

# PKI Options for Secure EMail

This paper can form a foundation for implementing PKI Based Email Security Solutions. This is in the form of a questionnaire that lists out the requirements. Several members of the industry and individuals have contributed by providing content and editing. The audience for this Technical Perspective includes both the businessperson looking for a high level description of the technology and the IT professional who is unfamiliar with PKI and Email Security concepts. Our goal is to familiarize the reader with the requirements of PKI and Email Security, the architectural components and how they interact. More on understanding of PKI can be found in a related paper named "What is PKI?".

It has been internationally recognized that **E-Mail Authentication** is achieved only with **PKI**. The requirements of e-mail security are as follows:

- R1. Message confidentiality using encryption** - protects your sensitive information from being viewed by anyone other than the intended recipients.
- R2. Authentication with digital signatures** - verifies that the sender and the recipient are exactly who they say they are.
- R3. Integrity with digital signatures** - ensures the contents of your email cannot be altered in transit without detection.
- R4. Non-repudiation with digital signatures** - ensures the sender cannot deny emailing the message at a later date (this is particularly vital with financial transactions being conducted and authorized over email)

"PKI Options for Secure Email" - is a deliverable from the Wonder Software's Business Solutions Group (BSG). Several member organizations and individuals have contributed by providing content, editorial assistance and editorial reviews.

Authors:

R K Verma  
Gromax Infonet

R Saran  
Wonder Software Tech.

## **On with PKI**

A true **PKI EMail Security Solution** is expected to meet the following:

PKI Secure Messaging Requirements:

- Message confidentiality using encryption: **R1**
- Authentication with digital signatures: **R2**
- Integrity with digital signatures: **R3**
- Non-repudiation with digital signatures: **R4**
- Revocation: **R5**
- Historical Data Recovery and Verification: **R6**
- External Communication: **R7**
- Roaming: **R8**

## **PKI Technology Requirements**

- PKI Architectures: **PKI**
  - 1 CA support:
  - 2 Revocation Support:

- Cryptographic Algorithms: Algorithms
  - EA Encryption Algorithms:
    - DES
    - RC2
    - RC4
    - AES
  - HA Hash Algorithms:
    - MD5
    - SHA-1
    - SHA
  - SA Signature Algorithms:
    - RSA
    - DSA
- Standards Compliance: Standards
  - 1 X.509 Digital Certificate:
  - 2 DSA/RSA Signing:
  - 3 DES/CAST/IDEARC2/RC4/AES/TWOFISH/RSA Encryption:
  - 4 Mobile Cryptographic Tokens(Smart Card, USB Tokens):

## **Key Life Cycle Management**

- Key Life Cycle Management: Key Life Cycle Management
  - User Initialization: **UI**
    - 1 Offline Creation of Private Key and Self Signed Certificate:
    - 2 Offline Creation of Certificate Signing Request: To get the public key signed by CA at a later time.
    - 3 Offline Installation of Owner's Public Key:
    - 4 Online Creation of Private Key and Digital Certificate:
    - 5 Safe Acceptance of the CA public key: Automatic display of certificate before optional installation.
  - Key Pairs: **KP**
    - 1 Key Pairs Expiration Date:
    - 2 Historical Records of Expired Certificates: Storage of expired certificates in marked location.
    - 3 Transparency of Keys to Users:
  - Key Backup / Restore: **KBR**
    - 1 Key Backup and Restore:
    - 2 Historical Data availability:
  - Password Management: **PM**
    - 1 Different Passwords for different Private Keys:
    - 2 Password Rules: e.g. Min Password length etc.
    - 3 Password safety: e.g. Support for Password change etc.
  - Certificate Revocation: **CR**
    - 1 Certificate Revocation List Support:
    - 2 Off-Line Revocation Checking Capability:
    - 3 Historical record of Revoked Certificates:

## **Client Software: Some Essentials**

- Client Software: Client Software

- 1 Client Side Software Support:
- 2 Easy Client Software Installation:
- 3 Private Keys Protection: Protection extra to password provided.
- 4 Off-line Capability: Write/Sign/Encrypt mail offline, send at a later time.
- 5 Verification of Historical Signatures: Public key attached with the document.
- 6 Transparency: Regular dialogs to inform the user of the beginning and end of an activity.
- 7 User Mobility: Private Key on mobile smart-card or other token.

