NIC PKI GLOSSARY

Document Classification:

Public

Version Number: 1.1

Issue Date: July 14, 2024

عام

Document Revision History

Version	Date	Author(s)	Revision Notes
1.0	May, 2023	Ammar Alsofyani	Initial Document
1.1	2024	Ammar Alsofyani , Abdulaziz Aldwish	Annual review

1. Introduction

This document contains the definitions or terms accepted by NIC and used throughout NIC PKI documentation. The definitions in this document shall apply equally to both the singular and plural forms of the terms defined. When the context requires, any pronoun shall include the corresponding masculine, feminine and neuter forms.

2. Audience

This document is intended for the use of participants in NIC and any parties contracted by them to participate in the Saudi National PKI.

3. Definitions

- **Access**
  Ability to make use of any information system (IS) resource.

- **Access Control**
  The process of ensuring that systems are accessed only by those authorized to do so, and only in a manner for which they have been authorized.

- **Access Control List (ACL)**
  ACLs control who can access different parts of a system. In the Sentry family of products, ACLs are used primarily to control who has access to files and directories on a Web server.

- **Algorithm**
  An algorithm is a set of rules that specifies a method of carrying out a task (e.g., encryption algorithm).

- **Anonymity**
  Ability to use public keys while only revealing information about the participating entities that is pertinent to the situation.

- **Applicant**
  Any entity that has applied to get a Certificate, such as subscribers or CAs wishing to cross-certify with or join the NIC.

- **Arbitration**
  The non-judicial submission of a controversy to selected third parties for their determination.

- **Availability**
  The property of a system or a system resource that ensures it is accessible and usable upon demand by an authorized user.

- **Archive**
  To store records for a given period of time for security, backup, or auditing purposes.

- **Audit**
  Audit is defined as an independent review and examination of system records and activities to assess the adequacy and effectiveness of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies or procedures.

- **Audit Policy**
  This document details the auditing policies of PKI for the National Information Center.

- **Asset Register**
  A record of items considered worthy of identification as discrete assets.

- **Asymmetric Encryption**
  Encryption that uses different keys for encryption and decryption.

- **Attack**
  An attempt to gain unauthorized data access.

- **Audit Logs**
  All significant transactions are recorded in audit logs. Audit logs are valuable because they record all significant operations.

- **Authentication**
  A process used to confirm the identity of a person or to prove the integrity of specific information.

- **Authority Revocation List (ARL)**
  A list of revoked CA certificates.

- **Authorization**
  Determining whether a subject is trusted for a given purpose.

- **Backup**
  Copy of files and programs made to facilitate recovery if necessary.

- **BS ISO/IEC 17799:2005**
  An international standard for Information Security Management. It provides a comprehensive set of controls comprising best practices in information security.

- **Business Continuity Policy**
  A document that outlines the policy to ensure that plans and procedures are in place for a prompt resumption of the Saudi National PKI processes in the event of a disruption to normal operational activities.

- **CA Administrator**
  A trusted person who uses certificate software to enable and disable users individually or in bulk, revoke user's keys, initiate key recovery for users, create new encryption key pairs for users, disable and re-enable a user's ability to sign

files, and increase the maximum number of users in a CA domain. The Administrator can also review audit logs. Depending on the organization's security policy, the Administrator may also be able to change default user certificate lifetimes (and perhaps disable certificate updates) and default Encryption and Verification policies. They can also issue new CRLs.

- **Certificate**
  A digital identifier linking an entity and a trusted third party able to confirm the entity's identity. It is used to verify the identity of an individual, organization, or Web server, and to ensure non-repudiation in business transactions. Three major kinds of certificates are used in a PKI: CA certificates, device certificates, and end-entity certificates. In this context, the terms 'Certificate' and 'Digital Certificate' are used interchangeably.

- **Certification path**
  An ordered sequence of certificates that, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path.

