IdenTrust
part of HID Global

Glossary of Terms and Acronyms

Glossary

Accept or Acceptance	Acceptance is a subscriber act that triggers the subscriber's rights and obligations with respect to a certificate under a specific CP, CPS and/or RPS.
Access	Ability to make use of any information system resource.
Access Control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems.
Account Password	An account password is a value selected by an applicant and known only to that applicant which value is provided during the registration process and utilized to authenticate when retrieving or managing a certificate.
Accreditation	Formal declaration by a designated approving authority that an information system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.
Activation Code	An activation code is a randomly generated, secret numeric code created by the CA or RA and securely delivered to the applicant for use by the applicant for authentication purposes.
Activation Data	Private data, other than keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or decryption events).
Agency	Any department, subordinate element of a department, or independent organizational entity that is statutorily or constitutionally recognized as being part of the Executive Branch of the Federal Government.
Agency CA	A CA that acts on behalf of an agency, and is under the operational control of an agency.
Antecedent Event	An antecedent event is an event through which an applicant has previously provided in-person proof of identity. As an example, an applicant may have previously provided proof of identity to an HR Individual. See also Sponsor Antecedent.
Applicant	The subscriber is sometimes also called an "applicant" after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed.
Archive	Long-term, physically separate storage.
Assurance Level	Assurance Level is the level of confidence that a participant should have that the assertion or use of a private/public key pair or certificate correctly

Glossary of Terms and Acronyms

	references the identity, authority, or subscribing organization of the subscriber, and that the key pair is correctly bound to the identified subject, and that the subject controls the private key, and that the private key has not been compromised.
Attribute Authority	An entity recognized by the Federal PKI Policy Authority or comparable agency body as having the authority to verify the association of attributes to an identity.
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.
Audit Data	Chronological record of system activities (i.e., audit trail) to enable the reconstruction and examination of the sequence of events and changes in an event.
Authenticate	To confirm the identity of an entity when that identity is presented.
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.
Authority Information Access	An extension in a certificate that 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.
Authorized Registration Authority	A Registration Authority that is either an IdenTrust-employed registration agent, an RA under contract for managing certificates, or an agency under a contractual or other agreement to perform RA functions.
Authorizing Official	An authorizing official is an individual designated in a written agreement within a CA, or RA who can appoint and authorize other Individuals to act as LRAs or Trusted Agents for that organization.
Backup	Copy of files and programs made to facilitate recovery if necessary.
Binding	Process of associating two related elements of information.
Biometric	A physical or behavioral characteristic of a human being.
Business Associate	A business associate helps covered entities carry out health care activities and functions under a written business associate contract or other

Glossary of Terms and Acronyms

	arrangement with the business associate that establishes specifically what the business associate has been engaged to do and requires the business associate to comply with the requirements to protect the privacy and security of protected health information.
CA Certificate	The CA certificate is the certificate containing the public key that corresponds to the CA private signing key used by a CA to create or manage certificates.
CA Facility	The collection of equipment, personnel, procedures and structures that are used by a CA to perform certificate issuance and revocation.
CA/B Forum or CA/Browser Forum	The Certificate Authority and Browsers Forum is a voluntary organization of leading Certification Authorities and vendors of internet browser software and other applications. Members of the CAB Forum provide guidelines known as the CA/Browser Forum Baseline Requirements for the issuance and management of publicly-trusted certificates and means of implementation for the extended validation SSL certificate standard as a way of providing a heightened security for internet transactions and creating a more intuitive method of displaying secure sites to internet users.
CA Private Signing Key	The CA private signing key is the private key that corresponds to the CA's public key listed in the CA certificate and used to sign and otherwise manage certificates.
Card Authentication Certificate	A card authentication certificate is a certificate that is Issued to a smart card controlled by the organization identified within the certificate.
Card Management System	The Card Management System is responsible for managing the content in smart cards.
Certificate	A digital representation of information which at least (a) identifies the certification authority issuing it, (b) names or identifies its subscriber, (c) contains the subscriber's public key, (d) identifies its operational period, and (e) is digitally signed by the certification authority issuing it.
Certificate Chain	A certificate chain is an ordered series of certificates connecting a subscriber's certificate to the root certificate. CA certificates in a certificate chain are connected by successive, superior CA certificates up to the root certificate, which may be a self-signed certificate.
Certificate Information System	The Certificate Information System is a database maintained by IdenTrust that contains account information about applicants and subscribers.