## **PKI Management: Some Essentials**

- PKI Management: PKI Management
  - PKI Management Transactions using the software
    - 1 CA Certificate Installation:
    - 2 Other's Certificate Installation:
    - 3 Basic Revocation Checking:
    - 4 External Revocation Checking:
    - 5 Private Key Backup and Restore:

## **Platforms**

- Platforms
  - Client Operating Systems
    - MS Windows 95
    - MS Windows 98
    - MS Windows ME
    - MS Windows NT3.1
    - MS Windows NT4
    - MS Windows CE
    - MS Windows 2000
    - MS Windows XP
    - Sun Solaris
    - Redhat Linux
    - HPUX
    - IBM
    - Novell Client
    - MS Internet Explorer
    - Netscape Navigator
  - Directory Support
    - MS Active Directory
    - Novell Directory Server
    - LDAP Directory Support

## **Client Software: Utilities**

- Utilities
  - E-Mail Signing
    - Text Message
    - File Attachment

- E-Mail Encryption
  - Text Message
  - File Attachment
- Mail Client Independence
- Mail Account Independence
- Free Signed Mail Verifier for the recipient
- Free Encrypted Mail Reader for the recipient
- Ease of Use
  - Sign/Verify mail directly on current window of any mail client
  - Cut from mail client and paste in application window to Sign/Verify

### **Protection of the Protector**

A security guard without a gun means the guard himself is unprotected. The password or if PKI is being used then the private key are the protector of the user. It is important to know as to how does the solution protect the password or the private key of the user.

1. While using a message broker service it is obvious that the password is known to the third party using which they provide connectivity.
2. If PKI is being used and the private key is stored on the hard drive, then anyone who knows the password can sign as the user. However, if the private key is stored on a removable and mobile token such as Smart-Card or USB token then this can be considered as secure.

### **Mail Client, Account & Server Independence**

The user may find himself in difficulty if suddenly he realizes that a new email id that he created with another email service provider cannot be used with the security solution that he has. Hence, mail client independence is as important as any other feature of the solution. Moreover, security solutions are self-centric, this means that the sender and the recipient somehow must use the solution. Thus if the sender becomes mail client dependent then so does the recipient.

1. If the software forces the user to use a specific mail client, account or server then the solution may be used only within a closed group.
2. However, if the software allows the user to use any mail client, account or server then the solution can be used freely for correspondence by anyone with anyone.

### **Everybody Must Buy**

It is normal for any solution provider to expect that every user of his solution will buy it. However, for the user this is a problem. In a situation where a buyer of the solution must correspond in security and with authentication with several people, some of whom are not willing to buy the solution, then the user's capability becomes limited and he must find a different solution that does not force the recipient to buy to read the message or to verify the sender's signature on it. Hence, there can be two kinds of solutions.

1. The solutions that force the recipient to buy the solution or join a closed group.
2. The solutions that make available a free version of the software that any recipient can use to verify and read the messages received.

### **Mobility**

The last question a user must ask while evaluating various options of Email Security Solutions is that will he really be mobile with the solution he is paying for. By mobility it means the solution can be used from anywhere. The best example of anywhere is a Cyber Café. The user goes to a cyber café, wants to write or

receive mail on his existing email account. However, he desires the same level of email security that he has in his office or home. How does he get it?

1. The solution must be available in the Cyber Café or at least be available for free download.
2. If the solution is password based then the user should remember his password.
3. If the solution is PKI based then the user must have his private key with him.