Table of Contents

A digital code (generated and authenticated by public key encryption) which is attached

To an electronically transmitted document to verify its contents and the sender's identify.

A digital signature is a most mathematical scheme for demonstrating the authenticity of a digital message or documents .

A valid digital signature gives a recipient reason to believe that the message was created by a known sender and that the message was not altered in transit

Digital signatures are a standard element of most cryptographic protocolare commonly used for software distribution.

Applications of digital signatures:

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

The United States govt. printing office (GPO) publishers electronic version of the budget.

For additional security there are some precautions:

Putting a private key on smart card:

All public key/private key cryptosystem depend entirely on keeping the private secret .A private key can be stored on a user’s computer and protected by a local password but this has two disadvantages

The user can omly sign documents on that particular computer.

The security of the private key depended entirely on the security of the computer.

Using smart card readers with a separate keyboard:

Enter in a pin code to activate the smart card commonly requires a numeric keypad.

Other smart card design:

Smart card design is active field ,and there are smart card schemes which are intended to avoid these particular problems ,though so far with little security profs.

Using digital signature only with trusted applications:

One of the main difference b/w a digital signature is that the user does not “see” what he signs.

Related Posts:

1. Types of Attack
2. Security threats
3. Computer and cyber security
4. Introduction to network security
5. Intrusion detection tool
6. Categories of security assessments
7. Security terminologies and principals
8. Intodoction to intrusion
9. Intrusion detection tool
10. Categories of security assessments
11. Intrusion terminology
12. Cryptography attacks
13. Cryptography
14. SSH
15. MD5
16. Message digest functions
17. Authentication Functions
18. One way hash function
19. Hash function in network web security
20. Digital signature standard
21. SSL Secure socket layer