2018-06-11-identrust-glossary-of-terms-and-acronyms-en

IdenTrust
part of HID Global

Glossary of Terms and Acronyms

Certificate Management Authority	An entity that is delegated or outsourced the task of actually manufacturing the certificate on behalf of an Authorized CA.
Certificate Policy	A Certificate Policy is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.
Certificate Profile	A certificate profile is the format and contents of data fields in a certificate that identify the Issuer, the subject, the public key and other information about the Subject.
Certificate-Related Information	Information, such as a subscriber's postal address, that is not included in a certificate.
Certificate Revocation List	A Certificate Revocation List is a list of certificates that have been revoked prior to the expiration of their validity period.
Certificate Status Authority	A Certificate Status Authority is the component of a PKI that provides authoritative responses to online requests for certificate status information, such as certificate validity, validation of the entire certificate chain, and revocation status.
Certificate Type	Certificate type defines a more granular certificate usage or function within a particular Assurance Level.
Certification	The technical evaluation, made as part of and in support of the accreditation process that establishes the extent to which a particular computer system or network design and implementation meet a pre-specified set of security requirements.
Certification and Accreditation	Process of testing all aspects of system security leading to a formal declaration by a designated approving authority that an information system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.

2018-06-11-identrust-glossary-of-terms-and-acronyms-en

IdenTrust
part of HID Global

Glossary of Terms and Acronyms

Certification Authority	A Certification Authority is an organization that attests to the binding between an identity and cryptographic key pair.
Certification Authority Revocation List	A signed, time-stamped list of serial numbers of CA public key certificates, including cross-certificates that have been revoked.
Certification Authority Software	Key management and cryptographic software used to manage certificates issued to subscribers.
Certification Practice Statement	A Certification Practice Statement is a statement of the practices that a CA employs in creating, issuing, managing, and, revoking certificates in conformance with a particular CP.
Client (application)	A system entity, usually a computer process acting on behalf of a human user that makes use of a service provided by a server.
Client-authenticated SSL/TLS-Encrypted Session	A Client-authenticated SSL/TLS-Encrypted Session is a session securely communicated through use of the Secure Sockets Layer and Transport Layer cryptographic protocols.
Common Criteria	A set of internationally accepted semantic tools and constructs for describing the security needs of customers and the security attributes of products.
Component Private Key	Private key associated with a function of the certificate issuing equipment, as opposed to being associated with an operator or administrator.
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.
Computer Security Objects Registry	Computer Security Objects Registry operated by the National Institute of Standards and Technology.
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes.
Content Signing Certificate	A content signing certificate is a certificate that is utilized by a CMS to digitally sign content embedded in smart cards.
Covered Entity	A covered entity is an individual, organization, or agency that protects the privacy and security of health information and provides individuals with certain rights with respect to their health information.

