

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

IMPORTANCE AND IMPLEMENTATION OF DIGITAL SIGNATURE IN OFFICE DOCUMENTS

Nikita Patel¹, Rakesh Patel², Ankita Gupta³

Student, B.E.(IT) Kirodimal Institute of Technology, Raigarh(C.G.), India^{1,3}

Lecturer, Department of Information Technology Kirodimal Institute of Technology Raigarh(C.G.), India²

ABSTRACT

In a document add visible signature lines to capture one or more digital signatures. Add an invisible digital signature to a document. The 2007 Microsoft Office system introduces the ability to insert a signature line into a document. You can insert signature lines only into Word documents and Excel workbooks. Law Firms Confirmation letters and documents can be digitally signed allowing law firms legal consent from their clients without them ever being in the same room. This paper is to propose a kind of digital signature which is used in office data.

I. INTRODUCTION

Digital signature or digital signature scheme is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit. Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering. A digital signature (not to be confused with a digital certificate) is an electronic rather than a written signature that can be used by someone to authenticate the identity of the sender of a message or of the signer of a document. To digitally sign an Office document, you must have a current (not expired) digital certificate. A digital signature scheme allows one to sign an electronic message and later the produced signature can be validated by the owner of the message or by any verifier. Most of the existing digital signature schemes were developed based on the use of hash function and message redundancy to resist against forgery attack.

II. HOW A DIGITAL SIGNATURE WORKS

If you are sending a sensitive document, you would want the recipient of the document to know that it was from you and you would also want to ensure that the document gets to the recipient in the very same state you sent it in, without any alterations. The process of digitally signing your document would go something like this:

- First, you should copy the document and paste it into an e-mail note.
- Second, you use a special software to obtain a mathematical summary (commonly known as a message hash) of the contract.
- Thirdly, you will use a private key that you purchased from a trusted public-private key authority for encrypting the message hash.
- Lastly, you send your document with the message hash as your digital signature.

The digital signature can be used for signing any form of electronic document whether or not the message is encrypted. The digital signature is protected with a digital certificate that authenticates it. Your digital certificate will contain the certification-issuing authority's digital signature which makes it possible for anyone to verify that your certificate is real.

Create a signature line in Word or Excel

1. In the document or worksheet, place your pointer where you want to create a signature line.

2. On the **Insert** tab, in the **Text** group, click the **Signature Line** list, and then click **Microsoft Office Signature Line**.
3. In the **Signature Setup** dialog box, type information that will appear beneath the signature line:



- **Suggested signer** : The signer's full name.
- **Suggested signer's title**: The signer's title, if any.
- **Suggested signer's e-mail address**:The signer's e-mail address, if needed.
- **Instructions to the signer**:Add instructions for the signer.

4. Select one or both of the following check boxes:

- **Allow the signer to add comments in the Sign dialog box** .Allow the signer to type a purpose for signing.
- **Show sign date in signature line** Signature date will appear with signature

Add a Digital Signature in an MS Word Document

The digital signature feature is a very useful and popular feature of Microsoft Word. This article has very useful computer support tips for common PC users.

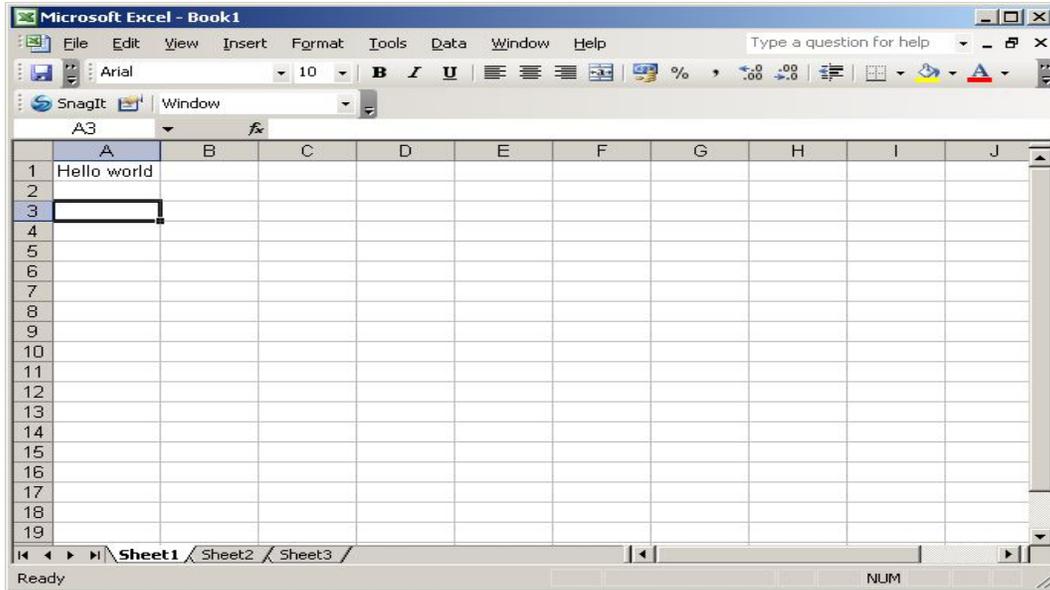
- Adding a digital signature is a process of signing your word document with an image (may be photo or image of your signature) followed by your name, designation, company, etc
- After inserting a digital signature, you can't add anything into the document. You have to remove the digital signature to append something. You can also edit your digital signature whenever you need to.