- **Certificate Policy (CP)**
  A named set of rules that indicate the applicability of a certificate to a particular community and/or class of application with common security requirements.

- **Certification Practice Statement (CPS)**
  A statement of the practices which a certification authority employs in issuing and managing certificates.

- **Certificate Profile**
  The specification of the fields to be included in a Certificate.

- **Certification Authority (CA)**
  Authority trusted by one or more users to create and issue digital certificates and vouch for the binding between the data items in a certificate and the subject. In this context, a CA can be the Root CA, DTSPs, Issuing CAs, and any entity allowed to cross certify with the NIC.

- **Digital Trust Service Provider (DTSP)**
  The entity which is licensed to issue digital certificates or provide another service or mission relating to that or to the electronic signatures according to the e-transactions law.

- **Certificate Revocation List (CRL)**
  Data structure that enumerates digital certificates that have been invalidated by their issuer prior to when they were scheduled to expire.

- **Certificate Status Request**
  An electronic Record that requests the status of a Digital Certificate to establish if the Digital Certificate is valid or invalid.

- **Certificate Status Response**
  A digitally signed Record provided by a CRL or OCSP responder in response to a Certificate Status Request.

- **Change Management**
  It is the process of developing a planned approach to change in an organization. Typically the objective is to maximize the collective benefits for all people involved in the change and minimize the risk of failure of implementing the change.

- **Change Management Policy**
  The document that outlines the principles for undertaking any changes in the Saudi National PKI environment.

- **Ciphertext**
  A term used to describe text (or data) that has previously been encrypted; see Encryption.

- **Classification**
  A systematic arrangement in groups or categories according to criteria.

- **Common Criteria**
  A standard for evaluating information technology products and systems, such as operating systems, computer networks, distributed systems, and applications. It states requirements for security functions and for assurance measures.

- **Compliance Audit**
  A review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, to detect breaches in security, and to recommend any indicated changes in control, policy and procedures.

- **Compliance Officer**
  The NIC PKI Compliance Officer is responsible for developing and implementing a legally and regulatory PKI compliant governance and compliance framework for the NIC.

- **Compromise**
  Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.

- **Concept of Operations (ConOps)**
  A high level requirements document that provides:
  - purpose of a system
  - business need(s) that a system will satisfy
  - user expectations
  - basic concepts behind a system
  - system's characteristics and behaviors from a user's point of view

- **Confidentiality**
  Confidentiality is the guarantee that data is not shared with unauthorized entities.

- **Cross Certification**
  The act or process by which two Certification Authorities establish a trust relationship by issuing each other Digital Certificates.

- **Cross Certificate**
  A certificate issued by a Certification Authority to establish a trust relationship between it and another Certification Authority that is not part of the hierarchy.

- **Cross Certification Policy**
  A policy that outlines the issues and criteria for cross-certification of the Certification Authority of an applicant's Public Key Infrastructure (PKI) with the Saudi National Root CA if approved by the NIC inside and outside the Kingdom of Saudi Arabia.

- **Cryptographic Algorithm or Cipher**
  The mathematical function used for encryption and decryption. Generally there are two related functions: one for encryption, the other for decryption.

- **Cryptographic Key**
  A mathematical term or other parameter used to define how a given algorithm will transform data into ciphertext.

- **Cryptographic Module**
  A Cryptographic Module is hardware, software, or firmware or any combination of them which, by using Cryptography, can protect the information stored therein.

- **Cryptography**
  The art or science of transforming clear, meaningful information into an enciphered, unintelligible form using an algorithm and a key.

- **Cryptosystem**
  An algorithm plus all possible plaintexts, ciphertexts, and keys.

- **Data Integrity**
  When digital signatures are used, the assurance that the data is unchanged from the moment that a digital signature is applied to the data.

- **Decryption**
  Decryption is the process of transforming ciphertext back into plaintext. It is the reverse of encryption.