2018-06-11-identrust-glossary-of-terms-and-acronyms-en

IdenTrust
part of HID Global

Glossary of Terms and Acronyms

Critical Infrastructure	Those physical and cyber-based systems essential to the minimum operations of the economy and government, including but not limited to telecommunications, energy, banking and finance, transportation, water systems, and emergency services, both governmental and private.
Cross-Certificate	Cross-certification is the issuance of a certificate used to establish a trust relationship between two PKIs. The cross-certificate is the certificate Issued by one PKI to another PKI for cross-certification.
Cryptographic Module	A cryptographic module is secure software or hardware that: (a) generates key pairs; (b) stores cryptographic information; and (c) performs cryptographic functions.
Cryptographic Service Provider	A Cryptographic Service Provider is an independent software module or set of programs (e.g. an application program interface, or "API") used with a given device to provide a concrete implementation of a set of cryptographic algorithms to be used for authentication, encoding, encryption and other cryptographic functions.
Cryptoperiod	Time span during which each key setting remains in effect.
Data Encryption Standard	NIST data encryption standard adopted by the US government as FIPS PUB 46, which allows only hardware implementations of the data encryption algorithm.
Data Integrity	Assurance that the data are unchanged from creation to reception.
Device	A device is a non-human subscriber of a certificate. Examples of devices include but are not limited to routers, firewalls, servers, and other devices capable of securely handling private keys and properly implementing PKI technologies.
Device Certificate	A device certificate is a certificate issued to a device.
Digital Signature	A digital signature is the result of or mathematical transformation of a document or message through use of cryptography. To digitally sign a message is the act of applying a digital signature. A relying party in receipt of a document or message with a digital signature can accurately determine: (a) whether the transformation was created using the private key corresponding to the public key; and (b) whether the message or document has been altered since the transformation was made.

2018-06-11-identrust-glossary-of-terms-and-acronyms-en

Glossary of Terms and Acronyms

Direct	Direct refers to the Direct Project (http://wiki.directproject.org/)/. Direct Project developed the original Direct Ecosystem Community Certificate Policy Version 0.9 in accordance with its consensus process.
Directory Information Tree	A Directory Information Tree is data represented in a hierarchical structure containing the distinguished names of directory service entries.
DirectTrust	DirectTrust is a non-profit, competitively neutral, self-regulatory entity operated by and for participants in the Direct community. DirectTrust operates the Direct Trust Policy Authority (DTPA) that is responsible for the DirectTrust CP, the approval of related practice statements, and overseeing the conformance of CA practices with DirectTrust CP.
DirectTrust Certificates	DirectTrust certificates are those certificates that are issued for use within Direct as defined in the Direct Project Applicability Statement for Secure Health Transport and more specifically by the DirectTrust Certificate Policy.
Distinguished Name	A distinguished name is a unique name-identifier for the issuer or the subject of a certificate so that he, she or it can be located in a directory.
Domain Bound Certificate	A domain bound certificate is a certificate that contains a domain name in the form of a dNSName in the subjectCommonName and subjectAlternativeName extensions of the certificate.
Domain Name	The label assigned to a node in the Domain Name system.
Domain Registrant (also Domain Name Registrant)	Sometimes referred to as the “owner” of a domain name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a domain name is used, such as the natural person or Legal Entity that is listed as the “Registrant” by WHOIS or the Domain Name Registrar.
Dual Use Certificate	A certificate that is intended for use with both digital signature and data encryption services.
Duration	A field within a certificate, which is composed of two subfields; “date of issue” and “date of next issue”.
E-commerce	The use of network technology (especially the internet) to buy or sell goods and services.
Employee	Any person employed by an agency or organization.

