing their response with the attached hash. Common hashing algorithms are MD5, SHA-1 and SHA-256. Electronic has adopted the SHA-1 and SHA-256 algorithms because of their wide acceptance as a security standard.

– Message Authentication Codes (MAC) - MAC prevents an attacker from getting the original message, modifying it, and adding a new hash. In this case, the symmetric key is connected to the MAC and then hashed (HMAC). Without the key, an attacker cannot forge a new message. Electronic uses HMAC where appropriate.

B. Authenticity

Digital signatures ensure the authenticity of a document by verifying the digital identity of the signer. For example, a digitally signed quarterly financial statement allows recipients to verify the sender's identity and ensures that the financial information has not been altered since it was sent. Digital signatures are created using asymmetric key cryptography. To encrypt a document, the author of the document encrypts the document using the public key. Because the recipient is the only person with the private key, he or she is the only one who can decrypt the message. Digital signatures change the use of public and private keys to authenticate a document. The author encrypts the hash of the message with the private key. Only the public key can correctly decrypt the hash and use it to see if it matches the new hash of the document. Because the recipients of the document have the author's public key, they have more confidence that the person who signed the document was the person who encrypted the original hash.

The process of creating a digital signature is as follows:

– A hash of the original document is created.
– A digital signature is created that encrypts the hash with the private key.
– The signature is attached to the document.

Electronic Acrobat supports multiple digital signatures placed anywhere in a document for proper presentation. In fact, Electronic Acrobat keeps track of all previously "signed" versions in a document to make it easier to check for changes made during the document's life cycle. In addition, Electronic offers a certified signature, which is the first signature on a document. With a certified signature, the author can specify which changes are allowed to ensure integrity. Electronic Acrobat will then detect and prevent these modifications.

C. Non-repudiation

Non-repudiation is a document security service that prevents the person signing the document from denying that they signed the document. This service is often supported by authentication and timestamping capabilities.

D. Public Key Infrastructure (PKI)

A public key infrastructure (PKI) basically provides a digital certificate that allows the recipient of a document to know if a particular public key really belongs to a particular person. Digital certificates bind a person (or organization) to a public key. Certification Authorities (CAs) issue these certificates, and recipients must trust the CA that issued the certificate.

X.509 is a widely accepted certificate standard that Electronic uses. If the certificate has expired or the private key is compromised, the CA will revoke the certificate and record the revocation. As part of the digital certificate authentication process, recipients can check the status of the certificate.

The validity of a certificate can be checked using the following standard methods:

– Certificate Revocation List (CRL)
– Online Certificate Status Protocol (OCSP)

Electronic uses both CRL and OCSP. The following additional mechanisms may constitute a PKI:

– Public Key Cryptography Standards (PKCS), a set of standard protocols for PKI used by several vendors. Standards include RSA encryption, password-based encryption, extended certificate syntax, and cryptographic message syntax for Secure Multipurpose Internet Mail Extensions (S/MIME).
– Registration Authority - used to verify the biographical data of individuals wishing to receive a certificate.
– Certificate repository - repositories that store digital certificates.
– Key update, backup, restore and history - key maintenance and archiving mechanisms.
– Cross-Certification - In the unlikely event of a single global PKI, this mechanism allows users from one PKI to validate user certificates from another trusted PKI.
– Timestamp is a critical component of non-repudiation that offers a time stamp from a trusted third party.

V. CONCLUSION

The use of sensitive and critical information in electronic processes is essential for thousands of businesses and government agencies. Document security solutions use standards-based document and digital signature control methods to provide effective solutions that enhance the confidentiality and confidentiality of electronic documents and forms. A complete set of desktop and server solutions offer convenient, easy-to-

use document security capabilities that encourage users to keep information confidential and help organizations comply with the most stringent rules for sharing information electronically. The security solutions described above enable organizations to replace paper-based business processes with electronic ones to reap the benefits of increased operational efficiency, reduced costs, and improved customer and consumer satisfaction.

REFERENCES

1. http://www.en.wikipedia.org/wiki/Digital_preservation
2. http://www.en.wikipedia.org/wiki/six_key_criteria_for_providing_document_peristant_security
3. https://www.gov.uk/data/NC_framework_document_-_FINAL.pdf
4. http://www.en.wikipedia.org/wiki/Document_security
5. Adrian Spalka, Armin Cremers, and Hanno Langweg. Protecting the Creation of Digital Signatures with Trusted Computing Platform Technology Against Attacks by Trojan Horse. In IFIP Security Conference, 2001