Add one or more signature lines to a document

The 2007 Microsoft Office system introduces the ability to insert a signature line into a document. You can insert signatures lines only into Word documents and Excel workbooks.A signature line looks like a typical signature placeholder that might appear in a print document, but it works differently. When a signature line is inserted into an Office document, the document author can specify information about the intended signer, as well as instructions for the signer. When an electronic copy of the document is sent to the intended signer, this person sees the signature line and a notification that his or her signature is requested. The signer can click the signature line to digitally sign the document. The signer can then either type a signature, select a digital image of his or her signature, or write a

signature by using the inking feature of the Tablet PC. When the signer adds a visible representation of his or her signature to the document, a digital signature is added simultaneously to authenticate the identity of the signer. After a document is digitally signed, it will become read-only to prevent modifications to its content.

Starting with Microsoft Office 2003, digital signatures can be added to office documents (e.g. a spreadsheet).



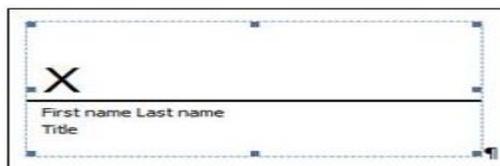
Digital signatures can be used for many types of documents where traditional pen-and-ink signatures were used in the past. However, the mere existence of a digital signature is not adequate assurance that document is what it appears to be. Moreover, government and enterprise settings often need to impose additional constraints on their signature workflows, such as restricting user choices and document behavior during and after signing.

Signature lines in Word and Excel

A signature line resembles a typical signature placeholder that might appear in a printed document. However, it works differently. When a signature line is inserted into an Office file, the author can specify information about the intended signer, and instructions for the signer. When an electronic copy of the file is sent to the intended signer, this person sees the signature line and a notification that their signature is requested. The signer can:

- Type a signature.
- Select a signature digital image.
- Write a signature by using the inking feature of the Tablet PC.

When the signer adds a visible representation of a signature to the document, a digital signature is added at the same time to authenticate the signer's identity. When you sign a signature line, you add a visible representation of your signature and a digital signature.



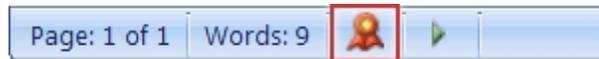
In the file, right-click the signature line. From the menu, select **Sign**. To add a printed version of your signature, type your name in the box next to the **X**. The signature line. To select an image of your written signature, click **Select Image**. In the **Select Signature Image** dialog box, find the location of your signature image file, select the file that you want, and then click **Select**.

Reducing risk with digital signatures

Using signature lines in Office files makes it possible for organizations to reduce risk when you use electronic transactions and to streamline paper processes for contracts or other agreements. Digital signatures provide a record of exactly what was signed and can be verified in the future. When the signer adds a visible signature to the document, a digital signature is added at the same time to authenticate identity. After a document is digitally signed, it becomes read-only to prevent modifications.

Add an invisible digital signature to a document

If you do not need to insert visible signature lines into a document, but you still want to provide assurance as to the authenticity, integrity, and origin of a document, you can add an invisible digital signature to the document. You can add invisible digital signatures to Word documents, Excel workbooks, and PowerPoint presentations. Unlike an Office signature line, an invisible digital signature is not visible within the contents of the document itself, but recipients of the document can determine that the document has been digitally signed by viewing the document's digital signature or by looking for the **Signatures** button on the status bar at the bottom of the screen.



