ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 5, Special Issue 14, December 2016

3rd National Conference on Recent Trends in Computer Science and Engineering and Sustainability in Civil Engineering (TECHSYNOD'16)

19th, 20th and 21st December 2016

Organized by

Department of CSE, MCA &CE, Mohandas College of Engineering and Technology, Thiruvananthapuram, Kerala, India

A Survey on Digital Signature Schemes

Reji PI, Rashmi S Nair

Asst. Professor, Computer Science and Engineering, Mohandas College of Engineering and Technology, Thiruvananthapuram, Kerala, India

Asst. Professor, Computer Science and Engineering, Mohandas College of Engineering and Technology, Thiruvananthapuram, Kerala, India

ABSTRACT: Digital signature is a method to provide authenticity and integrity to the digital data. In this paper we discuss different types of digital signatures. The key generation, signing and verification of Digital Signatures with appendix, Digital signatures with message recovery, Digital signatures based on RSA and Blind signature schemes is discussed. The drawback of each method is also mentioned.

KEYWORDS: RSA, Blind signature, authenticity, integrity

I. INTRODUCTION

A digital signature is a mathematical scheme to demonstrate the authenticity of a digital data. A valid digital signature allows the recipient to believe that the message was created by a known sender proving the authentication and non-repudiation of the data and also that the message was not altered during its transmission. A digital signature must be verifiable, i.e., if a dispute arises an unbiased third party must be able to solve the dispute equitably, without requiring access to the signer's secret

A digital signature scheme consists of basically three algorithms:

- A key generation algorithm for the generation of unique private keys and a corresponding public key.
- A *signing* algorithm produces a signature when provided with a message and a private key.
- A *signature verifying* algorithm checks the authenticity of given message.

II. APPLICATIONS OF DIGITAL SIGNATURES

Digital signatures can provide assurance of the evidence to provenance, identity, and status of an electronic document as well as acknowledging informed consent and approval by a signatory.

- **Authentication**
  Digital signatures can be used to authenticate the source of messages. When ownership of a digital signature secret key is bound to a specific user, a valid signature shows that the message was sent by that user.
- **Integrity**
  There are situations where there is a need for confidence that the message has not been altered during transmission. Although encryption hides the contents of a message, it may be possible to *change* an encrypted message without understanding it. However, if a message is digitally signed, any change in the message after signature invalidates the signature.
- **Non-repudiation**
  Non-repudiation is an important aspect of digital signatures. An entity that has signed some information cannot at a later stage deny having signed it.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 5, Special Issue 14, December 2016

3rd National Conference on Recent Trends in Computer Science and Engineering and Sustainability in Civil Engineering (TECHSYNOD'16)

19th, 20th and 21st December 2016

Organized by

Department of CSE, MCA &CE, Mohandas College of Engineering and Technology, Thiruvananthapuram, Kerala, India

III. DIFFERENT TYPES OF DIGITAL SIGNATURES ARE

- Digital Signatures with appendix
- Digital signatures with message recovery
- Digital signatures based on RSA
- Blind signature schemes

A. DIGITAL SIGNATURES WITH APPENDIX

Key generation Process

- Alice selects a private key which defines a signing algorithm SA which is a one-to-one mapping SA: Mh → S
- Alice defines the corresponding public key defining the verification algorithm VA such that VA(m*, s) = true if SA(m*) = s and false otherwise, for all m*∈ Mh and s∈S, where m* = h(m) for m ∈ M.
- The public key VA is constructed such that it may be computed without knowledge of the signer's private key SA

Signature generation process

- Compute **m* = h(m)**, **s = SA(m*)**
- Send **(m, s)**

Signature verification process

- Obtain A's public key **VA**
- Compute **m* = h(m)**, **u = VA(m*, s)**
- Accept the signature iff **u = true**

Here M is the message space , h is a hash function with domain M, Mh is the image of h and S is the signature space
Examples: ElGamal, DSA, DSS.

