PKI SOLUTIONS

PKI Glossary of Terms

Over the course of Public Key Infrastructure (PKI) design, implementation, and management, you will encounter many terms and acronyms that are defined in this document.

The biggest part of the PKI implementation process is meeting with the stakeholders to ask and answer questions about where things are, how they work, what they struggle with today, and how they see a new PKI accomplishing business goals and requirements. It's in these meetings, like most IT discussions, where terminology can be thrown about pretty freely with the assumption that everyone knows what the terms and acronyms mean.

Providing a glossary of PKI terminology will help to keep the vagueness and misunderstandings from getting in the way of good discovery and planning.

ADCS - Active Directory Certificate Services

Active Directory® Certificate Services (AD CS) is an Identity and Access Control security technology that provides customizable services for creating and managing public key certificates used in software security systems that employ public key technologies.

AIA - Authority Information Access

AIA is an X.509 certificate extension that contains CA certificate access information. Systems use the AIA location to retrieve a copy of the issuing CA's certificate to form a validation chain. This can point to an LDAP and an HTTP location.

AES - Advanced Encryption Standard

AES superseded the DES standard. It is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting data. It improved on DES by its ability to use 128-256-bit key sizes and as a symmetric-key algorithm can encrypt large amounts of data quickly. This is also applicable for key-archival to protect user private keys protected in transit to a CA.

Assurance Level

The level of assurance refers to the strength of the binding between the public key and the individual whose subject name is cited in the certificate, the mechanisms used to control the use of the private key, and the security provided by the PKI itself. Common levels are Low, Medium and High. An example would be High, Medium and Low assurance levels stipulated in a Certificate Policy where High could mean verification of identity through a government-issued ID as well as a face-to-face interview;

PKI GLOSSARY OF TERMS

Asymmetric Encryption

Encryption system that uses a public-private key pair for encryption and decryption, as well as for digital signatures. Also known as a public-key algorithm. Common asymmetric algorithms are RSA, Diffie-Hellman, and ECDSA and DSS/DSA. The public key is used to encrypt a message and the associated private key is used to decrypt the message. For example, Bob wants to send an encrypted message to Alice. Alice sends her public key to Bob who encrypts the message and sends it to Alice. Alice then decrypts the message with her private key. Helen who has been listening in and also has the public key (it is public, after all!) but she is unable to decrypt Bob's message since she doesn't have Alice's private key.

CA - Certification Authority

A Certification Authority (CA) is the core component of a Public Key Infrastructure (PKI) responsible for establishing a hierarchical chain of trust and are configured to reflect the trust boundaries of their operators.

CA (Certification Authority) Hierarchy

A certificate hierarchy is the functional design and placement of CA servers in a PKI infrastructure. Common examples are single, two-tier and three-tier hierarchy. The CA certifies the identity of a certificate request, issues and validates certificates and manages certificate revocation. It also is responsible for attesting to the identity of users, computers, and organizations. This encompasses both root CA and subordinate CAs. CA's may be operated by different entities and are configured to reflect the trust boundaries of their operators.

CAWE - Certificate Authority Web Enrollment

Certification Authority Web Enrollment is a role in ADCS used to enroll non-domain joined users and devices for certificates from a CA and supports CMS PKCS#10 requests.

CDP - CRL Distribution Points

A CDP is the place for the retrieval of the latest CA CRLs. This is usually a Lightweight Directory Access Protocol (LDAP) server for AD lookup or HTTP (web) server for a public URL.

CEP/CES - Certificate Enrollment Web Services

CEP (Certificate Enrollment Policy) and CES (Certificate Enrollment Service) combine to enable policy-based certificate enrollment when the client computer is not a member of a domain or when a domain member is not connected to the domain or when the client (member or not) cannot communicate with DCs and CAs.

Certificate AutoEnrollment

AutoEnrollment is the capability to automatically enroll AD users and computers for certificates. This is accomplished by certificate template configuration and Active Directory group policy.

Certificate Extensions

Shown in the certificate data, certificate extensions provide additional information about the certificate. Extensions include what the certificate can be used for, basic constraints, revocation locations, OSCP locations, details about the issuers' Signing Key, etc. An extension can be configured to specifically designate enforcement and use policies as well as key usage such as Code Signing, server and/or client authentication and digital signing.

