Global Information Assurance Certification Paper

- John MacMichael
- 7 November 2003
- Overview of Public Key Infrastructure (PKI), contrasting X.509 and PGP specifications, with particular emphasis on the flexibility provided by the X.509 Optional Extensions.
- GIAC Security Essentials Certification (GSEC) Practical Assignment
- Version 1.4b (amended August 29, 2002)
- Draft 1 of this document

Abstract/Summary

There are a number of different yet viable Public Key Cryptography systems--or Public Key Infrastructure (PKI) implementations--which exist and are in widespread use throughout the internet community. This paper examines the underpinning services which comprise all PKI implementations, examines the primary differences between the X.509 and PGP standards and eventually asserts that X.509 implementations will becoming the defacto standard as PKI implementations become more widespread. The paper then examines the Optional Extensions field of the X.509 certificate as a method of flexibility inherent in the IETF 3280 protocol.

There are a number of different yet viable Public Key Cryptography systems--or Public Key Infrastructure (PKI) implementations--which exist and are in widespread use throughout the internet community. Several of the more prominent implementations are Pretty Good Privacy (PGP), Simple PKI (SPKI), Simple Distributed Security Infrastructure (SDSI), and X.509 Public Key Cryptography. PKI has been on the verge of widespread deployment internationally as early as 1997; each successive year, numerous trade journals have dubbed the ensuing year as the "year of PKI."[1] Yet full full-fledged implementation of a standardized cross platform PKI within the business and government communities continues to lag. There is no commitment to a homogeneous PKI for a variety of factors; the primary impediment to broader use of Public Key Infrastructure (PKI) is the lack of an accepted unified standard which communicates across implementations. Differing implementations of a PKI generally can not communicate with other implementations because of inherent differences in the protocol framework that comprises each particular implementation.

At the highest level of view, a Public Key Infrastructure, or PKI, is a set of mechanisms (laws, policy, procedures, and technologies) for the use of digital credentials, to include digital signatures and document encryption, that provides confidentiality, authenticity, integrity and non-repudiation in regards to the transmission of electronic messages and data. The actual methods in which each of the aforementioned PKI methods implements these services is different, however, they have in common a digital signature as well as public and private keys. These are used in conjunction with digital certificates as a mechanism for the purpose of providing authenticity (entity authentication) while also simultaneously providing integrity over signed data.[2] These topics are defined:

Confidentiality –Ensures that the content of information is kept from all but those authorized to have access it. In a PKI it ensures that only the sender and intended recipient, also known as the relying party, are able to view the message or data transmitted by the sender.

Authentication – In a PKI, authentication encompasses both entity authentication and data origin authentication, depending on which values the digital signature is computed over. The authentication allows for verification of identities in that the transmitter and receiver of a message are the same as those that are represented in the message header. "Data origin authentication implicitly provides data integrity; if a message is modified, the source has changed."[3]

---

1 Berinato.

2 Lloyd; Adams, p.118.

3 Menezes; VanOorschot; Vanstone, Chp. 1, p. 4.

Data Integrity – Addresses the possible alteration of data between sender and receiver; to insure data integrity the intended receiver must be able to detect unauthorized data manipulation through either intentional or accidental means. Manipulation may encompass insertion, deletion, or substitution.

Non-repudiation – Through authentication and data integrity, proof is provided regarding both the integrity and origin of data; this then positively links actions related to data to a given individual or entity. This positive linking prevents the entity from denying having performed a particular action related to data, and provides the service of non-repudiation.

Through the use of PKI and digital certificates, which bind a public key to an individual, device, or organization and carry the signature of a trusted Certification Authority, the above listed services may be provided by any of the previously named PKI implementations.

With a growing number of PKI options, organizations and individuals must decide which implementation they will employ. Individuals generally seek out the implementation that the greatest numbers of their associates use, this might be termed the "Instant Messenger" effect. Individuals will use the use the same proprietary instant messenger application that the greatest numbers of their associates use. While it may be trivial for an individual or organization to use more than one instant messenger; the same is not true for PKI usage. Within an organization, the use of a particular PKI is generally mandated at the corporate level; the choice of the particular implementation must be a mix of scalability, usability, and--perhaps most importantly--the ability to communicate both inside and outside of the organization. It can be argued that PGP is the most popular cryptography for use by individuals while the X.509 frame work has gained the most widespread acceptance at the organizational level. PGP has become popular with individuals because it is free to download and is easy to install and use. It is estimated that there are over 15000 keys on the public key ring and that number is growing by 1000 keys per month[4]. PGP is intuitive and provides instant feedback as to the status of the information, email, and signatures. PGP provides a method for the individual to seamlessly encrypt, decrypt, and sign data. At the organizational level the Department of Defense, many governmental organizations, and many business have chosen to implement a Public Key Cryptography system as described in IETF RFC 3280 X.509 Version 3 public-key Certificate and version 2 Certificate Revocation List (CRL). It is clear that any business that has more than routine transactions with governmental agencies should consider an option which includes an ability to send and receive information which conforms to the X.509 architecture.