- **Digital Signature**
  The result of a transformation of data by means of a cryptographic system using keys such that a person who receives the initial data can determine whether:

- The transformation was created using the key that corresponds to the signer's key; and
- The data has been altered since the transformation was made.

- **Directory**
  Databases that can be used to search for and retrieve attribute-value pairs. Directories can be configured to use (or support) authentication and access control protection. The schema of a directory describes the objects in the directory.

- **Directory Service Markup Language**
  DSML is a vocabulary and schema for describing the structure and content of directory services information in an XML Document. Directory information can then be easily used by any application that makes use of XML, including browsers and e-commerce applications.

- **Dispute Parties**
  Two or more parties engaged in a disagreement or dispute arising out of the PKI activities of the NIC.

- **Dispute Resolution**
  Dispute resolution is the process of resolving disputes between parties. Methods of dispute resolution adopted in the Saudi National PKI include Informal Negotiation, Mediation and Arbitration.

- **Dispute Resolution Policy**
  The Dispute Resolution Policy is applicable to all participants of the NIC and it defines the types of claims and disputes it applies to, to whom it applies, the dispute resolution procedure, and any exceptions or exclusions.

- **Distinguished Name (DN)**
  The complete name of a Directory entry. The distinguished name is composed of the entry's RDN and the RDNs of each of the entries that lie directly between the entry and the root of the tree.

- **Encipher**
  Conversion of plain data into encrypted data (plaintext into ciphertext).

- **Encryption**
  The process of transforming plaintext data into an unintelligible form such that the original data either cannot be recovered.

- **Encryption Certificate**
  A Certificate containing a public key that is issued to encrypt electronic messages, files, documents, or information.

- **End Entity Certificate**
  A certificate issued to an entity that cannot itself issue certificates (in essence, it is not a CA).

- **End User**
  An Entity that uses the keys and certificates created within a public key infrastructure for purposes other than the management of keys and certificates. An End-User may be a Subscriber, a Relying Party, or a device.

- **Enrolment**
  A process by which an individual or an organization registers to receive services from, or make transactions with, a specific Program.

- **Entity**
  A person, device, organization, or piece of information. In a PKI, an entity may be thought of as anything to which a certificate may be issued.

- **Evaluation Assurance Level 4+**
  A Common Criteria assurance level assigned to a product that has been methodically designed, tested and reviewed.

- **Hardware Security Module**
  A hardware device used for storing cryptographic keys and performing cryptographic functions.

- **Hypertext Transfer Protocol (HTTP)**
  Hypertext Transfer Protocol is a TCP-based, application-layer, client-server, Internet protocol [R2616] used to carry data requests and responses in the World Wide Web.

- **Identification**
  The process of establishing the identity of an individual or organization, i.e., to show that an individual or organization is a specific individual or organization. In this context, identification refers to two processes: (1) establishing that a given name of an individual corresponds to a real-world entity, and (2) establishing that an individual applying for or seeking access to something under the name is, in fact, the named individual.

- **Identification & Authentication (I&A)**
  The process used to determine and prove the identity of an applicant for a Certificate.

- **Integrity**
  A condition in which the data has not been changed or destroyed in an unauthorised way.

- **Internet Engineering Task Force (IETF)**
  A large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual. The mission of the IETF is to produce high quality, relevant technical and engineering documents that influence the way people design, use, and manage the Internet in such a way as to make the Internet work better.

- **Intellectual Property**
  Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.

- **Interoperability**
  Interoperability implies that equipment and procedures in use by two or more entities are compatible, and hence that it is possible to undertake common or related activities.

- **Issuing certification authority (Issuing CA)**
  Issuing CAs are CAs issuing Certificates to Subscribers.

- **Key backup**
  A reserve copy of data that is stored separately from the original, for use if the original becomes lost or damaged.

- **Key Escrow**
  A deposit of the private key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the subscriber, the terms of which require one or more agents to hold the subscriber's private key for the benefit of the subscriber, an employer, or other party.

- **Key Lifetime**
  The length of time for which a key is valid.