2018-06-11-identrust-glossary-of-terms-and-acronyms-en

Glossary of Terms and Acronyms

Encrypted Network	A network that is protected from outside access by NSA approved high-grade (Type I) cryptography. Examples are SIPRNET and TOP SECRET networks.
Encryption	The process of transforming text into an unintelligible form, in such a way that the original data either cannot be obtained, or can be obtained only by using a decryption process.
Encryption Certificate	A certificate containing a public key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes.
End Entity	Relying parties and subscribers.
Enrollment Work Station	An Enrollment Work Station is the customer side computer application that interfaces with the CMS to accomplish certificate registration.
Federal Bridge Certification Authority	The Federal Bridge Certification Authority consists of a collection of Public Key Infrastructure components (Certificate Authorities, Directories, Certificate Policies and Certificate Practice Statements) that are used to provide peer-to-peer interoperability among agency principal CA.
Federal Bridge Certification Authority Membrane	The Federal Bridge Certification Authority Membrane consists of a collection of Public Key Infrastructure components including a variety of Certification Authority PKI products, Databases, CA specific Directories, Border Directory, Firewalls, Routers, Randomizers, etc.
FBCA Operational Authority	The Federal Bridge Certification Authority Operational Authority is the organization selected by the Federal Public Key Infrastructure Policy Authority to be responsible for operating the Federal Bridge Certification Authority.
Federal Public Key Infrastructure Policy Authority	The Federal PKI Policy Authority is a federal government body responsible for setting, implementing and administering policy decisions regarding interagency PKI interoperability that uses the FBCA.
Federal Information Processing Standards	These are Federal standards that prescribe specific performance requirements, practices, formats, communications protocols, etc. for hardware, software, data, telecommunications operation, etc. Federal agencies are expected to apply these standards as specified unless a waiver has been granted in accordance to agency waiver procedures.
Firewall	Gateway that limits access between networks in accordance with local security policy.

2018-06-11 identrust-glossary-of-terms and acronyms-en

IdenTrust
part of HID Global

Glossary of Terms and Acronyms

Fully Qualified Domain Name	A domain name that includes the labels of all superior nodes in the internet Domain Name System.
GET Method	An OCSP request using the GET Method is a specifically constructed message requesting certificate status.
Government	The U.S. Federal Government and its authorized agencies and entities.
Government Agency	A government agency is an agency, unit, department, division or other subdivision of any governmental authority of any jurisdiction.
Group Address Certificate	A group address certificate is a group certificate that contains a health endpoint name in the certificate subject.
Group Address Encryption Certificate	A group address encryption certificate is a group address certificate that can be only used for encryption services.
Group Address Signing Certificate	A group address signing certificate is a group address certificate that can only be used to create a digital signature.
Group Certificate	A group certificate can be either a group domain-bound certificate or a group address end-entity certificate.
Group Domain-Bound Certificate	A group domain-bound certificate is a domain bound device certificate that contains a health domain name in the certificate subject. Group domain-bound certificates may be held by a third party that controls and manages access to the private key of the certificate.
Group Domain-Bound Encryption Certificate	A group domain-bound encryption certificate is a group domain-bound Device certificate that can be only used for encryption services.
Group Domain-Bound Signing Certificate	A group domain-bound signing certificate is a group domain-bound device certificate that can only be used to create a digital signature.
Health Domain Name	A health domain name is a string conforming to the requirements of RFC 1034 and identifies the organization that assigns the health endpoint names.
Health Endpoint Name	A health endpoint name is a string conforming to the local-part requirements of RFC 5322. Health endpoint names express real-world origination points and endpoints of health information exchange, as vouched for by the organization managing the health domain name.

2018-06-11-identrust-glossary-of-terms-and-acronyms-en

Glossary of Terms and Acronyms

Healthcare Entity	A healthcare entity is an entity involved in healthcare, that has agreed to protect private and confidential patient information consistent with the requirements of HIPAA although it is not a covered entity or business associate as defined under HIPAA at 45 CFR 160.103.
Health Information Service Provider	A Health Information Service Provider is an entity that processes Direct-compliant messages to and from Direct addresses, each of which is bound to a Direct-compliant X.509 digital certificate. Acting in the capacity of an agent for the subscriber, the HISP may hold and manage private keys associated with a DirectTrust certificate on behalf of the subscriber.
High Assurance Guard	An enclave boundary protection device that controls access between a local area network that an enterprise system has a requirement to protect, and an external network that is outside the control of the enterprise system, with a high degree of assurance.
High Risk FQDN List	A list of fully qualified domain names that have been identified through research during the verification and validation of the SSL application as being high subscriber risk.
ID Form	The ID Form a document incorporated into the Agreement and is a document that, among other things (a) is used by the applicant to provide personally identifying information as part of the certificate registration process, (b) must be signed by the applicant, and (c) contains a declaration of identity by the applicant.
Identification and Authentication	Identification and authentication is the process of affirming that a claimed identity is correct by comparing the claims offered by an applicant with previously proven information.
Identity Certificate	An identity certificate is a certificate issued to a subscriber that can be used to authenticate the subscriber by a relying party.
IdenTrust subjectID or IdenTrust SubjID	An IdenTrust SubjectID is included in the subjectDN field of certificates as an (ou) attribute and, for certificates where use includes authentication of the subject of the certificate, is also utilized as a User Principle Name (UPN) structure in the subjectAlternativeName extension of the certificate. The IdenTrust subjectID in any given certificate issued by the IdenTrust CA is to be unique among IdenTrust SubjectIDs operational within the PKI.
Individual	An Individual is a natural person and not a juridical person or legal entity.

