PKI Glossary

Term	Definition
3DES	See TDEA and DES
AD	Active Directory is the name of the Microsoft directory product.
AD CS	Active Directory Certificate Services is the name of the Microsoft CA product.
AES	Advanced Encryption Standard also known by its original name Rijndael is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001.
AIA	The authority information access extension indicates how to access information and services for the issuer of the certificate in which the extension appears. Information and services may include on-line validation services and CA policy data.
API	Application Programming Interface is a way for two or more computer programs or components to communicate with each other. It is a type of software interface, offering a service to other pieces of software.
ASN.1	Abstract Syntax Notation One (ASN.1) is a standard interface description language (IDL) for defining data structures that can be serialized and deserialized in a cross-platform way. It is broadly used in telecommunications and computer networking, and especially in cryptography.
Asymmetric Encryption	Asymmetric Encryption is an encryption system that uses two keys, a public-private key pair for encryption and decryption, as well as for digital signatures. Common asymmetric algorithms are RSA, Diffie-Hellman, and ECDSA, and DSS/DSA.
CA	Certificate Authority The entity in a Public Key Infrastructure (PKI) that is responsible for issuing public-key certificates and exacting compliance to a PKI policy. Also known as a Certification Authority.
CAMS	Card Application Management System is a system that can manage applications on smartcards
CAPI	While CAPI can stand for Common Application Programming Interface, in the context of PKI is it most often referred to as MS-CAPI and stands for Cryptographic Application Programming Interface. CAPI is an application programming interface included with Microsoft Windows operating systems that provides services to enable developers to secure Windows-based applications using cryptography. It is a set of dynamically linked libraries that provides an abstraction layer which isolates programmers from the code used to encrypt the data.
CDP	CRL Distribution Point A pointer to where CRL's are to be published.
Certificate	A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its Subscriber, (3) contains the Subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it.
Certificate Template	Certificate templates is a Microsoft Term used to set the format and content of type of certificate to be produced on a CA. Configurations include enrollment permissions, renewals, certificate purpose, lifetime, key length, extensions, issuance requirements, etc.

PKI Glossary

Term	Definition
	When used in a Windows enterprise environment, Certificate Templates exist in the certificate templates container of Active Directory. X.509 attribute extensions are used to define a template's structure.
CLM	Certificate Lifecycle Management is software that allows for the management of certificates throughout their lifecycle
CN	Common Name is the name in a certificate for the entity being issued the certificate.
CMS	Card Management System is software that allows for the management of smartcards and tokens.
CNG	Crypto Next Generation is a term used by Microsoft to describe a technology introduced in Windows Server 2008 that enables hardware and software vendors to interface with Microsoft crypto capability
Code Signing	Code signing creates a digital signature associated with 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 governing policy for the PKI service and all of its components. This document includes the governing attributes such as CA and end-entity certificate lifetimes, CRL requirements and 2uthorized certificate usages and reliance
CPS	Certificate Practices Statement . This document that outlines all of the accepted practices for the management of the PKI services and all of the components including how to manage the Root CA and Issuing CAs, key roles and responsibilities, creation of CA certificates and CRLs, enrolment and approval of end-entity certificates, publication and reliance upon CRLs by relying parties. The CPS is supported by operational procedures and work instructions
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 list of all of the reported compromised certificates that have been issued by the CA, that would otherwise be considered valid. A CRL does not contain expired certificates, as they should not be considered valid.
CRL Overlap Period	A CRL Overlap period is set on the CA to allow time to perform Emergency CRL Signing or to recover the CA before the last CRL expires. The CRL Overlap configuration is set for 1 days, for example, and the base CRL nextUpdate setting is 9 days, then the CRL is valid for a total of 10 days from issuance. This would allow for a 9 day recovery window
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. The cross certificates can also implement rules to limit trust such as name constraints.
CSP	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.