After a document has been digitally signed, it becomes read-only to prevent modifications.

1. Click the **Microsoft Office Button** , point to **Prepare**, and then click **Add a Digital Signature**.
2. If you want to state your purpose for signing the document, type this information in the box under **Purpose for signing this document** in the **Sign** dialog box.
3. Click **Sign**.

Add invisible digital signatures in Word, Excel, or PowerPoint

To protect the authenticity of a document's content, you can add an invisible digital signature. Signed documents have the **Signatures** button at the bottom of the document.



1. Click the **File** tab.

2. Click **Info**.
3. Under **Permissions**, click **Protect Document**, **Protect Workbook** or **Protect Presentation**.
4. Click **Add a Digital Signature**.
5. Read the Word, Excel, or PowerPoint message, and then click **OK**.
6. In the **Sign** dialog box, in the **Purpose for signing this document** box, type the purpose.
7. Click **Sign**.

Remove a digital signature from an Office document

You can remove a digital signature from a Microsoft Office document that has been digitally signed.

1. Open the document that contains the signature you want to remove.
2. Click the Microsoft Office Button , point to Prepare, and then click View Signatures.
3. In the Signatures task pane, point to the signature that you want to remove, click the arrow that appears on the right, and then click Remove Signature.
4. When you are asked if you want to permanently remove the signature, click Yes.

Remove invisible digital signatures from Word, Excel, or PowerPoint

1. Open the document, worksheet, or presentation that contains the invisible signature you want to remove.
2. Click the File tab.
3. Click Info.
4. Click View Signatures.
5. The document, worksheet, or presentation view returns, and the Signatures pane appears.
6. Next to the signature name, click the arrow.
7. Click Remove Signature.
8. Click Yes.

Digitally sign with a stamp

This topic explains how you can digitally sign a Microsoft Office document with a stamp in Word documents and Excel workbooks. If a document is changed after it is signed, the signature is invalidated.

Insert a stamp signature line into an Office document

The feature is only available if you:

- Are using the Chinese (Simplified), Chinese (Traditional), Japanese, or Korean language version of Microsoft Office, or
- Installed the 2007 Microsoft Office system Multi-Language Pack for one of these languages, or
- Enabled support for one of these languages through the Microsoft Office Language Settings.

III. DIGITAL SIGNATURE TECHNOLOGY

A. Functions of Digital Signature

Digital Signature is a method to encrypt a message (such as documents, contracts, notifications) which will be transferred, adopting data-exchanging protocol and data-encrypting algorithm. An abstract is produced in this procession. The abstract is like signature or seal which can be used by receiver to verify the identity of the sender .

functions of digital signature:

- (1)Assuring data integrity. Once the message changes a little, the abstract will change a lot for hash function’s peculiarity, so that avoids the message being distorted.
- (2)Anti-denibility. Using public key cryptography algorithm, the sender can’t deny that he has sent the message for he has the private key.
- (3)Avoiding receivers forging message that is claimed to be from the sender.

B. Public Key Encrypting Scheme

As the base of digital signature technology, public key encrypting technology should be introduced first in the following content. In the traditional cryptography system, the cipher code used in the process of encrypting plain text into cipher text and in the inverse process is the same. This method is called symmetric cryptography technology. Public key encrypting scheme is a kind of unsymmetric cryptography technology. It resolves the difficult problems in application. Its basic idea: the keys of the two parties are different. Every user has a key pair. One is private key which is saved by the user himself, another one is issued in public places such as internet for downloading or enquiring. Public key algorithm is very slow (with contrast to private algorithm). It is designed for a little data, but not for much data. It is usually used together with hash function in digital signature.

C. Hash Algorithm

Hash algorithm is an algorithm which is used to compute a data fingerprint of a data block. It is a one-way function. Which satisfies the following conditions:

- 1) Can receive data with any length;
- 2) Can produce abstract with fixed length;
- 3) Can compute abstract easily;
- 4) Can not compute message from abstract.