2018-06-11-identrust-glossary-of-terms-and-acronyms-en

IdenTrust
part of HID Global

Glossary of Terms and Acronyms

Individual Accountability	The principle that requires individual users be held accountable for their actions through technical controls, which associate the identity of the user with the time, method, and degree of access to a system.
Information System Security Officer	Person responsible to the designated approving authority for ensuring the security of an information system throughout its lifecycle, from design through disposal.
Information Technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. Information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services, and related resources.
Inside Threat	An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.
Integrity	Protection against unauthorized modification or destruction of information. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.
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.
Interim Authority to Operate	When a system does not meet the requirements for accreditation, but the criticality of the system mandates that it become operational, temporary authority to operate may be granted. Interim authority to operate is contingent upon the implementation of proposed solutions and security actions according to an agreed upon schedule within a specified time period.
Intermediate CA	A CA that is subordinate to another CA, and has a CA subordinate to itself.
Issue/Issuance	To issue, or issuance is the act performed by a CA in creating a certificate, listing as issuer itself or, alternately, listing as issuer a name which the CA has obtained a license to use for such purpose. Issuance also involves notifying the applicant of certificate contents, that the certificate has been created and that the certificate is available for acceptance.

2018-06-11-identrust-glossary-of-terms-and-acronyms-en

Glossary of Terms and Acronyms

Issuer	An issuer is the organization that owns a CA private key used to digitally sign certificates and is named (or uses a name to which it owns or has licensed for such purpose) as the issuer in the issuer DN field in a certificate.
Identity Verification Provider	An identity verification provider is an organization that provides affirmation of identity and claims made by an applicant in support of I&A. Identity verification providers are considered authoritative and must able to demonstrate through policy and audit that the data is accurate and maintained with appropriate integrity, privacy and confidentiality.
Key	A key is a broad term encompassing all of the defined keys.
Key Changeover	The procedure used by an authority to replace its own private key (e.g., due to compromise) and replace current valid certificates issued with old key.
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, upon provisions set forth in the agreement.
Key Exchange	The process of exchanging public keys in order to establish secure communications.
Key Generation Material	Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.
Key Pair	Two mathematically related keys having the properties that (a) one key can be used to encrypt a message that can only be decrypted using the other key, and (b) even knowing one key, it is computationally infeasible to discover the other key.
Key Storage Module	A key storage module is secure software or a hardware cryptomodule used to store private keys and to perform private key operations such as digital signature generation. Key storage mechanism is used to refer to cryptomodules used by a subscriber in daily operations and is inclusive of software and hardware cryptomodules as well as different form factors such as smart cards or USB tokens.
Least Privilege	The principle that requires that each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks in order to limit the damage that can be caused by accident, error, or unauthorized use.