The differences between the PGP and X.509 architectures are great and irreconcilable; the inability to interface between these two implementations

4 Metzger.

manifests as differences between X.509 Version 3 certificates and PGP Keys (certificates) as well as the difference in the trust model. The IETF protocol which defines the X.509 V3 certificates and the structure of the PGP certificates are sufficiently different to prevent any cross communication between these two implementations. Further compounding the problem of interoperability is the underlying trust model on which each implementation is built. Trust decisions in the PGP model are offloaded to individuals. The PGP model uses the 'web of trust' approach. There is no central authority which all users trust, but instead, individuals sign each other's keys and progressively form a web of individual public keys interconnected by links formed by these signatures. Users must find an introducer whom they trust to begin the process of trust. This in effect means that there is no positive system to provide mapping between key identification and user identification. There is also no guaranteed key revocation mechanism.

The X.509 architecture uses the traditional hierarchical trust architecture which relies on an outside source to manage both trust decisions and revocation services. The trust decisions are managed by a Certificate Authority (CA) and / or Registration Authority (RA); the revocation decisions are managed by the CA. Individuals within the X.509 architecture must implicitly trust the CA and RA; if the individual trust the CA and the CA trusts another individual, the trust placed in the CA is communicated to all users who are trusted by the CA. In summary, PGP relies on self-managing security architecture while the X.509 architecture is both managed and controlled.

Use and implementation of the X.509 Public Key Infrastructure trust model creates a substantial rift in the traditional trust model. In the traditional model, the user or organization held the responsibility for verifying the identity of the user, usually defined by an identification card, a personal meeting, or a third party counsel. The entity to be trusted was personally known and identified to the trusting organization and could be tied concretely to physical credentials. The X.509 model for Public Key Cryptography offloads this trust to a third party, the Certification Authority, which provides verification by cryptographically binding an entity's identity to a unique cryptographic key – a digital certificate. Each party can then present or cryptographically employ such a digital certificate which to either proves their identity or electronically "sign" digitized information. This model removes the physical barriers as well as the time barriers needed for the trust relationship to occur; however, each party must implicitly trust the third party intermediary as well as the associated framework. For this to be accomplished, it is required that the organization be able to unambiguously and correctly associate a digital certificate with the correct entity.[5]

Widespread use of PKI to provide authentication and non-repudiation has

5 Lloyd; Adams, p 85.

begun at fringe elements of both business and other trust relationships. The Government, most notably in the form of the Department of Defense, mandate for PKI implementation will undoubtedly spearhead the efforts and cause Public Key (PK) cryptography to become more widely accepted. Eventually software will exist that will allow secure communications through any electronic medium; stakeholders will inherently trust any other entity that has completed the validation process. The opportunity for misuse of digital certificates by many actors exists.[6] The hurdle for organizations is to implement this trust relationship securely while assuaging the fears and concerns of primary stakeholders as well as actors within the bounds of the system.

Acceptance of this model requires forward thinking organizations that will accept and implement the PKI trust model. Factors that will retard the implementation of the PKI as a trust model include:

- Fear of the new model by stakeholders
- Lack of a ubiquitous infrastructure
- Liabilities, monetarily and otherwise, which an organization may be subject to in the event of a breach or failure of PKI implementation
- Lack of resolve, on many fronts, to implement PKI
- A less than fully implemented method of Certificate Revocation

Factors that will speed the implementation of PKI as a trust model include:

- The "Digital Security Act" of Oct 2001
- Widespread PKI enabled end-user applications
- Implementers and users familiar with PKI technology and applications
- Timely and reliable methods to verify certificate validity

Eventually, it may be inevitable that one of these two standards may eclipse the other. It is likely that the continued growth of X.509 architecture implementations will outstrip that of PGP implementations due to several factors: continued businesses implementation of the X.509 architecture will make it necessary for individuals to utilize X.509 system, individuals will continue to merge their personal and business lives, users will begin to understand the implications of PGP trust model, and the infrastructure costs associated with the managed and controlled X.509 architecture will continue to decrease. Barring a newer implementation which becomes ratified through the IETF and implemented by vendors, X.509 version 3 certificates and version 2

6 Brands, p.13

CRLS will continue to gain the market share and will continue to be refined in their specific implementations.

