ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Digital Signature System

Fajer Aldeen Kahled
B.Tech Student,
Department of CSE,
Lords Institute of Engineering and Technology.

Nasar Abdallah Saeed
B.Tech Student,
Department of CSE,
Lords Institute of Engineering and Technology.

G.Shaik Mahboob
M.Tech,
Department of CSE,
Lords Institute of Engineering and Technology.

ABSTRACT

Digital signature is cryptography method used for converting the data into different form and the data can be read by using a key. The digital signature is authentication process to accept a license on a online interface. Digital signatures are different from electronic signatures and these are based on mathematical algorithms.

The digital signature is a document which is based on the owner's private key. In this paper we will see how digital signature cryptography algorithms are implemented and how they are transmitted over the network.

Information on digital signature types, key hash algorithm, uses are explained in digital signature power point presentation.

INTRODUCTION

This application makes use of Digital Signature Algorithm (DSA) along with a hash function. The hash code is provided as input to a signature function along with a random number generated for this particular signature. The signature function also depends on the sender's private key and a set of parameters known to a group of communicating principals. This set constitutes a global public key. The result is a signature consisting of two components

At the receiving end, verification is performed. The receiver generates a quantity that is a function of the public-key components, the sender's public key, and the hash code of the incoming message. If this quantity matches with one of the components of the signature, then the signature is validated.

This application makes sure that the security services Authentication, Secrecy, Integrity, and Non-repudiation are provided to the user. This application allows keeping the information out of the hands of unauthorized persons. This is called Secrecy.

It also deals with determining whom a person is communicating with before revealing sensitive information or entering a business deal. This is called Authentication.

EXISTING SYSTEM

These days almost all organizations around the globe use a messaging system to transfer data among their employees through their exclusive intranet. But the security provided is not of high standards. More and more unauthorized people are gaining access to confidential data.

DISADVANTAGES OF EXISTING SYSTEM:

- The validity of sender is not known.
- The sender may deny sending a message that he/she has actually sent and similarly the receiver may deny the receipt that he/she has actually received.
- Unauthorized people can gain access to classified data.
- Intruders can modify the messages or the receiver himself may modify the message and claim that the sender has sent it.

PROPOSED SYSTEM

The system will provide the following security services:

Confidentiality:

Confidentiality is the protection of transmitted data from passive attacks. With respect to the release of message contents, several levels of protection can be identified. The broadest service protects all user data transmitted between two users over a period of time.

For example, if a virtual circuit is set up between two systems, this broad protection would prevent the release of any user data transmitted over the virtual circuit. Narrower forms of this service can also be defined, including the protection of a single message or even specific fields within a message. These refinements are less useful than the broad approach and may even be more complex and expensive to implement. The other aspect of confidentiality is the protection of traffic flow from analysis. This requires that an attacker not be able to observe the source and destination, frequency, length, or other characteristics of the traffic on a communications facility.

Authentication:

The authentication service is concerned with assuring that a communication is authentic. In the case of a single message, such as a warning or alarm signal, the function of the authentication service is to assure the recipient that the message is from the source that it claims to be from. In the case of an ongoing interaction, such as the connection of a terminal to a host, two aspects are involved. First, at the time of connection initiation, the service assures that the two entities are authentic (i.e. that each is the entity that it claims to be).

Second, the service must assure that the connection is not interfered with in such a way that a third party can masquerade as one of the two legitimate parties for the purposes of unauthorized transmission or reception.

Integrity:

Integrity basically means ensuring that the data messages are not modified. An integrity service that deals with a stream of messages assures that messages are received as sent, with no duplication, insertion, modification, reordering or replays. The destruction of data is also covered under this service. Thus the integrity service addresses both message modification and denial of service.

Non-repudiation:

Non-repudiation prevents either sender or receiver from denying a transmitted message. Thus, when a message is sent, the receiver can prove that the message was in fact sent by the alleged sender.

Similarly, when a message is received, the sender can prove that the message was in fact received by the alleged receiver.

RSA Approach

In the **RSA** approach, the message to be signed is input to a hash function that produces a secure hash code of fixed length. This hash code is then encrypted using the sender’s private key to form the signature. Both the message and the signature are then transmitted. The recipient takes the message and produces a hash code.

The recipient also decrypts the signature using the sender’s public key. If the calculated hash code matches the decrypted signature, the signature is accepted as valid. Because only the sender knows the private key, only the sender could have produced a valid signature.

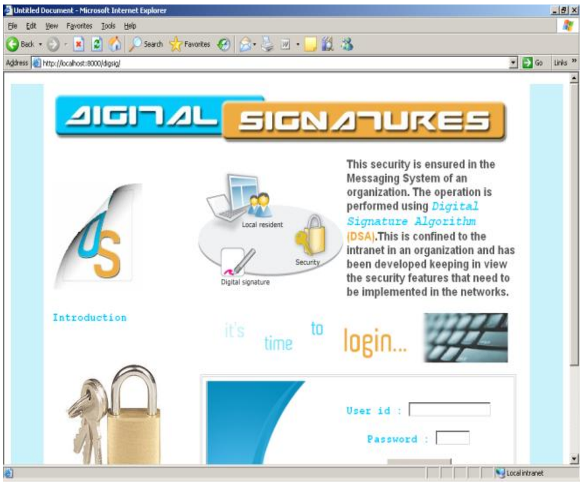
DSS Approach

The Digital Signature Standard approach also makes use of a hash function. The hash code is provided as input to a signature function along with a random number generated for this particular signature. The signature function also depends on the sender’s private key and a set of parameters known to a group of communicating principals.