2018-06-11-identrust-glossary-of-terms-and-acronyms-en

Glossary of Terms and Acronyms

Legal Non-Repudiation	How well possession or control of the private signature key can be established. See Non-Repudiation.
Life Cycle	Stages through which an information system passes, typically characterized as initiation, development, operation, and termination.
Licensed Notary	A licensed notary is an individual commissioned by a government agency to perform notarial acts within that government's jurisdiction and whose commission remains in good standing. Licensed notaries may include but are not limited to consulate officers, court clerks and may include bank officers or other Individuals.
Lightweight Directory Access Protocol	Lightweight Directory Access Protocol is a protocol used by browsers and clients to look up information in directory services based on the x.500 standard.
Local Registration Authority	A Local Registration Authority is an Individual who collects and confirms applicant identity information and any other information provided by the applicant for inclusion in a certificate.
Machine Operator	A machine operator may be a primary machine operator or a secondary machine Operator.
Memorandum of Agreement	Agreement between the Federal PKI Policy Authority and an agency allowing interoperability between the agency principal CA and the FBCA.
Mission Support Information	Information that is important to the support of deployed and contingency forces.
Mutual Authentication	Occurs when parties at both ends of a communication activity authenticate each other (see authentication).
National Security System	Any telecommunications or information system operated by the United States Government, the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions, but does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

2018-06-11-identrust-glossary-of-terms-and-acronyms-en

IdenTrust
part of HID Global

Glossary of Terms and Acronyms

NIP Number	A National Provider Identifier or NPI is a unique 10-digit identification number issued to health care providers in the United States by the Centers for Medicare and Medicaid Services.
Non Declared Entity	A non-declared entity is an entity that has not asserted it will protect personal health information with privacy and security protections that are equivalent to those required by HIPAA and is not a patient/consumer.
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.
Object Identifier	An object identifier is a unique numeric identifier registered under the ISO registration standard to reference a specific object or object class. OIDs are used to uniquely identify the CP, certificate types, cryptographic algorithms, and other objects within the PKI.
Online Certificate Status Protocol	Online Certificate Status Protocol is an internet protocol described in RFC 2560 used to obtain revocation status of a certificate.
OCSP Request	An OCSP request is a message by a relying party to a CSA requesting the current status of a certificate via OCSP. An OCSP request includes but is not limited to the following data attributes: (a) date and time of the request; (b) requester identifier (c) certificate serial number; (d) issuer DN hash; and (e) issuer key hash.
OCSP Response / OCSP Responder	An OCSP response is the message sent by the CSA in response to an OCSP request, which indicates whether the status of the certificate in question is valid, revoked, or unknown. The OCSP response includes but is not limited to the following data attributes: (a) date and time of the response; (b) Certificate serial number; (c) issuer DN hash; (d) issuer key hash, (e) success or failure indication; and (f) digital signature of the OCSP.
Operational Period	An operation period is a certificate's actual term of validity, beginning with the start of the validity period and ending on the earlier of: (a) the end of the validity period disclosed in the certificate, or (b) the revocation of the certificate.
Organization	An organization is an entity legally recognized in its jurisdiction of origin, (e.g., a company, corporation, partnership, sole proprietorship, government agency, non-government organization, university, trust, special interest group, or non-profit corporation).

2018-06-11-identrust-glossary-of-terms-and-acronyms-en

Glossary of Terms and Acronyms

Out-of-Band	Communication between parties utilizing a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal Service mail to communicate with another party where current communication is occurring online).
Outside Threat	An unauthorized entity from outside the domain perimeter that has the potential to harm an Information System through destruction, disclosure, modification of data, and/or denial of service.
Participants	Participants include all entities operating within an OBB PKI.
Participant CA	A participant CA is a legal entity that is Issued a sub-CA certificate by a Root CA.
Physically Isolated Network	A network that is not connected to entities or systems outside a physically controlled space.
PKI Service Providers	PKI service providers are CAs, RAs, CSAs, and repositories providing services described in a CP.
PKI Sponsor	A natural person or PKI sponsor who is employed by the sponsoring organization or an authorized agent who has express authority to represent the organization but is not the subscriber for non-human system devices that are named as public key certificate subjects. The PKI sponsor is responsible for meeting the obligations of subscribers as defined throughout a CP.
Policy Approval Authority	A Policy Approval Authority is an organization or committee responsible for approval of CPs, CPSs, and other policy documents related to a PKI.
Policy Management Authority	Body established to oversee the creation and update of a CP, approve the corresponding CPS, review the results of CA audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate policies.
Policy Qualifier	An attribute within the CP descriptor that is included in a certificate profile and is used to provide additional information specific to the named CP and certificate policy OID.
Principal CA	The Principal CA is a CA designated by an agency to interoperate with the FBCA. An agency may designate multiple principal CAs to interoperate with the FBCA.
Privacy	Restricting access to subscriber or relying party information in accordance with federal law and agency policy.