The architecture for both the X.509 Version 3 certificates and Version 2 CRL's is incredibly flexible; this flexibility allows tailoring of implementations which fill the requirements of organizations with drastically different needs. The flexibility manifests itself similarly but by different names in each mechanism. The X.509 Version 3 certificate and its Certificate Extensions (optional extensions) are graphically represented in figure 1. The optional fields allow for individual PKI implementations to define specific security features which may be required for a narrowly defined purpose. The optional fields provide "methods for associating additional attributes with users or public keys and for managing certificate hierarchy"[7] In effect; these extensions may be used to incorporate implementation specific requirements into the Certificate. What follows is a review of both the syntax and a synopsis of the meaning of the X.509 version 3 certificates and version 2 CRL's with emphasis on the optional extensions.

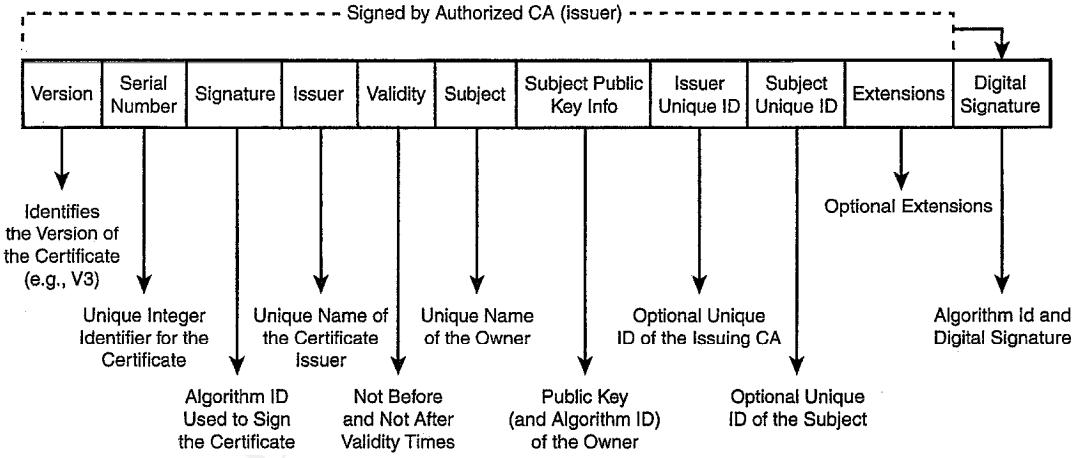

Figure 1. X.509 Version 3 Certificate[8]

The X.509 framework has evolved from its original inception; however, the original model remains intact. Both the Certificate and CRL formats were extended through each revision but are backward compatible through the use of the "critical" and "non-critical" designations. Each optional extension contains an object identifier value which governs the basic data type (text, string, date) and may either be an optional standard or private extension. The Extensions

[7]Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. p. 59.

[8]Lloyd; Adams, p 72.

field, as seen above in the Version 3 certificate provide a great deal of flexibility to the X.509 certificate standard and are one of two types: Standard Extension or Private Extensions. The extensions include an Object ID (OID) and corresponding ASN.1 encoded structure. Each extension includes a flag known as a criticality indicator which indicates whether an occurrence of an extension is either critical or non-critical. When an optional extension is marked critical, an application validating a certificate must process and understand the field extension; if this can not be accomplished the certificate must be rejected. An application validating a certificate may gracefully ignore an unrecognized non-critical CRL entry extension. . The optional flag is a powerful device which may provide a specific feature significant for a particular implementation; however, use of the critical field may cause unwanted rejections of the certificate if it is not recognized by another X.509 implementation. The following descriptions of the standard extensions are summarized from RFC3280 and in some cases are quoted directly from that document:

Authority Key Identifier – Mandated by RFC3280 for inclusion in all but self-signed certificates, this is used when an issuer has multiple keys available to the internet community. It is a unique identifier that serves to distinguish which of the multiple keys issued corresponds to the signed certificate.

