American International Journal of Sciences and Engineering Research
Vol. 1, No. 1; 2018
Published by American Center of Science and Education, USA

Public-key Infrastructure

K. M. Anwarul Islam
Department of Business Administration
The Millennium University, Dhaka, Bangladesh

Md. Rezaul Karim Miajee
Faculty of Computer Science and Technology
The Millennium University, Dhaka, Bangladesh

Received: September 9, 2018 Accepted: September 22, 2018 Online Published: November 30, 2018

Abstract
This paper presents the profiles related to public-key Infrastructure (PKI) for the Internet. The PKI manages public keys automatically through the use of public-key certificates. It provides a basis for accommodating interoperation between PKI entities. A large-scale PKI issues, revokes and manages digital signature public-key certificates to allow distant parties to reliably authenticate each other. A sound digital signature PKI should provide the basic foundation needed for issuing any kind of public-key certificate.

Keywords: Public-key, Infrastructure, PKI.

Internet Publications for Standards

The Internet Activities Board (IAB) is the body responsible for coordinating Internet design, engineering and management. The IAB has two subsidiary task forces: • The Internet Engineering Task Force (IETF), which is responsible for short-term engineering issues including Internet standards. • The Internet Research Task Force (IRTF), which is responsible for long-term research. The IETF working groups meet three times annually at large conventions to discuss standards development, but the development process is conducted primarily via open email exchanges. Participants of IETF are individual technical contributors, rather than formal organisational representatives. The most important series of Internet publications for all standards specifications appear in the Internet Request for Comments (RFCs) document series. Anyone interested in learning more about current developments on Internet standards can readily track their progress via e-mail. Another important series of Internet publications are the Internet Drafts. These are working documents prepared by IETF, its working groups, or other groups or individuals working on Internet technical topics. Internet Drafts are valid for a maximum of six months and may be updated, replaced or rendered obsolete by other documents at any time. Specifications that are destined to become Internet standards evolve through a set of maturity level as the standards evolve, which has three recognised levels: Proposed Standard, Draft Standard and Refined Standard. To review the complete listing of current Internet Drafts, Internet standards associated with PKI will be briefly summarised in the following. A public directory service or repository that can distribute certificates is particularly attractive. The X.500 standard specifies the directory service. A comprehensive online directory service has been developed through the ISO/ITU standardisation processes. These directory standards provide the basis for constructing a multipurpose distributed directory service by interconnecting computer systems belonging to service providers, governments and private organisations. In this way, the X.500 directory can act as a source of information for private people, communications network components or computer applications. When the X.500 standards were first developed in 1984–1988, the

use of X.500 directories for distributing public-key certificates was recognised. Therefore, the standards include full specifications of data items required for X.500 to fulfil this role. Since the X.500 technology is somewhat complex, adoption of X.500 was slower than expected until the mid-1990s. Nevertheless, deployment of X.500 within large enterprises is increasing and some organisations are finding this repository a useful means of public-key certificate distribution. The Internet Lightweight Directory Access Protocol (LDAP) is a protocol which can access information stored in a directory, including access to stored public-key certificates.

LDAP is an access protocol which is compatible with the X.500 directory standards. However, LDAP is much simpler and more effective than the standard X.500 protocols. The X.509 certificate format describes the authentication service using the X.500 directory. The certificate format specified in the Privacy-Enhanced Mail (PEM) standards is the 1988 version of the X.509 certificate format. The certificate format specified in the American National Standards Institute (ANSI) X9.30 standards is based on the 1992 version of the X.509 certificate format. The ANSI X9.30 standard requires that the issuer unique identifier field be filled in. This field will contain information that allows the private key to sign the certificate and be uniquely identified. The certificate format used with the Message Security Protocol (MSP) is also based on the 1988 X.509 certificate format, but it does not include the issuer unique identifier or the subject unique identifier fields that are found in the 1992 version of the X.509 format. The ISO/IEC/ITU X.509 standard defines a standard CRL format. The X.509 CRL format has evolved somewhat since first appearing in 1988. When the extension fields were added to the X.509 v3 certificate format, the same type of mechanism was added to the CRL to create the X.509 v2 CRL format. Of the various CRL formats studied, the PEM CRL format best meets the requirements of the PKI CRL format. ITU-T X.509 (formerly CCITT X.509) and ANSI X9.30 CRL formats are compared with the PEM CRL format to show where they differ. For example, the ANSI X9.30 CRL format is based on the PEM format, but the former adds one reason code field to each certificate entry within the list of revoked certificates. All CAs are assumed to generate CRLs. The CRLs may be generated on a periodic basis or every time a certificate revocation occurs. These CRLs will include certificates that have been revoked because of key compromises, changes in a user's affiliation, etc. All entities are responsible for requesting the CRLs that they need from the directory, but to keep querying the directory is impractical. Any CA which generates a CRL is responsible for sending its latest CRL to the directory. However, CRL distribution is the biggest cost driver associated with the operation of the PKI. CAs certifying fewer users result in much smaller CRLs because each CRL requested carries far less unwanted information. The delta CRL indicator is a critical CRL extension that identifies a delta CRL. The use of delta CRLs can significantly improve processing time for applications that store revocation information in a format other than the CRL structure. This allows changes to be added to the local database while ignoring unchanged information that is already in the local database.