Certificate Chain

A certificate chain is a hierarchal collection of certificates where the root of trust is a at the top of the PKI hierarchy. Trust is further gained by verifying that each certificate in the chain:

- Shows the validity period, including current date and time
- Is not in the local Untrusted Certificate store
- Shows that policies from the issuing CA and above are in place

PKI GLOSSARY OF TERMS

Certificate Stores
Certificate stores are a combination of logical groupings and physical storage. Common stores include Personal, Trusted Root Certification Authorities, Intermediate Certification Authorities, and Untrusted Certificates. These stores identify the descriptions and purposes of certificates found within. For example, the Personal store will show the certificates issued to the local user or computer and associated with a private key. The Intermediate Certification Authorities store will contain subordinate CA certificates.

Certificate Template
Certificate templates define the format and content of a certificate. Configurations include enrollment permissions, renewals, certificate purpose, lifetime, key length, extensions, issuance requirements, etc. They exist in the certificate templates container of Active Directory. X.509 attribute extensions are used to define a template's structure.

Certreq.exe
Certreq.exe is a command line tool which constructs requests to a CA, retrieves the signed certificate and installs into the local certificate store. Using a .inf (INF) file configured with attributes that contain Subject Name, OID, extensions, etc., a request can be generated and built as a Request file ready for enrollment with the CA. A request can be built from a device in a separate forest from an available CA.

Certutil.exe
Certutil is the powerful command-line program consisting of a large library of uses for the management of certificates and CAs in a PKI infrastructure. Its uses include but are not limited to:

- Configuring certificate services
- Backup and restore
- Verify certificates and properties, key pairs and chains
- Viewing and setting CA registry
- Publishing to Active Directory
- Diagnostics and dumps

CN - Common Name
The common name is the name of the End-Entity or subscriber in a certificate.

CNG/KSP - Cryptography API: Next Generation
Windows Cryptography API: Next Generation (CNG) (KSP = Key Storage Provider) and features support for Suite B algorithms, hardware security modules, and more. The CNG API replaces the CryptoAPI but is backwards compatible to all its algorithms.

Code Signing
Code signing provides a digital signature to executable files (.exe), dynamic link libraries (.dll), ActiveX controls (.ocx), Microsoft Visual Basic documents (.vbd), Cabinet files (.cab), Java Archive files (.jar), Windows Installer files (.msi or .msp), driver files (.sys), and scripts. This signature provides verification of the signing individual and ensures the contents haven't been manipulated.

CP - Certificate Policy
The Certificate Policy, based on RFC 3647, is a named set of rules that define all aspects associated with the assurance levels, generation, production, distribution, recovery, accounting, auditing and administration management of certificates.

CPS - Certification Practice Statement
A Certification Practice Statement, based on RFC 3647, is a public document describing the framework of the management of the PKI and its CAs. The CPS states the procedures, practices and requirements employed in all areas of the PKI. It's location (CDP) is configured at the build of all Issuing CAs and specified in certificates issued by the CAs in the PKI covered by the CPS.

PKI GLOSSARY OF TERMS

Credential Roaming
Credential Roaming is where a user certificate and protected credential information is roamed between computers allowing for the prevention of excessive enrollment by users on multiple computers and loss of certificates if a user's profile is deleted.

CRL - Certificate Revocation List
A CRL is a signed, time-stamped list of certificate serial numbers and reason codes of revoked certificates by the Certification Authority. CRLs are normally published to a publicly-available website for revocation checking. Once revoked a certificate is invalid prior to its expiration.

CRL Overlap Period
A CRL Overlap period is set on the CA as a post-install configuration to allow time to perform Emergency CRL Signing or to recover the CA before the last CRL expires. The CRL Overlap configuration if set for 3 days, for example, is then added to the Base CRL Next Update setting (3 days) extending the CRL validity to 6 days, allowing at least 3 days to recover. Thus, the CRL overlap period should equal the minimum time permitted for recovery or emergency CRL signing.

CRL Partitioning
CRL Partitioning is the practice of renewing a CA with new keys to reduce the size of a large CRL.

CRL Pre-Fetch
CRL Pre-fetching downloads CRLs before they are needed for revocation checking allowing the client to check revocation against locally downloaded CRLs instead of having to download a CRL during the Certificate Validation and Certificate Revocation process.