PKI Glossary

Term	Definition
CSR	Certificate Signing Request What the end-entity provides the CA, includes the public key and all of the naming components that need to be added to the certificate.
CTL	Certificate Trust List
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 fact that not all services and systems understand them, as well as 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 is a restricted variant of Basic Encoding Rules for producing unequivocal transfer syntax for data structures described by ASN.1.
DES	Data Encryption Standard is a symmetric-key algorithm for the encryption of digital data. Although its short key length of 56 bits makes it susceptible to attack and is no longer considered secure. DES evolved into 3DES or TDEA but this has also been found to be susceptible to compromise.
DH	Diffie–Hellman key exchange is a mathematical method of securely exchanging cryptographic keys over a public channel. DH is one of the earliest practical examples of public key exchange implemented within the field of cryptography being first published in 1976.
Digest	A digest is the output produced by a hash function after it processes a message.
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 is a set of values based on the X.500 or LDAP standards. A DN often is forms the Subject but can also be seen in a number of other places like the SAN, AIA and CDP
Document Signing	Document signing applies a digital signature to a document. The digital signature verifies the identity of the user that signed the document, ensuring the signer cannot later claim that they signed it. 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. Digital signing also allows a recipient to verify that content of the document was not modified after the digital signature was applied to the document.
DR	Disaster Recovery is the process followed when a major event affects the operation of services.
DRBCP	Disaster Recovery and Business Continuity Plan is the plan that tells operators what to do in an emergency.

PKI Glossary

Term	Definition
DSA	Digital Signature Algorithm is an algorithm used to perform digital signatures as per the X.509 standard
EAP	Extensible Authentication Protocol (EAP) is an authentication framework frequently used in network and internet connections.
ECC	Elliptic Curve Cryptography ECC is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC allows smaller keys compared to non-EC cryptography (based on plain Galois fields) to provide equivalent security.
ECDH	Elliptic-curve Diffie–Hellman (ECDH) is a variant of the Diffie–Hellman protocol using elliptic-curve cryptography. ECDH is a key agreement protocol that allows two parties, each having an elliptic-curve public–private key pair, to establish a shared secret over an insecure channel. This shared secret may be directly used as a key, or to derive another key. The key, or the derived key, can then be used to encrypt subsequent communications using a symmetric-key cipher.
ECDSA	Eliptic Curve Digital Signature Algorithm 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.
EE	End Entity is a certificate issued to user or device that will use the certificate and private key pair.
EFS	Encrypted File System
EKU	Enhanced Key Usage is both a certificate extension and a certificate extended property value.
EoI	Evidence of Identity is the process and documents required to prove a person's identity.
EV	Extended Validation certificates are used for HTTPS websites and software. The registration process for these certificates validates the legal entity controlling the website or software package.
FIPS	Federal Information Processing Standards are standard produced by NIST in order to give some assurance on if something can be trusted.
FQDN	Fully Qualified Domain Name is usually the name given to a device which includes the hostname of that device.
Hash	A Hash is a digital figureprint designed to allow a user to
HSM	Hardware Security Module The HSM is a trusted network computer where the cryptographic processes that PKI requires to remain secure and can be used virtually or on a cloud environment.
HTTPS	HyperText Transport Protocol – Secure Hypertext Transfer Protocol Secure is an extension of the Hypertext Transfer Protocol. It is used for secure communication over a computer network and is widely used on the Internet. In HTTPS, the communication protocol is encrypted using Transport Layer Security.

PKI Glossary

Term	Definition
ICA	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.
IPSec	
ISM	Information Security Manual - The ISM is produced by the Australian Signals Directorate. The purpose of the ISM is to outline a cyber security framework that an 5rganization can apply, using their risk management framework, to protect their systems and data from cyber threats. https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism
Issuance	Issuance is the act of an Issuing Authority in creating a certificate that is bound to a subscriber. The process requires authentication of the subscriber and/or subject.
IT	Information Technology
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 where a private key is archived to allow a user who has lost their private key to recover encrypted data. This should only be done with encryption keys, not signing keys. Within Microsoft AD CS the use of a Key Recovery Agent allows a 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.
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.
L2TP	Layer 2 Tunneling Protocol – is a 5unnelling protocol used in creating VPN connections. However, it only provides 5unnelling – bundling up data for private transportation over public networks. For VPN functionality, it uses Ipsec, which provides encryption and confidentiality.
LDAP	Lightweight Directory Access Protocol (LDAP) is a vendor-neutral software protocol used to lookup information or devices within a network.
LoA	Levels of Assurance are the levels you can trust something to based on the assurance that has gone into the trust of that service.
M of N Authentication	The MofN feature provides a means by which organizations employing cryptographic modules for sensitive operations can enforce multi-person control over access to the cryptographic module, or selected aspects of it. MofN involves a splitting of an authentication secret into multiple parts or splits. The shared secret is distributed (or "split"). Further information: https://thalesdocs.com/gphsm/luna/6.3/docs/network/Content/overview/security_features/mofn_about.htm
MFA	Multi-Factor Authentication is authentication using more than one form such as something you have (a card or USB key), something you know (username and password) or something you are (biometric authentication).