- **Key Update**
  When key pairs are updated, they are replaced with the new key pairs, and new public key certificates are created. The new keys and certificates have no relation to the old keys and certificates.

- **Key**
  When used in the context of encryption, a series of numbers which are used by an encryption algorithm to transform plaintext data into encrypted (ciphertext) data, and vice versa.

- **Key Pair**
  A set of mathematically related keys, a public key and a private key, that are used for asymmetric cryptography and are generated in a way that makes it computationally infeasible to derive the private key from knowledge of the public key.

- **LDAP Intelligent Referral**
  LDAP functionality enabling a server which receives a search request for an object in a naming context it doesn’t host, to return a referral listing the LDAP servers where the naming context can be found.

- **Liability**
  A Liability is product, service or payment, owed to another party. Liabilities are connected directly to damages that may have resulted from failure of an obligation or warranty.

- **Lightweight Directory Access Protocol (LDAP)**
  A client-server protocol that supports basic use of the X.500 Directory (or other directory servers) without incurring the resource requirements of the full Directory Access Protocol (DAP).

- **Local Registration Authority (LRA)**
  A Registration Authority with responsibility for a local community.

- **Mediation**
  Mediation is the process of facilitated communication between opposing parties by an impartial third party, known as the mediator.

- **National Information Center (NIC)**
  The National Information Center (NIC) is the entity controlling and managing the National Public Key Infrastructure for the Kingdom of Saudi Arabia including all participants. The NIC's mandate is stipulated in the Saudi e-Transactions law, which is to supervise the tasks relating to management and usage of digital certificates in the Kingdom. The NIC owns the Root CA. The NIC also includes the National Information Center – PKI Center (NIC-PKIC) which operates the Saudi National Root CA and the CAs of DTSPs who choose to outsource their operations to the NIC-PKIC.

- **National Information Center PKI Center (NIC-PKIC)**
  The National Information Center-PKI Center (NIC-PKIC) is the operational component of the NIC providing a full range of CA and certificate lifecycle services. It operates the National Root CA and the CA's of DTSPs who choose to outsource their operations to the NIC-PKIC.

- **Non-repudiation**
  Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. Technical non-repudiation refers to the assurance a Relying Party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding signing Private Key. Legal non-repudiation refers to how well possession or control of the private Signing Key can be established.

- **Object Identifier (OID)**
  The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class.

- **Obligation**
  An obligation is a requirement that must be fulfilled. For example, the client's obligation is to pay the bill and the vendor's obligation to deliver the product.

- **OCSP Responder**
  A process that responds to Certificate Status Requests and that can issue one of three responses: “Valid”, “Invalid”, or “Unknown,” based on Certificate Revocation Lists or other mechanisms provided to it by Certification Authorities.

- **On-Line Certificate Status Protocol (OCSP)**
  Protocol used to provide real-time validation of a digital certificate’s status.

- **Online Validation**
  Online validation occurs when a CA can be queried directly about a certificate’s validity every time the certificate is used.

- **Out-of-Band**
  Communication between parties utilizing a means or method that differs from the current method of communication.

- **Participant**
  An individual or organization that plays a role within the NIC as a subscriber, relying party, CA, RA, DTSP, repository service provider, or similar entity.

- **Parties**
  The entities whose rights and obligations are intended to be controlled by the CP and CPS. These entities may include certificate applicants, CAs, subscribers, and relying parties.

- **Password**
  A sequence of characters which allows users access to a system.

- **Personal Identification Number (PIN)**
  A sequence of digits used to verify the identity of the holder of a token. It is a kind of password.

- **PKCS#11**
  Cryptographic Token Interface Standard.

- **PKCS#7**
  Cryptographic Message Syntax.

- **Plaintext**
  Data before the application of a cryptographic algorithm.

- **Privacy Policy**
  A Document which describes policies dealing with the collection, storage, access, use and disclosure of Personal Information.