Cross-Certificate
A Certificate used to establish a trust relationship between two Certification Authorities. Authorities in separate forests with two one way trusts established.

Cross Certification
Cross certification enables entities in one public key infrastructure (PKI) to trust entities in another PKI and establish an agreement of responsibilities and liability of each party. This doesn't join separate PKI hierarchies however, entities in each PKI are subject to the policies specified in the certificates.

CSP - Crypto Service Provider
Crypto Service Providers are typically a .dll and signature file referenced in the registry and provide cryptography services used in data signing and hashing along with the generation, protection and storage of key material.

CSR - Certificate Signing Request
A Certificate Signing Request (CSR) (PKCS#10) is a request file sent to a Certificate Authority (CA) to receive a certificate and contains information about the subject making the request, the subject's public key, a set of attributes, a set of X.509 extensions, and a signature. These can be generated on non-Windows devices and by using OpenSSL or a method using CMP (Certificate Management Protocol).

CTL - Certificate Trust List
A Certificate Trust List is a set of items signed by a trusted entity. A CTL is a list of hashes of certificates or a list of file names. All the items in the list are authenticated and approved by a trusted signing entity.

Delta CRL
A Delta CRL contains the list of revoked certificates since the last base CRL issuance to allow clients to maintain knowledge of revocation while using less bandwidth for that knowledge. Delta CRLs are useful if there's a lot of revocation happening that then means a large CRL to download, but less often. The disadvantages of using Delta CRLs include the time it takes for a client to read both the newest Delta CRL and the Base CRL to verify the freshest revocation list. For these reasons, we don't recommend employing Delta CRLs in most PKI implementations.

DER - Distinguished Encoding Rules
DER is a set of rules for encoding ASN.1 defined data as a stream of bits for external storage or transmission. DER encoded certificate files are supported by almost all applications. OpenSSL and Keytool support DER encoded certificate files

DES - Data Encryption Standard
DES is a block cipher that encrypts data in 64-bit blocks. DES is a symmetric algorithm that uses the same algorithm and key for encryption and decryption.

Diffie-Hellman Key Agreement
The Diffie-Hellman algorithm is not based on encryption and decryption but instead relies on mathematical functions using an agreed upon public key value and a large prime number that, when computed with their secret (private) keys, enable two parties to generate a shared secret key for exchanging information securely.

Digital Certificate
A digital Certificate represents the identity of a user, computer or program. It contains information about the issuer and the subject and also certificate-specific data such as the CA signature and its validity period. It is signed by a certification authority (CA) which vouches for the identity of the user, computer, or program based on the information in the certificate. A minimum of verified information includes Subject Name identity, the issuing authority and validity period.

Digital Signature
A digital signature is a cryptographic technique that uses a mathematical algorithm that binds a sender's identity to a digital message or document based on a subscriber's private key. It secures the message or document and verifies the integrity of the signature allowing a Relying Party to be sure that the file or document has not been altered or interfered with.

DN - Distinguished Name
A DN is a unique name or character string that unambiguously identifies an entity according to the hierarchical naming conventions of X.500 directory service. Examples are:
- CN - Common name, subject name (widgets.contoso.com)
- O - Organization (contoso.com)
- S - State (Illinois)
- C - Country (US)

Document Signing
Document signing applies a digital signature to a document. The digital signature provides non-repudiation where someone can't deny later that they ever signed it. Also, it denies an ability to fake a valid signature.

The digital signature:
- Verifies the identity of the user that signed the document. Typically, this is either the last person to edit the document before distribution or the person that verifies that the content represents the views of the organization distributing the document.
- Allows a recipient to verify that content of the document was not modified after the digital signature was applied to the document.

DSA - Digital Signature Algorithm
DSA is a public key algorithm specified by Digital Signature Standard (DSS). DSA is only used to generate digital signatures and cannot be used for data encryption. It does provide a standard used for authentication and integrity of a digital signature as well as non-repudiation where someone can't later deny having signed a document using a digital signature.

ECC - Elliptic Curve Cryptography
Elliptic Curve Cryptography is an efficient approach to public key cryptography based on properties of elliptic curves. The primary advantage of ECC is efficiency. For example, ECC keys between 163 bits and 512 bits are one-sixth to one-thirtieth the size of equivalent RSA keys. As key size increases the efficiency of ECC increases.