PKI Glossary

Term	Definition
Name Constraints	The Name Constraints extension is used in CA certificates. It specifies the constraints that apply on subject distinguished names and subject alternative names of subsequent certificates in the certificate path. These constraints can be applied in the form of permitted or excluded names.
NDES	Network Device Enrolment Service NDES allows software on routers and other network devices running without domain credentials to obtain certificates based on the Simple Certificate Enrolment Protocol (SCEP). 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 is a United States Federal Government standards body. NIST run a laboratory where they test, develop and recommended standards and best practices for Government such as FIPS.
Non-Repudiation	Non-repudiation refers to the inability of 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. It is used in secure communications to prevent replay attacks. Each packet or conversation is uniquely numbered to ensure both parties are receiving information relating to their request. In PKI, this is optionally used to protect OCSP queries from cached/replay attacks. The signing of a nonce is often used in certificate based authenticaitons.
OCSP	Online Certificate Status Protocol OCSP is used by Certificate Authorities to check the revocation status of an X. 509 digital certificate.
OID	Object Identifier is a globally unique value used in ASN.1
PEAP	The Protected Extensible Authentication Protocol, also known as Protected EAP or simply PEAP, is a protocol that encapsulates the Extensible Authentication Protocol (EAP) within an encrypted and authenticated Transport Layer Security (TLS) tunnel. The purpose is to correct deficiencies in EAP.
PED	Pin Entry Device. Enables you to manage the security administration functions on a Thales Luna hardware security module (HSM). The PED device provides the flexibility to administer an HSM locally or remotely, while still maintaining the highest levels of security through FIPS 140-2-validated two-factor authentication.
PEM	Privacy Enhanced Mail is a file format for X.509 certificate files using Base64 encoding to store and send keys, certificates, and other data.
PIV	Personal Identity Verification is a standard produced by NIST for the storage of identity data on smartcards for Federal Government agencies. It was made a requirement for adoption by Federal Government agencies in Homeland Security Presidential Directive 12. The buying power of Federal Government has made this a defacto industry standard.

PKI Glossary

Term	Definition
PKCS	Public Key Cryptography Standards is a group of 15 numbered standards developed by RSA but now widely adopted. These standards are defined and published by RSA Security LLC. Some common PKCS techniques are PKCS 7, PKCS 10, PKCS 11 and PCKS 12, which cover things like messaging syntax and formatting for digital certificates and how private keys get stored.
PKE	Public Key Enablement is a generic term covering many aspects of the use of PKI
PKI	Public Key Infrastructure The framework and services that provide for the generation, production, distribution, control, accounting, and destruction of public key certificates. Components include the personnel, policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, recover, and revoke public key certificates
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. In most instances a policy CA is not required.
PPTP	Point-to-Point Tunneling Protocol (PPTP) is an obsolete method for implementing virtual private networks. PPTP has many well known security issues.
PQC	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	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. The public key corresponding to a certificate is embedded in the certificate itself.
Public Key Encryption	Public-key encryption uses two separate keys that are mathematically related, to encrypt and decrypt the content. The public key can be distributed widely while the private key remains with the user or device that created the key pair.
RA	Registration Authority validates user information for the CA and can be used to authority certificate creation by the CA after authorisation. It can also be used as a source of EE registration information.
RADIUS	Remote Authentication Dial-In User Service is a networking protocol that provides centralized authentication, authorization, and accounting management for users who connect and use a network service.
RCA	Root Certification Authority is the root of the hierarchy of a PKI. A Root CA will have a self signed certificate.