- **Public Key**
  The public component of a pair of cryptographic keys used for asymmetric cryptography. In a public key cryptosystem, this key of a user's key pair is publicly known.

- **Public Key Cryptography**
  A form of asymmetric encryption where all parties possess a pair of keys, one private and one public, for use in encryption and digital signing of data.

- **Public Key Infrastructure**
  The infrastructure needed to generate, distribute, manage and archive keys, certificates and certificate revocation lists, and OCSP responders.

- **Publish/Publication**
  To record or file information in a repository in order to disclose and make publicly available such information in a manner that is consistent with the CP, CPS and applicable law.

- **Privacy**
  Restricting access to subscriber or Relying Party information in accordance with Privacy policy and applicable laws.

- **Private Key**
  The secret component of a pair of cryptographic keys used for asymmetric cryptography. In a public key cryptosystem, this key is known only by its user.

- **Re-key (a certificate)**
  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.

- **Renew (a certificate)**
  The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.

- **Revocation**
  Revoking a certificate makes the certificate invalid, effectively suspending all of the certificate user's privileges in the PKI. Revocation is necessary if the CA administrator wants to retract the certificate before it expires. Certificates are revoked by marking them as invalid in the Secure Directory. Users of the PKI are notified of a certificate's revoked status during online validation or with CRLs.

- **Revoke (a Certificate)**
  To prematurely end the operational period of a certificate effective at a specific date and time.

- **Registration**
  The process for receiving and processing applications for Keys and Certificates, including collection of Registration Information.

- **Registration Authority (RA)**
  An entity which registers Applicants for Keys and Certificates and that is responsible for the identification and authentication of Subscribers and other

End Entities. RAs may have other functions or obligations specified in the relevant CP.

- **Registration Information**
  The RA is an entity approved and trusted by a DTSP to support registration and to perform the identification and authentication (I&A).

- **Relative Distinguished Name (RDN)**
  The name of the actual entry itself, before the entry's ancestors have been appended to the string to form the full distinguished name.

- **Relying Party (RP)**
  A Relying Party is any entity that places comfort on information provided by DTSPs approved by the NIC regarding a specific transaction that the RP uses to accept or reject their participation in the transaction.

- **Relying Party Agreement (RPA)**
  An agreement between a Digital Trust Service Provider or a CA and a relying party that establishes the rights and responsibilities between the two parties regarding the verification of digital signatures or other uses of certificates.

- **Repository**
  A system where CRLs, ARLs and public key certificates are stored for access by Entities. In this context, Repositories support CRLs and OCSP responders.

- **Request for Comment (RFC)**
  A document that describes the specifications for a recommended technology. RFCs are used by the Internet Engineering Task Force (IETF) and other standards bodies.

- **Revoked**
  With respect to a Digital Certificate, the designation by an Issuer that a previously valid certificate is invalid.

- **Right**
  A right is a result or outcome that a party is justly entitled to. For example, the customer’s right is to receive a product or service in the manner in which it was specified. The vendor’s right is to receive payment for products and services provided.

- **Risk Assessment**
  A study of vulnerabilities, threats, likelihood, loss or impact, and the theoretical effectiveness of security measures.

- **Root Certification Authority (Root CA)**
  It is the apex of a PKI hierarchy which is owned and provided by the NIC. It is self-signed and self-certified.

- **Secure Hypertext Transfer Protocol (HTTPS)**
  An Internet protocol for providing client-server security services for HTTP communications. When used in the first part of a URL (the part that precedes the colon and specifies an access scheme or protocol), this term specifies the use of HTTP enhanced by a security mechanism, which is usually SSL.

- **Security Policy**
  This document details the security policy for the National Information Center.

- **Security Zone**
  An area to which access is limited to authorized personnel.

- **Secure Sockets Layer (SSL)**
  Secure Sockets Layer (SSL) is an Internet protocol (originally developed by Netscape Communications, Inc.) that uses connection-oriented end-to-end encryption to provide data confidentiality service and data integrity service for traffic between a client (often a web browser) and a server, and that can optionally provide peer entity authentication between the client and the server.