PKI GLOSSARY OF TERMS

ECDH - Elliptic Curve Diffie-Hellman
ECDH is based on the Diffie-Hellman algorithm using elliptic curve cryptography to establish a shared secret over an insecure channel or network.

ECDSA - Elliptic Curve Digital Signature Algorithm
ECDSA is a Digital Signature Algorithm that uses keys derived from elliptic curve cryptography that efficiently provides equivalent security. It provides RSA level security but with much smaller key sizes. For example, an ECDSA 256-bit key size secures better than the RSA 2048. The decreased bandwidth in key exchanges is an obvious advantage of ECDSA.

EFS - Encrypting File System
Encrypting File System is a feature in the Windows operating system that enables users to encrypt files and folders on an NTFS volume disk. A PKI can manage EFS with EFS certificate templates.

EKU - Enhanced Key Usage
Enhanced Key Usage is both a certificate extension and a certificate extended property value. After a computer's identity, for example, is verifiable by an issued certificate an EKU specifies the uses for which a certificate is valid.

Examples are:
- Server Authentication =1.3.6.1.5.5.7.3.1
- Client Authentication =1.3.6.1.5.5.7.3.2
- Secure E-mail EKU=1.3.6.1.5.5.7.3.4
- Code Signing EKU=1.3.6.1.5.5.7.3.3
- Time stamping EKU=1.3.6.1.5.5.7.3.8
- Encrypting File System EKU=1.3.6.1.4.1.311.10.3.4
- Document Signing EKU=1.3.6.1.4.1.311.10.3.12

End-Entity
A certificate issued to an entity that cannot itself issue certificates. Because the entity that requests such a certificate is sometimes referred to as the client, end-entity certificates are sometimes called client certificates.

EV – Extended Validation Certificate
An EV certificate used for HTTPS websites and software that proves the legal entity controlling the website or software package.

FIPS - Federal Information Processing Standard
FIPS is a standard published by the National Institute of Standards and Technology. FIPS 140-2 is the benchmark for validating the effectiveness of cryptographic hardware.

Hash or Message Digest
A fixed-size result obtained by applying a mathematical function (the hashing algorithm) to an arbitrary amount of data.

Hash Algorithm
An algorithm used to produce a fixed-length hash value of some piece of data, such as a message or session key. Typical hashing algorithms include CMAC,MD2, MD4, MD5, SHA-1, and SHA-2.

HSM - Hardware Security Module
A hardware security module is a physical computing device that safeguards and manages digital keys for strong authentication and provides cryptographic operations processing. They are typically certified for physical security at various FIPS 140-2 security levels. HSMs are recommended in most PKI implementations since the CA private keys are not software-based and thus insecure, but instead are hardware-based and only available from within the HSM itself.

HTTPS - Hypertext Transfer Protocol Secure
A communication protocol that uses the HTTP (Hypertext Transfer Protocol) and the SSL/TLS protocols to provide encrypted communication and secure identification of a Web server.

PKI GLOSSARY OF TERMS

Identity Assurance
There are three main methods to provide the assurance of the identity of an authorized user.

They are:
- Something that the user knows (e.g. password),
- Something that the user possesses (e.g. a token) or
- Something that the individual "is" (e.g. biometrics such as a finger print reader.

Intermediate CA
An intermediate CA is a CA that is subordinate to another CA and issues certificates to other CAs in the CA hierarchy. These can be Issuing CAs and Policy CAs depending on the PKI design.

Issuance
Issuance is the act of an Issuing Authority in creating a certificate which is bound to a subscriber. The process requires authentication of the subscriber and/or subject.

Issuing Certification Authority
An Issuing CA is online and issues certificates to users, computers, services and programs as well as regularly publishing a CRL. It also manages the design and publication of templates that enforce policies and procedures defined either at the Issuing CA (two-tier hierarchy) or from the Policy CA (three-tier hierarchy). An Issuing CA also services Certificate Authority Web Enrollment, NDES, CEP/CES and others in the enrollment and distribution of certificates in a PKI or to another PKI using cross-certification, for example.

Kerberos
Kerberos is a protocol that defines how clients interact with a network authentication service and builds on symmetric key cryptography and optionally may use public-key cryptography during certain phases of authentication.