2018-06-11-identrust-glossary-of-terms-and-acronyms-en

Glossary of Terms and Acronyms

Privacy Practices and Procedures	A written statement describing policies and procedures for the protection of individual information to which requirements of confidentiality apply.
Private Key	(1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.
Public Key	(1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is made publicly available normally in the form of a digital certificate.
Public Key Cryptography	Public Key Cryptography is a type of cryptography also known as asymmetric cryptography that uses mathematical algorithms and unique key pairs of mathematically related numbers. The public key can be made available to anyone who wishes to use it, while the private key is kept secret by its holder. Private keys can be used to decrypt information or generate a digital signature; the corresponding public key is used to encrypt that information or verify that digital signature. In addition, the public key cannot be used to derive the private key without a large work factor.
Public Key Infrastructure	A set of 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, and revoke public key certificates.
Reasonable Reliance	Reliance on a certificate is considered reasonable reliance when a relying party has: • Agreed to be bound by the terms and conditions of a CP and CPS; • Verified the digital signature and certificate were valid at the time of reliance by using OCSP and the certification path validation process as required by a CP and CPS; and • Used the certificate for purposes appropriate under the CA'S CPS, without knowledge of any facts that would cause a person of ordinary business prudence to refrain from relying on the certificate, and under circumstances where reliance would be reasonable and otherwise in good faith in light of all the circumstances that were known or should have been known to the relying party prior to reliance.

2018-06-11 identrust-glossary-of-terms and acronyms-en

Glossary of Terms and Acronyms

Registration	Registration is the process of receiving or obtaining a request for a certificate from an applicant, and collecting and entering the information needed from that applicant to include in and support I&A and the issuance of a certificate.
Registration Agent	A registration agent is an Individual appointed directly by a CA or RA. A registration agent may also be an LRA or Trusted Agent appointed by a CA or RA or may also be a licensed notary or other official of a government agency. A registration agent assists CAs and RAs by providing in-person I&A.
Registration Authority	A Registration Authority is an organization that is responsible for collecting and confirming an applicant's identity and any other information provided by applicant for inclusion in a certificate.
Registration Authority Agreement	A Registration Authority agreement is an agreement entered into between an organization and a CA authorizing the organization to act as a Registration Authority for the CA, and detailing the specific duties and obligations of the RA, including but not limited to the procedures for conducting appropriate I&A on applicants.
Registration Practices Statement	The Registration Practices Statement describes the registration practices of an external RA in performance of duties and obligations to fulfill the requirements of a CP.
Re-key (a certificate)	Re-keying a certificate consists of creating new certificate with a different public key (and serial number) while retaining the remaining contents of the old certificate that describe the subject. The new certificate may be assigned a different validity period, key identifiers, specify a different CRL distribution point, and/or be signed with a different key. Re-key of a certificate does not require a change to the subject name and does not violate the requirement for name uniqueness.
Relying Party	A relying party is an organization, subscriber, device or any entity that relies upon the information contained within a certificate and upon certificate status received from a CSA.
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.
Repository	A repository is an online system maintained by or on behalf of a CA for storing and retrieving certificates and other information relevant to