B. DIGITAL SIGNATURES WITH MESSAGE RECOVERY

Key generation

- A selects a private key defining a signing algorithm SA which is a one-to-one mapping SA: MS → S
- A defines the corresponding public key defining the verification algorithm VA such that VA•SA is identity map on MS.
- The public key VA is constructed such that it may be computed without knowledge of the signer's private key SA

The signing process

- Compute **m* = R(m)**, **R** is a **redundancy function** (invertible)
- Compute **s = SA(m*)**
- Obtain authentic public key VA
- Compute m* = V(s)

The signature verification process

Verify if m* ∈ MS (if not, reject the signature)
Recover the message m = R-1(m*)

Here M is the message space, MS is the signing space and S is the signature space.

C. DIGITAL SIGNATURES BASED ON RSA

Key generation

1. Generate two **large**, **distinct primes** *p, q* (100÷200 decimal digits)
2. Compute $n = p \times q$ and $\varphi = (p-1)\times(q-1)$

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 5, Special Issue 14, December 2016

3rd National Conference on Recent Trends in Computer Science and Engineering and Sustainability in Civil Engineering (TECHSYNOD'16)

19th, 20th and 21st December 2016

Organized by

Department of CSE, MCA &CE, Mohandas College of Engineering and Technology, Thiruvananthapuram, Kerala, India

3. Select a **random number** $1 < e < \varphi$ such that $\gcd(e, \varphi) = 1$
4. Compute the **unique** integer $1 < d < \varphi$ such that $ed \equiv 1 \bmod \varphi$
5. (d, n) is the private key
6. (e, n) is the public key

At the end of key generation, p and q must be destroyed

Signature generation. In order to sign a message m, A does the following

1. Compute m* = R(m) an integer in [0, n–1]
2. Compute s = m*d mod n
3. A's signature for m is s

Signature verification. In order to verify A's signature s and recover message m, B does the following

1. Obtain A's authentic public key (e, n)
2. Compute m* = se mod n
3. Verify that m* is in MR; if not reject the signature
4. Recover m = R-1(m*)

D. BLIND SIGNATURE SCHEMES

Blind signature schemes are two-party protocols between a sender A and a signer B. The basic idea is the following A sends a piece of information to B which B signs and returns to A . From this signature, A can compute B 's signature on an a priori message M of A 's choice. At the completion of the protocol, B knows neither the message M nor the signature associated with it. The purpose of a blind signature is to prevent the signer B from observing the message it signs and the signature; hence, it is later unable to associate the signed message with the sender A.

IV. COMPARISON OF THE DIFFERENT METHODS USED:

Method	Specialty
Digital Signatures with appendix	Require the message as input to the verification
Digital signatures with message recovery	A priori knowledge of the message is not required for the verification algorithm
Digital signatures based on RSA	Includes the features of both Digital Signatures with appendix and Digital signatures with message recovery
Blind Signature Schemes	Allows sender A to remain anonymous so that spending patterns cannot be monitored

Table1: Comparison between the different methods discussed.

V. CONCLUSION

We have discussed about various methods of digital signatures. Each method has its pros and cons. On the basis of the significance of the application we can make use of any one of the methods mentioned above.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization *Volume 5, Special Issue 14, December 2016*

3rd National Conference on Recent Trends in Computer Science and Engineering and Sustainability in Civil Engineering (TECHSYNOD'16)

19th, 20th and 21st December 2016

Organized by

Department of CSE, MCA &CE, Mohandas College of Engineering and Technology, Thiruvananthapuram, Kerala, India

REFERENCES

[1] Boyd C. (1986). Digital multi-signature, In Cryptography and Coding. Editors, Beker H.J. and Piper F. C., Clarendon Press, London, p.p. 241 – 246.
[2] D. Stinson, Cryptography, Theory and Practice, CRC Press, Second edition, 2000.
[3] W. Stallings, Cryptography and Network Security: Principles and Practice, Second edition, Prentice Hall, 1999.
[4] . J. Menezes and P. C. van Oorschot and S. A. Vanstone, Handbook of Applied cryptography, vCRC Press, 1996.