Key Archival
Key archival is the use of a Key Recovery Agent certificate's public key to encrypt a private key so that it can be stored as a blob in the CA database, smartcard or HSM and retrieved at a later date. This requirement is specified in a template and allows a user who has lost their private key to recover encrypted data.

Key Pair
In an asymmetric cryptosystem, a key pair consists of a private key and its mathematically related public key having the property that the public key can verify a digital signature that the private key creates.

Key Recovery Server
A key recovery server provides key escrow for encrypted private keys in the certificate database for recovery after loss.

KRA - Key Recovery Agent
A key recovery agent is a person in the CA Role who is authorized to recover a certificate on behalf of an end user. The agent must configure and enroll for a KRA certificate.

KSP - Key Storage Provider
KSP is an independent software module that implements functionality to create, manage, store, and retrieve private keys. It also provides increased auditing functionality for CNG use.

Message
A Message is a digital representation of information that may be encrypted for privacy, digitally signed for authentication purposes, or both.

Message Digest
The output produced by a hash function upon processing a message.

NDES – Network Device Enrollment Service

NDES is Microsoft's implementation of SCEP (Simple Certificate Enrollment Protocol). Since Windows Server 2012 R2 the NDES Policy Module provides customizable processing and authentication of NDES enrollments. Based on HTTP, it's used to enroll non-AD joined devices and appliances, switches and routers, VOIP solutions, embedded OS, and Linux. In most environments, NDES is deployed in conjunction with MDM implementations such as AirWatch, MobileIron and Microsoft Intune.

NIST - National Institute of Standards and Technology

NIST is a non-regulatory federal agency within the U.S. Department of Commerce that advances measurement science, standards and technology.

Non-Repudiation

Non-repudiation refers to the inability for signers to deny that a signature is theirs. The secure digital signature provides irrefutable evidence of the message's sender as well as the time it was sent, but it is only as defensible as the PKI is strong.

Nonce

A nonce is a randomly generated number that may only be used once.

OCSP - Online Certificate Status Protocol

Online Certificate Status Protocol (OCSP) is an Internet protocol designed for efficient CRL distribution and obtaining the revocation status of a certificate. OCSP addresses shortcomings with the CRL based revocation and size by the caching of CRLs from multiple CAs. It has, however, been made obsolete by RFC 2560.

OCSP Responder

An OCSP Responder is an ADCS Role service. It features CRL caching, auditing and high availability for checking revocation status.

OID - Object Identifier

An object identifier is a globally unique value used in Abstract Syntax Notation (ASN.1) represented as a dotted decimal string, such as 1.3.6.1.4.1.311.21.43. National registration authorities issue root object identifiers to individuals or organizations, who manage the hierarchy below their root object identifier. OIDs in a PKI are used to identify specific policies or uses based on a company's ARC where those OIDs are prefaced by the ARC defined here:

- 1 = iso
- 3 = org
- 6 = dod
- 1 = internet
- 4 = private
- 1 = enterprise
- 311 = Microsoft

OpenSSL

OpenSSL is a widely used cryptography library and tool that provides an open source implementation of the SSL and TLS protocols. It is often used to generate keys and requests for non-Windows devices.

PEM – Privacy Enhanced Mail

A file format for X.509 certificate files using Base64 encoding to store and send keys, certificates and other data. A PEM certificates file contains the certificate content and adds two boundary lines "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----". In windows this is equivalent to a .CER encoded Base-64 certificate file.

PKCS

PKCS is a group of 15 numbered standards developed by RSA but now widely adopted. Common are PCKS#7, PCKS#10 and PCKS#12.

PKI GLOSSARY OF TERMS

PKI - Public Key Infrastructure
PKI is a set of roles, policies, people, software, hardware, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates. A PKI establishes a trust hierarchy in the provisioning of digital certificates throughout an organization providing secure authentication and encryption. A PKI consists of Certification Authorities that ensure that entities are who they say they are, use encryption algorithms for the security of data transmissions, and provide non-repudiation to resolve by digital signature any question of who did what and when.

PKIView
The PKI Health Tool, PKIView, provides a graphical display to manage a CA hierarchy, Active Directory Public Key Services containers and information specific to all AIA and CDP URLs defined in the PKI and on the CAs.