This set constitutes a global public key. The result is a signature consisting of two components.

SCREEN SHOTS:

Home:

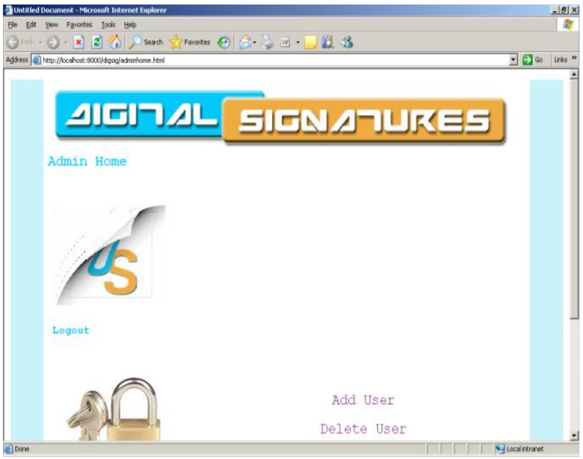


This security is ensured in the Messaging System of an organization. The operation is performed using Digital Signature Algorithm (DSA).This is confined to the intranet in an organization and has been developed keeping in view the security features that need to be implemented in the networks.

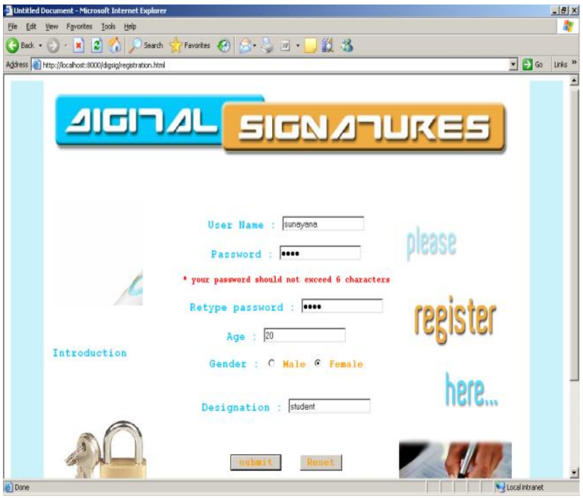
User id :

Password :

Authority Home:


Untitled Document - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://localhost:8000/digsig/adminhome.html
Go Links
DIGITAL SIGNATURES
Admin Home
Logout
Add User
Delete User
Done
Local intranet

Add User:


Untitled Document - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://localhost:8000/digsig/registration.html
Go Links
DIGITAL SIGNATURES
Introduction
please register here...
submit
Reset
Done
Local intranet

User Name : sunayana

Password : ••••

* your password should not exceed 6 characters

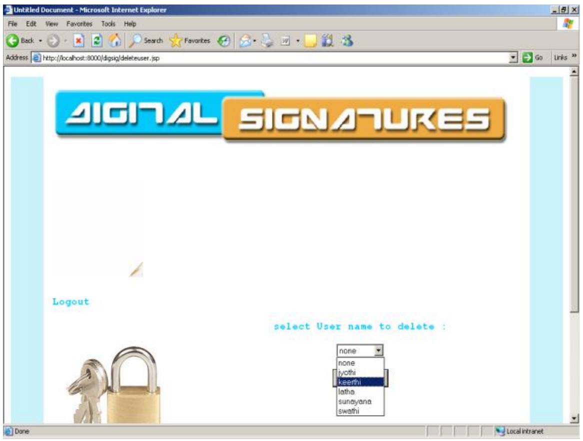
Retype password : ••••

Age : 20

Gender : ○ Male ● Female

Designation : student

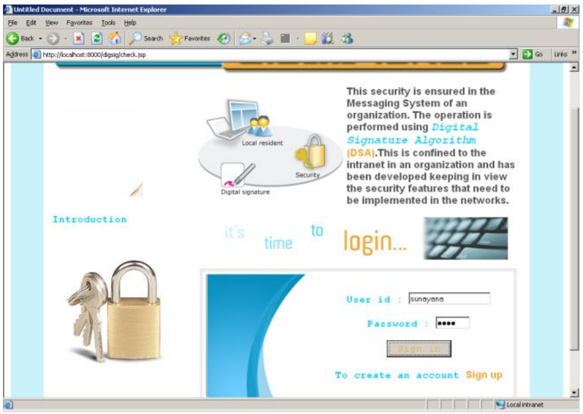
Delete User:


Untitled Document - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://localhost:8000/digsig/deleteuser.jsp
Go Links
DIGITAL SIGNATURES
Logout
Done
Local intranet

select User name to delete : none

- none
- jyothi
- keerthi
- latha
- sunayana
- swathi

User Login:


Untitled Document - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://localhost:8000/digsig/check.jsp
Go Links
Local resident
Security
Digital signature
Introduction
it's time to login...
Sign in
Local intranet

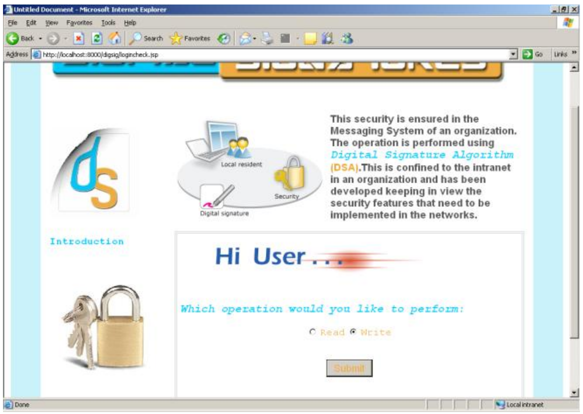
This security is ensured in the Messaging System of an organization. The operation is performed using Digital Signature Algorithm (DSA).This is confined to the intranet in an organization and has been developed keeping in view the security features that need to be implemented in the networks.

User id : sunayana

Password : ••••

To create an account Sign up

User Home:


Untitled Document - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://localhost:8000/digsig/logincheck.jsp
Go Links
Local resident
Security
Digital signature
Introduction
Submit
Done
Local intranet

This security is ensured in the Messaging System of an organization. The operation is performed using Digital Signature Algorithm (DSA).This is confined to the intranet in an organization and has been developed keeping in view the security features that need to be implemented in the networks.

Hi User...

Which operation would you like to perform:

○ Read ● Write

CONCLUSION

Digital signatures are used for used in biometric identifiers. The usage of digital signature has been growing in areas of security agencies and in law enforcement and in consumer marketing agencies. This is secure method for performing the license agreements on a online basis.

REFERENCES

1. Mindi McDowell, Allen Householder. National Cyber Alert System Cyber Security Tip ST04-018. Available: http://www.us-cert.gov/cas/tips/ST04-018.html. Last accessed 28th Oct 2009.

2. Bengisu Tulu, Haiqing Li, Brian Hilton, Samir Chatterjee, Thomas Horan. (INDER SCIENCE PUBLISHERS). Implementing digital signatures for healthcare enterprises: the case of online disability evaluation reports. International Journal of Healthcare Technology and Management 2005 . 6

3. WS-Security Authentication and Digital Signatures with Web Services Enhancements . Available: http://msdn.microsoft.com/en-us/library/ms996951.aspx. Last accessed 28th Oct 2009.

4. Ricky M. Magalhaes. (May 29, 2003). Authentication, Access Control & Encryption. Digital Signatures.

5. American Bar Association. Digital Signature Guidelines. Available: 5. http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html . Last accessed 29th Oct 2009.

6. CGI Group. Public Key Encryption and Digital Signature. Available: 1. http://www.cgi.com/cgi/pdf/cgi_whpr_35_pki_e.pdf. Last accessed 29th Oct 2009.

7. your Dictionary.com. digital signature definition - computer. Available: http://www.yourdictionary.com/computer/digital-signature. Last accessed 29th Oct 2009.

8. John Smith. Adobe LiveCycle® Server Digital Signatures ES. Available: http://learn.adobe.com/wiki/display/security/Digital+Signatures. Last accessed 29th Oct 2009.

9. cryptobot e-sign. Security Robot for "Encrypting, Sending, Decrypting and Storing" Your e-Document & e-Signature. Available: http://www.cryptbot.com/e_sign.asp. Last accessed 29th Oct 2009.

10. Sinewave Computer Services Pvt. Ltd. Digital Certificate. Available: http://www.sinewave.co.in/Products/DigitalCertificate/DigitalCertificate.htm?gclid=CPCLiOr8450CFQEupAod0Wb9Ow. Last accessed 30th Oct 2009.

11. Journal of AHIMA. (1998). Implementing Electronic Signatures . Available: http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_021585.hcsp?dDocName=bok1_021585. Last accessed 30th Oct 2009.

12. Karen Pauli. (Oct 2007). Electronic Signature and Secure Forms in the Insurance Industry: Taking the P&C Pen to the Web. Available: http://www.adobe.com/financial/pdfs/electronic_secure_forms.pdf. Last accessed 30th Oct 2009.

13. Dr Paul Schapper. Authentication & Digital Signatures in E- Law and Security. Available: http://idbdocs.iadb.org/wsdocs/getdocument.aspx?docnum=645472. Last accessed 30th Oct 2009.

14. Mindi McDowell . How to Use Encryption and Digital Signatures . Available: http://www.bestsecuritytips.com/xfsection+article.articleid+166.htm. Last accessed 30th Oct 2009.

15. silicon.com . (2001). Seven Steps to Digital Signature Implementation. Available: http://whitepapers.silicon.com/0,39024759,60010898p,00.htm. Last accessed 30th Oct 2009.