Attacks and Forgeries

- attacks
 - key-only attack
 - known message attack
 - generic chosen message attack
 - directed chosen message attack
 - adaptive chosen message attack
- break success levels
 - total break
 - selective forgery
 - existential forgery

Digital Signature Requirements

- must depend on the message signed
- must use information unique to sender
- to prevent both forgery and denial



- must be relatively easy to produce
- must be relatively easy to recognize & verify
- be computationally infeasible to forge
 - with new message for existing digital signature
 - with fraudulent digital signature for given message
- be practical save digital signature in storage

IV. USES OF DIGITAL SIGNATURES

- a) Authentication
- b) Integrity
- c) Non-repudiation

a) Authentication:

Digital signatures can be used to authenticate the source of messages.

b) Integrity:

If a message is digitally signed, any change in the message after signature will invalidate the signature. The message cannot be modified, and if modified a new message with a valid signature cannot be produced.

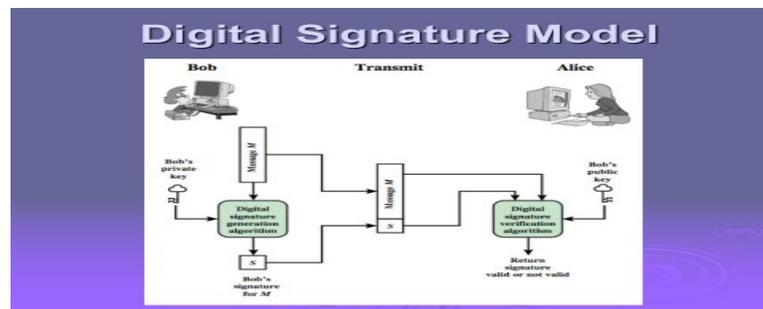
c) Non - repudiation :

It is an important aspect of digital signatures. A sender cannot deny having sent the document after signing it.

Advantages of Digital Signatures

The following are the main benefits of using digital signatures:

- Speed: Businesses no longer have to wait for paper documents to be sent by courier. Contracts are easily written, completed, and signed by all concerned parties in a little amount of time no matter how far the parties are geographically.
- Costs: Using postal or courier services for paper documents is much more expensive compared to using digital signatures on electronic documents.
- Security: The use of digital signatures and electronic documents reduces risks of documents being intercepted, read, destroyed, or altered while in transit.
- Authenticity: An electronic document signed with a digital signature can stand up in court just as well as any other signed paper document.



Disadvantages of Digital Signatures

Just like all other electronic products, digital signatures have some disadvantages that go with them. These include:

- Expiry: Digital signatures, like all technological products, are highly dependent on the technology it is based on. In this era of fast technological advancements, many of these tech products have a short shelf life.
- Certificates: In order to effectively use digital signatures, both senders and recipients may have to buy digital certificates at a cost from trusted certification authorities.
- Software: To work with digital certificates, senders and recipients have to buy verification software at a cost.
- Law: In some states and countries, laws regarding cyber and technology-based issues are weak or even non-existent. Trading in such jurisdictions becomes very risky for those who use digitally signed electronic documents.
- Compatibility: There are many different digital signature standards and most of them are incompatible with each other and this complicates the sharing of digitally signed documents.

V. CONCLUSION

This topic explains what a digital signature (also called digital ID) is, what it can be used for, and how you can use digital signatures in Microsoft Office Word 2007, Microsoft Office Excel 2007, and Microsoft Office Power Point 2007 . Increasingly, digital signatures are being used in Office Documents. Signatures facilitate validation and verification of the authenticity of paper documents, Validation refers to the process of certifying the contents of the document, while authentication refers to the process of certifying the sender of the document .In this article, the terms document and message are used interchangeably. digital signatures serve the purpose of validation and authentication of electronic documents. This technology is rather new and emerging and is expected to experience growth and widespread use in the coming years. Digital signatures are computed based on the documents (message/information) that need to be signed and on some private information held only by the sender.

VI. REFERENCES

1. *Cryptography and Network Security Fifth Edition by William Stallings*
2. *US ESIGN Act of 2000*
3. *The University of Virginia State of WI*
4. *National Archives of Australia*
5. *4 Malkin T, Micciancio D, Miner S. Efficient Generic Forward-secure Signatures with an Unbounded Number of Time Periods[C]. Proc. Of Advances in Cryptology-EUROCRYPT. 2002*
6. *Nahid Hasan, Founder and CEO of OutsourceBD.Net and a full time niche blog writer.*
7. *Margaret Rouse 2000 - 2014, TechTarget*
8. *2014 Microsoft Corporation*
9. *Didier Stevens Monday 5 January 2009*