Digital Signing Techniques

Since user authentication is so important for the PKI environment, it is appropriate to discuss the concept of digital signature at an early stage in this chapter. Digital signing techniques are employed to provide sender authentication, message integrity and sender non-repudiation, provided that private keys are kept secret and the integrity of public keys is preserved. Provision of these services is furnished with the proper association between the users and their public/private key pairs. When two users A and B communicate, they can use their public keys to keep their messages confidential. If A wishes to hide the contents of a message to B, A encrypts

Digital signing techniques are used in a number of applications. Since digital signature technology has grown in demand, its explosive utilisation and development will be expected to continue in the future. Several applications are considered in the following. • Electronic mail security: Electronic mail is needed to sign digitally, especially in cases where sensitive information is being transmitted and security services such as authentication, integrity and non-repudiation are desired. Signing an e-mail message assures all recipients that the sender of the information is the person who he or she claims to be, thus authenticating the sender. For example, the DSS is using MOSAIC to

provide security services for e-mail messages. The DSA has been incorporated into MOSAIC and is used to digitally sign e-mails as well as public-key certificates. Pretty Good Privacy (PGP) provides security services as well as data integrity services for messages and data files by using digital signatures, encryption, compression (zip) and radix-64 conversion (ASCII Armor). MIME defines a format for text messages being sent using e-mail. MIME is actually intended to address some of the problems and limitations of the use of SMTP. S/MIME is a security enhancement to the MIME Internet e-mail format, based on technology from RSA Data Security. Although both PGP and S/MIME are on an IETF standards track, it appears likely that PGP will remain the choice for personal e-mail security for many users, while S/MIME will emerge as the industry standard for commercial and organisational use. • Financial transactions: This encompasses a number of areas in which money is being transferred directly or in exchange for services and goods. One area of financial transactions which could benefit especially from the use of digital signatures is Electronic Funds Transfer (EFT). Digitally signing EFTs are a way of providing security services such as authentication, integrity and non-repudiation. Secure Electronic Transaction (SET) is the most important protocol relating to ecommerce. SET introduced a new concept of digital signature called dual signatures. A dual signature is generated by creating the message digest of two messages: order digest and payment digest. The SET protocol for payment processing utilises cryptography to provide confidentiality of information, ensure payment integrity and identity authentication. • Electronic filing: Contracting requirements expect certain mandated certificates to be submitted from contractors. This requirement is often filed through the submission of a written form and usually requires a handwritten signature. If filings are digitally signed and electronically filed, digital signatures may be used to replace written signatures and to provide authentication and integrity services. One of the largest information submission processes is perhaps the payment of taxes and the request for tax-related information will require signatures. In fact, the IRS in the USA is converting many of these processes electronically and is considering use of digital signatures. The IRS has several prototype under development that utilise digital signatures generated by using DSA. At present, individuals send their tax forms to the IRS in bulk transactions. The IRS will require them to sign the bulk transactions digitally to provide added assurances. In future, the electronically generated tax returns may be digitally signed. The taxpayer may send the digitally signed electronic form to the IRS directly or through a tax accountant or adviser. • Software protection: Digital signatures are also used to protect software. By signing the software, the integrity of the software is assured when it is distributed. The signature may be verified when the software is installed to ensure that it was not modified during the distribution process. • Signing and authenticating: Signing is the process of using the sender's private key to encrypt the message digest of a document. Anyone with the sender's public key can decrypt it. A person who wants to sign the data has only to encrypt the message digest to ensure that the data originated from the sender. Authentication is provided when the sender encrypts the hash value with the sender's private key. This assures the receiver that the message originated from the sender. Digital signatures can be used in cryptography-based authentication schemes to sign either the message being authenticated or the authentication challenge used in the scheme. The X.509 strong authentication is an example of an authentication scheme that utilises digital signatures.

Careful selection and appropriate protection of the prime numbers p and q, of the primitive element g of p and of the private and public components x and y of each key are at the core of security in digital signatures. Therefore, whoever generates these keys and their parameters is a vital concern for security. PCAs are responsible for defining who should generate these numbers. When generating the key for itself and its CA, each PCA needs to specify the acceptable algorithms used to generate the prime numbers and parameters. For example, a larger p means more security, but requires more computation in the signing and verification steps. Thus, the size of p allows a trade-off between security and performance. Each PCA must specify the range of p for itself, its CAs and its end users. The range of p is largest for the PCA and smallest for the end user. One-way hash functions and digital signature algorithms are used to sign certificates and CRLs. They are used to identify OIDs for public keys contained in a certificate. SHA-1 is the preferred one-way function for use in the Internet PKI. It was developed by the US government for use with both the RSA and DSA signature algorithms. However, MD5 is used in other legacy applications, but it is still reasonable to use MD5 to verify existing signatures. RSA and DSA are the most popular

signature algorithms used in the Internet. They combine RSA with either MD5 or SHA-1 one-way hash functions; DSA is used in conjunction with the SHA-1 one-way hash function. The signature algorithm with the MD5 and RSA encryption algorithm is defined in PKCS#1 (RFC 2437). The signature algorithm with the SHA-1 and RSA encryption algorithms is implemented using the padding and encoding mechanisms also described in PKCS#1 (RFC 2437).

References

Aboba, B., and D. Simon, 'PPP EAP TLS Authentication Protocol', RFC 2716, October 1999. 2. Abrams, M., and H. Podell, Computer and Network Security. Los Alamitos, CA: IEEE Computer Society Press, 1987.

Borman, D., 'TELNET Authentication Option', RFC 1416, February 1993. 18. Borman, D., and C. Hedrick, 'TELNET Remote Flow Control Option', RFC 1372, October 1992.

Cheng, P., et al.., 'A Security Architecture for the Internet Protocol', IBM Systems Journal, Number 1, 1998.

Copyrights