Policy CA
The Policy CA is an Intermediate Subordinate CA typically in the second tier of a three-tier PKI hierarchy placed directly beneath the Root CA. It issues certificates only to other CAs in the hierarchy directly and subordinate to it or two or more levels lower in the hierarchy. These CAs enforce the policies and procedures defined at the Policy CA.

PQC - Post-Quantum Cryptography
Post-quantum cryptography is the field of cryptography that deals with cryptographic algorithms that can run on classical computers and are secure against an attack by a large-scale quantum computer that runs much stronger and faster. These algorithms have been based on the assumption that the degree to which they are unable to be solved maps to their strength.

Private Key
The secret half of a key pair used in a public key algorithm, private keys are typically used to encrypt a symmetric session key, digitally sign a message, or decrypt a message that has been encrypted with the corresponding public key.

Public Key Certificates
The public part of an asymmetric key pair used for public key encryption techniques. The public key is typically used for verifying digital signatures or to encrypt messages to the owner of the private key.

Public Key Encryption
Public-key encryption uses two separate keys that are mathematically related, to encrypt and decrypt content. The public key can be distributed widely while the private key remains with the user or device that created the key pair.

Quantum Computing
The use of high-speed algorithms, such as Grover's Algorithm and Shor's Algorithm, by quantum computers allow for the solution of certain classes of problems much faster than classical computers presently which introduces threats to current well-known and established key cryptographies.

RA - Registration Authority
The RA is a PKI role involved in verifying identity and enrolling users. RAs work with a particular CA to vet requests for certificates that will then be issued by the CA. Included in this roll are renewals and request for certificate revocation or suspensions.

Re-Key
To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate on the new public key.

Relying Party
A recipient, or certificate user, who acts in reliance on that certificate and/or any digital signatures verified using that certificate, especially the certificate chain.

Repository
Repository refers to a website typically with the CDP site where public CA certs, CRLs, CP, CPS and other PKI documentation is available for review.

Revocation
Revocation of a certificate invalidates a previously signed certificate and is listed in the next published CRL by serial # and date of revocation. Revocation processing and management is key to any PKI and further secures the distribution of certificates in the environment by publishing revocation information and making it widely available.

Role Separation
As fully defined in a Certificate Policy, role separation is a core PKI design principle that sets the requirements for PKI management where no one single person has full control. Depending on the size of the operation of the PKI, separate roles can be as little as CA Administrator and CA Manager, to an additional separate two roles, Auditor and Backup Operator. Role separation should be fully defined in the Certificate Policy.

Root Certification Authority
The Root CA is the topmost CA in a PKI hierarchy and acts as the trust point for certificates issued by CAs in the environment. In a two or three-tier environment, the Root CA only issues certificates to subordinate CAs, such Policy CAs and Issuing CAs. The Root CA should be built, maintained and serviced offline, never connecting to a network. HSMs are often used within a private network to provide hardware-based key storage for the best protection of the Root CA's private keys.

As the beginning of trust in a PKI, the Root CA is the most important entity in the PKI. Policies and procedures should be well planned and designed and managed in accordance with the PKI Certificate Policy (CP).

RSA
RSA was one of the first practical key exchange and public-key cryptosystems and is widely used for secure data transmission. RSA is asymmetrical and its encryption and signing processes are performed through a series of modular multiplications. Security is increased by longer key-lengths such as the 2048-bit key size used as a minimum size today.

Sanitized Name
The form of a certification authority (CA) name that is used in file names (such as for a certificate revocation list) and in registry keys that contain illegal file names, registry key names, or Distinguished Name values, or that are illegal for technology-specific reasons.

SCEP - Simple Certificate Enrollment Protocol
SCEP is an enrollment method to allows a device to generate a certificate request and automatically submit to a CA. It can also support certificate revocation and CRL lookups. SCEP was originally designed by Cisco and can work for most non-Windows devices. NDES (Network Device Enrollment Service) is Microsoft's implementation of SCEP.

Self-Signed Certificate
A self-signed certificate is a certificate that uses its public key to verify its own signature and where the subject name is identical to the issuer name. A Root CA uses a self-signed certificate in its establishment as the root of trust in the PKI.

Session Key
Session keys are used in single communication settings usually using symmetric encryption. They are short-lived and discarded when no longer needed. Used for encrypting and decrypting large amounts of data, they are also employed in the public-private key exchange for sending and receiving messages in that process.