PKI Glossary

Term	Definition
Re-Key	A re-key involves changing out the cryptographic key that is being used in a cryptographic system application. This entails issuing a new certificate with the new public key embedded in it.
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 location where public CA certs, EE Certs, CRLs, CP, CPS, and other PKI documentation is available for review. It often takes the form of a HTTP website, but can be an LDAP Directory or even an FTP based site.
RFC	Request for Comments (RFC) is a publication in a series from the principal technical development and standards-setting bodies for the Internet, most prominently the Internet Engineering Task Force (IETF). PKI relies heavily on RFCs.
Revocation	Revocation of a certificate invalidates a previously signed certificate and is listed in the next published CRL by serial # and date of revocation. A revocation method is essential to a PKI. It ensures the remaining certificates can be trusted.
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 Administrators/Operators separated with an Operations Manager, with other roles such as Auditor/Security Officer, Platform Support, Registration Officers and Backup Operators all common roles. Role separation should be fully defined in the Certificate Policy.
RSA	Rivest Shamir Adleman – the inventors of composite prime group public key encryption and signature algorithms.
SAN	Subject Alternate Name The Subject Alternative Name (SAN) is an X.509 v3 certificate extension that binds additional information to the subject DN of this certificate. Common examples include DNS Name and RFC822 Name (email address).
SCEP	Simple Certificate Enrolment Protocol SCEP, is a protocol that allows devices to easily enrol for a certificate by using a URL and a shared secret to communicate with a PKI.
SCVP	Simple Certificate Validation Protocol is another protocol for the validation of certificates
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. An example of a protocol that uses session keys is TLS.
SHA	Secure Hash Algorithm SHA hash functions are used by Certificate Authorities when signing Certificate Revocation Lists and Digital Certificates. A Secure Hash Algorithm is meant to generate unique hash values from files. Common deprecated hashing algorithms including MD5 and SHA-1. SHA-2 is a common secure hashing algorithm and comes in the following sizes being SHA-128, SHA-256, SHA-384 and SHA-512. SHA-128 should be deprecated.
S/MIME	Secure/Multipurpose Internet Mail Extensions) is a standard for public-key encryption and signing of MIME data. S/MIME was originally developed by RSA Data Security, but is now

Term	Definition
	maintained as part of IETF standards. It is defined in a number of documents, most importantly RFC 8551
Smartcard	Either comes in a credit card-sized hardware token chip or USB form factor. It 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 is an older form of HTTPS authentication and encryption and is used exclusively for HTTPS traffic.
SSTP	Secure Socket Tunneling Protocol, is a VPN protocol that creates a tunnel between a client device and a server. Primarily, SSTP is used to secure remote access to private networks over the internet.
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
TDEA	Triple Data Encryption Algorithm is a symmetric-key block cipher, which applies the DES cipher algorithm three times to each data block. The Data Encryption Standard's (DES) 56-bit key is no longer considered adequate in the face of modern cryptanalytic techniques and supercomputing power. A CVE released in 2016, CVE-2016-2183 disclosed a major security vulnerability in DES and 3DES encryption algorithms. This CVE, combined with the inadequate key size of DES and 3DES, led to NIST deprecating DES and 3DES for new applications in 2017, and for all applications by the end of 2023.[1] It has been replaced with the more secure, more robust AES.
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 a 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 Server	A Time-Stamping Server is a server or service issuing time-stamps for use by other entities.
TLS	Transport Layer Security can be used for authentication and encryption but is newer than SSL and can be used for protocols including but not limited to HTTPS.
TPM	Trusted Platform Module (TPM) is an international standard for a secure cryptoprocessor, a dedicated microcontroller designed to secure hardware through integrated cryptographic keys. The term can also refer to a chip conforming to the standard ISO/IEC 11889.

Term	Definition
VA	Validation Authority is a sub-component of CA function that works in
Validation	Validation is the process by which an end-entity certificate certifies information in a certificate to confirm it's authenticity. This can include checking the chain of trust in a PKI, the date of expiry of a certificate, ensuring the certificate has not been revoked or tampered with.
Validity Period	The period that is defined within a certificate or CRL, during which that certificate or CRL is intended to be valid. For a certificate, it generally begins when the certificate is issued and ends at the end date embedded in the certificate unless it is revoked or suspended earlier.
VPN	A VPN, or Virtual Private Network, is a tool that encrypts your internet traffic and hides your IP (Internet Protocol) address to ensure a secure and private connection to the internet. This prevents third parties from snooping or collecting data about your activity because all information stays hidden behind a code.
X.509	X.509 is an International Telecommunication Union (ITU) standard defining the format of public key certificates. X.509 certificates are used in many Internet protocols, including TLS/SSL, which is the basis for HTTPS, the secure protocol for browsing the web. They are also used in offline applications, like electronic signatures.