Subject Key Identifier – When an entity has obtained multiple certificates, this unique identifier provides a means for identifying which certificate corresponds to the appropriate public key. While required for a CA this field is not mandatory for end entity certificates but should be included.

Key Usage – Sequence of one or more OID's that defines one or more purposes for the public key in the certificate (e.g. encipherment, signature, certificate signing) in addition to the usages mapped from the Key Usage field. This has the effect of limiting or restricting the key to a defined set of functions. In general, this extension will appear only in end entity certificates and, when used, this field should be marked critical. Additionally, it must appear in certificates which contain keys used to validate digital signatures on other public keys certificates or CRLs. Allowable combinations for this field are prescribed in the end entity Certificate Practices document.

Private Key Usage Period - This extension is used with digital signature keys but is designed for use within private PKIs which do not access the general internet community. The usage period allows specification of private keys which have a validity period that differs from that of the certificate. The specifications of notBefore and notAfter allow for a strict determination of when the key may be used. A PKI that accesses the internet and utilizes this extension must mark the extension as non-critical while utilizing either the notBefore or notAfter field.

CRL Distribution

Point – A non-critical extension, it identifies how CRL information is obtained and the location of the CRL partition where revocation information for this certificate resides. RFC3280 provides more detailed specification for this field.

Certificate Policies – A non-critical extension it defines one or more policy object identifiers (OID's) and optional qualifiers associated with the issuance and the use of the certificate. To promote interoperability, RFC3280 specifies that the OID be used absent of any qualifiers even while the RFC defined two qualifiers. The first is the Certification Practices Statement which provides a URI at which the end user can find the CPS published by the CA. The second is the User Notice which displays information to the relying party when a certificate is used.

Policy Mappings – Used only in CA certificates, this extension is used to set the issuing CA issuerDomainPolicy. It may contain one or more pairs of OIDs which define the policy mapping associated with the issuing CA. This must be marked non-critical.

Subject Alternative Name –This field allows for additional flexibility in allowing additional information to be included in a certificate. This information may be either defined by the specific organization or may conform to pre-existing definitions. Examples include: email address, DNA name, IP address, or URI. Use of the subject alternative name field is used to indicate to the relying party that additional information is available, because of the nature of the trust relationship in the X.509 model, all information included in this field must be verified by the CA or the RA prior to inclusion. This extension should not be marked critical.

Issuer Alternative Name – Similar in usage to the Subject Alternative Name, the Issuer Alternative name allows Internet style information to be contained within a certificate. This extension should not be marked critical.

Subject Directory Attributes – This field allows for inclusion of specific identification attributes within the certificate, for example, Organization, Nationality, Gender. This extension must be non-critical.

Basic Constraints – The basic constraints extension identifies whether the subject of the certificate is a CA and the maximum depth of valid certification paths that are included this certificate.

Name Constraints – Only used in CA certificates, this field defines the Internet name space in which certificates built by the CA may be located; this naming information is used to build the certification path. The Internet name space may include URI, email addresses, DNS information, and certain legacy information.

Policy Constraints – This field may only be used in certificates issued to CAs. It defines the

validation path through the process of constraining it. By using this field, specific policy mappings may be prohibited or it may implement a requirement that all certificates in a path must contain an acceptable policy identifier.

Extended Key Usage – All keys have a specific usage, be it signing, encryption, time stamping, or an organization specific requirement. Many organizations choose to limit a key to a specific use and issue keys for each purpose. The Extended Key Usage field allows for one key to have more than the primary purpose as specified in the keyPurposeID field. If this field is used, then the key may only be used for the purpose as specified within the extendedKeyUsage field. When the anyExtendedKeyUsage id is used, this will allow the key to be used for any purpose which the end application is able to recognize. The extension may be marked as either critical or non-critical, depending on the usage of the extendedKeyUsage field. While the organization employing a PKI may determine and write an appropriate usage key, the following key usages have been defined by RFC 3280: server authentication, client authentication, signing of downloadable executable code, email protection, time stamping, OCSP response signing. This field may be marked critical or non-critical depending on the usage; if the anyExtenddeKeyUsage field is used it should not be marked critical, else wise it may be marked non-critical.