SHA - Secure Hash Algorithm
SHA is a hashing algorithm that generates a message digest. It is used with the Digital Signature Algorithm (DSA) in the Digital Signature Standard (DSS), among other places. There are four varieties of SHA:

- SHA-1
- SHA-2 (SHA-256, SHA-384, and SHA-512)

S/MIME - Secure/Multipurpose Internet Mail Extensions

Originally developed as PKCS#7, S/MIME is a standard to secure MIME data with public key signing and encryption as defined in RFC 5751. A S/MIME template is available in ADCS that incorporates this standard for securing email in an enterprise.

Smartcard

Credit card-sized hardware token chip card that incorporates one or more integrated circuit (IC) chips to implement cryptographic functions, has inherent resistance to tampering and stores private keys. A PIV is a US Government issued smartcard with a picture image and storage of certificates and biometrics.

SSL - Secure Sockets Layer

SSL is a protocol to provide communication security over a computer network using X.509 certificates. It has since been superseded by the TLS protocol.

SAN - Subject Alternative Name

The Subject Alternative Name (SAN) is an X.509 v3 certificate extension that binds additional information to the subject DN of a certificate. Google Chrome, for example, only checks the SAN for identity. Accepted practice now is to include the Subject Name, or Common Name, in the SAN field.

Subject Name

The Subject Name is the Common Name of the certificate referring to the identity of the user, computer or service it is requested for. Supported keys in an enrollment include:

- L = Locality
- E, EMAIL = email address
- T, Title = Title of subject in an organization
- DC = One part of a DNS name (dc=contoso)

Subordinate CA

A CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA. They can be Issuing CAs at the bottom tier of a two or three-tier hierarchy or at the middle tier of a three-tier hierarchy serving as a Policy CA that issues certificates and enforces policies to Issuing CAs. These are sometimes referred to as Intermediate CAs.

Subscriber

A subscriber is an entity that enrolls for a certificate from an Issuing CA and bears ultimate responsibility for the use of the private key associated with the certificate. These responsibilities are detailed in the Certification Practice Statement (CPS) and the Certificate Policy (CP).

Suite B

Suite B is a set of advanced cryptographic algorithms promulgated by the National Security Agency as part of its Cryptographic Modernization Program. Protocols included are AES, SHA-2, ECDH and ECDSA.

Symmetric Key

A secret key used with a symmetric cryptographic algorithm and where the same key is used for both encryption and decryption.

Thumbprint

The thumbprint is a unique hash value using the SHA-1 algorithm that uniquely identifies a certificate. It is computed over the complete certificate, which includes all its fields, including the signature and is unrelated to the hash used in the digital signature, thus it is unique everywhere. Although a serial number is unique to CA, it may not be unique everywhere since the same number could be computed from another CA.

Time-Stamp
Time-stamping is used often in Code Signing or Document Signing and creates a notation that indicates, at a minimum, the correct date and time of an action or activity and the identity of the entity that created the notation.

Time-Stamping Authority
The Trust Service Provider operating, controlling and issuing time-stamps for use by other entities.

TLS - Transport Layer Security
TLS is a security protocol that supports confidentiality and integrity of messages in client and server applications communicating over open networks.

TPM - Trusted Platform Module
A TPM is a secure crypto-processor implemented in the form of a hardware chip embedded on a computer or device. It generates and protects cryptographic keys and is commonly used to authenticate hardware devices.

Validation
Validation is the process by which an end-entity certificate certifies the certificate chain of trust in a PKI.

Validity Period
The period that is defined within a certificate, during which that certificate is intended to be valid. It begins when the certificate is issued and ends with the completion of the validity or if it's revoked or suspended earlier.

X.509
X.509 is a standard defining the format of public key certificates, revocation lists, and the certification path validation algorithm used in a strict hierarchal PKI infrastructure. Additional it defines the extensions, certificate structure, certificate uses, etc. It is standardized in RFC 5280 for version 2 and version 3 certificates.

PKI SOLUTIONS

Contact Us

PKI Solutions Inc.
1710 SW Military Rd
Portland, Oregon 97219

pkisolutions.com
971.231.5523
info@pkisolutions.com

@PKISolutions
pkisolutions