- **Secure Hash Algorithm**
  Secure Hash Algorithm—a hash function first originated by the US National Security Agency and National Institute of Standards and Technology

- **Subject**
  The name given to a user of a public key security system.

- **Subscriber**
  An individual or organization whose public key certificates are signed by an issuing CA operating under the NIC. The subscriber could be either Human (citizens) or entity (Businesses or government departments) or non-human (devices).

- **Subscriber Agreement**
  An agreement between a DTSP and a Subscriber that establishes the right and responsibilities of the parties regarding the issuance and management of certificates.

- **Subscriber Information**
  Information supplied to a DTSP as part of a certificate application.

- **Subordinate CA**
  In a hierarchical PKI, a CA whose certificate signing Key is certified by another CA, and whose activities are constrained by that other CA. In this context, Subordinate CAs are DTSPs, i.e. all CAs signed by the Root CA.

- **Subordinate CA Agreement**
  An agreement between a CA and a Subordinate CA that establishes the right and responsibilities of the parties regarding the issuance and management of certificates.

- **Symmetric Key**
  A key that can be used to encrypt and decrypt the same data.

- **Time Stamp**
  A time stamp is a record that indicates (at least) the correct date and time of an action (expressly or implicitly) and the identity of the person or device that created the notation.

- **Transport Layer Security (TLS)**
  Transport Layer Security (TLS) Version 1.0 is an Internet protocol [R2246] based-on and very similar to SSL Version 3.0.

- **Token**
  A hardware security token containing a user's private key(s), public key certificate, and, optionally, a cache of other certificates, including all certificates in the user's certification chain.

- **Trust Anchor**
  A certificate that is trusted by the Relying Party on the basis of secure and authenticated delivery. The public keys included in trust anchors are used to start certification paths. The trust anchor in the Saudi PKI is the Root CA.

- **Trustworthy System**
  Computer hardware, software, and procedures that are reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy.

- **Uniform Resource Indicator/Identifier**
  A Uniform Resource Indicator/Identifier (URI) is a set of character strings that is used for identifying resources. A URI provides a simple and extensible means for identifying a resource that can then be used within applications. URI's form a superset of three distinct groups of identifiers; URLs - Uniform Resource Locators; URNs - Uniform Resource Names; and URCs - Uniform Resource Characteristics.

- **Uniform Resource Locator (URL)**
  A standardised device for identifying and locating certain records and other resources located on the World Wide Web.

- **Validation**
  The process of identification of certificate applicants. "Validation" is a subset of "identification" and refers to identification in the context of establishing the identity of certificate applicants.

- **Warranty**
  A warranty is a promise that the good being sold has been factually and accurately represented. A vendor obliged to provide representations regarding the product or service.

- **X.509**
  The ITU-T (International Telecommunications Union-T) standard for certificates. X.509 v3 refers to certificates containing or capable of containing extensions.

4. Abbreviations

ACL	Access Control List
ARL	Authority Revocation List
CA	Certification Authority
ConOps	Concept of Operations
CN	Common Name
CRL	Certificate Revocation List
CP	Certificate Policy
CPS	Certification Practice Statement
DTSP	Digital Trust Service Provider
DES	Data Encryption Standard
DN	Distinguished Name
DSA	Digital Signature Algorithm
DSML	Directory Service Markup Language
DSS	Digital Signature Standard
EAL4+	Evaluation Assurance Level 4+
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
HTTPS	Secure Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
LDAP	Lightweight Directory Access Protocol
LRA	Local Registration Authority
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
RA	Registration Authority
RDN	Relative Distinguished Name
RFC	Request for Comment
SHA	Secure Hash Algorithm
SSL	Secure Socket Layer
TLS	Transport Layer Security
URL	Uniform Resource Locator
URL	Uniform Resource Locator