CRL Distribution Points – One of the largest impediments to further acceptance of the PKI model is the lack of a pervasive method of certificate revocation. A CRL distribution point allows for partitioning of the CRL into more manageable pieces. The CRL distribution point extension is in effect an embedded pointer which points the software of the relying party to the CRL Distribution Point and is then in turn redirected to the correct CRL partition based upon this information.[9] This non-critical extension identifies to the relying party application where the information regarding the certificate in question resides. Additional information that may be included in this field are the reasons and cRLIssuer. When properly implemented, this field will indicate whether the certificate issuer is the same as the CRL issuer and may be used to provide the reasons the certificate in question was revoked.

Inhibit Any Policy – Only used in CA certificates, this field defines the number of additional certificates that may appear in the path before anyPolicy OID is no longer permitted.

Freshest CRL Pointer –This field provides another key method in the mechanism of certificate revocation; A Delta CRL is composed of a base

9 Verisign, Inc.

list and updates. The base list is a complete CRL as of a defined time period. The update or Delta CRL contains incremental CRL information. Delta CRL's may be formatted relative to a base CRL or relative to a particular point in time.[10] The Delta CRL allows the end user who has retrieved the latest full CRL to retrieve a smaller amount of updated CRL information thus maintaining a complete list of revoked CRL's and increasing the confidence in the PKI. The Delta CRL allows for more frequent publishing in an attempt to optimize the timeliness of available information against the required bandwidth for transmission or retrieval by the end user. The "Delta CRL Indicator" extension is used to denote which method is used while the Freshest CRL Pointer provides resolution to where the CRL update information is located. This extension must be marked non-critical.

RFC 3280 provides two private internet extensions which may be used within the Internet Public Key Infrastructure. These extensions provide information in URI format as to the location and format of information regarding the issuing CA or the subject. The following two extensions are defined:

Authority Information Access – This extension may be included in end entity or CA certificates and must be non-critical. The extension provides the relying party with instructions on how to locate information relevant to the CA. The types of information which may be included are Certificate Practices Statement (CPS) or information regarding online validation services (OCSP). It will not include information for CRL data as that has been provided in the public optional extensions.

Subject Information Access – This extension may be included in end entity or CA certificates and must be non-critical. It provides information about the subject relevant to the type of certificate in which it is included: CA or end entity certificates.

As has been demonstrated by the preceding explanations, the certificate extensions field provides a great deal of flexibility for the X.509 certificates. Further flexibility in a X.509 PKI implementation is built into the X.509 v2 CRL; while the X.509 Version 3 certificate uses optional fields the X.509 Version 2 CRL has both CRL Per-Entry Extensions and general CRL Extensions which allow association of additional attributes with the individual certificates, while retaining management of the certification hierarchy. Discussion of these fields is beyond the scope of this paper, however, the amount of modification and flexibility in the CRL is at least equal to that of the Version 2 Certificate. This

10 Lloyd; Adams, p118.

paper has discussed the differences between the X.509 architecture and that of the PGP PKI. It further examined the optional extensions field of the X.509 Version 2 Certificate; this examination has shown the flexibility and strength inherent in an X.509 PKI implementation

References

Berinato, Scott. “Only Mostly Dead” 23 May 2002. URL: http://www.csoonline.com. (24 Aug 2003).

Lloyd, Steve; Adams, Carlisle. Understanding PKI: Concepts, Standards, and Deployment Considerations, Second Edition. Massachusett: Addison Wesley Professional, 2002.

Menezes, Alfred. VanOorschot, Paul. Vanstone, Scott. Handbook of Applied Cryptography. Vanstone: CRC Press, 1996.

Metzger, Joe. “Benefits of PGP over other Encrypted Email Systems” http://www.scl.ameslab.gov/scl/Personnel/metzger/PGP/benefits.html (1 Sep 2003).

Brands, Steven. Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy. MIT Press, August 28, 2000.

Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. URL:http://www.ietf.org/rfc/rfc3280.txt (1 Sep 2003).

Verisign, Inc. “Certificate Revocation with VeriSign Manged PKI”. URL:http://www.verisign.com.au/whitepapers/enterprise/revocation/cert_revk2.s

html (1 Sep 2003)

Feghhi, Jalal. Feghhi, Jalil. Williams, Peter. Digital Certificates: Applied Internet Security. Massachusett: Addison Wesley Longman, 2002.

Nash, Andrew. Duane, William. Joseph, Celia. Brink, Derek. PKI: Implementing and Managing E-Security. Berkley: RSA Press, 2001.

Brands, Stefan. Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy. Massachusetts: MIT Press, 2000.