2018-06-11-identrust-glossary-of-terms-and-acronyms-en

Glossary of Terms and Acronyms

	certificates and digital signatures, including CPs, CPSs and information relating to certificate validity or revocation.
Requestor	A requestor is an authorized agent of an organization who invites an individual to apply for an affiliated certificate.
Responsible Individual	A trustworthy person designated by a sponsoring organization to authenticate individual applicants seeking certificates on the basis of their affiliation with the sponsor.
Revoke a Certificate	Revocation is the act of making a certificate permanently ineffective from a specified time forward. Revocation is effected by notation or inclusion in a set of revoked certificates (e.g., inclusion in a CRL).
Risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
Risk Management	The total process of identifying, controlling, and eliminating, or minimizing certain events that may affect system resources. It includes risk analysis, cost benefit analysis, selection, implementation, and test, security evaluation of safeguards, and overall security review.
Risk Tolerance	The level of risk an entity is willing to assume in order to achieve a potential desired result.
Root CA	In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.
Root Certificate	A root certificate, also known as a trust anchor, is a CA certificate Issued by a CA at the top of a hierarchical PKI.
Router	A special-purpose computer (or software package) that handles the connection between two or more networks. Routers spend all their time looking at the destination addresses of the packets passing through them and deciding on which route to send them.
Rules of Behavior	Rules that have been established and implemented concerning the use of, security in, and acceptable level of risk for the system.
Secondary Machine Operators List	The secondary machine operators list is a list of individuals who are designated by a primary machine operator to act in the role of secondary machine operator.

Glossary of Terms and Acronyms

Secret Key	A "shared secret" used in symmetric cryptography, wherein users are authenticated based on a password, Personal Identification Number (PIN), or other information shared between the user and the remote host or server. A single key is shared between two parties: the sender, to encrypt a transmission, and the recipient, to decrypt the transmission.
Sensitivity	The level of protection that information requires. An information technology environment consists of the system, data, and applications, which must be examined individually and in total. All systems and applications require some level of protection for confidentiality, integrity, and availability, which is determined by an evaluation of the sensitivity and criticality of the information processed, the relationship of the system to the organization's mission, and the economic value of the system components.
Separation of Duties/ Multi-party Control	Separation-of-duties or multi-party control are procedures or techniques whereby no single Individual possesses the equipment or authorization to view, alter, or otherwise have access to sensitive or confidential information in a particular PKI. Tasks are separated into multiple subtasks and distributed to more than one individual, requiring the participation of two or more individuals to complete the task. The purpose of separation-of-duties and multi-party control is to reduce risk of PKI compromise.
Server-Authenticated SSL/TLS-Encrypted Session	Server-authenticated SSL/TLS-encrypted sessions as discussed in the CP are those sessions in which a subscriber or client is directed to a specified secure URL (https://). The SSL-enabled client software confirms the identity of a secure server by validating the certificate presented by the server. The subsequent session established is encrypted through use of the Secure Sockets Layer and Transport Layer Security cryptographic protocols.
Server	A system entity that provides a service in response to requests from clients.
Signature Certificate	A public key certificate that contains a public key intended for verifying digital signatures (rather than encrypting data or performing any other cryptographic functions).
Signing Certificate	A signing certificate is a certificate issued to a subscriber that can be used to create digital signatures to establish the integrity of content.
Sponsor Antecedent	A sponsor antecedent is an organization that attests to the validity of an applicant through their on-going relationship, date of antecedent event and provides unique applicant identity information to the Registration Agent.

2018-06-11-identrust-glossary-of-terms-and-acronyms-en

Glossary of Terms and Acronyms

Sponsor	A sponsor is an organization that authorizes issuance of a certificate to an individual or a device. (e.g., an employee's supervisor who authorizes the issuance of a certificate to the employee, or the head if an information systems department that authorizes issuance of a device certificate to an SSL server). The sponsor is responsible for either supplying or confirming certificate attribute details to the CA or RA; and is also responsible for informing the CA or RA if the relationship with the subscriber or device is terminated or has changed such that the certificate should be revoked or updated.
SSL / TLS Certificate	A SSL / TLS certificate is a certificate issued to a device that is utilized to establish an encrypted session between a client and a server.
Subject Information Access	An extension in a certificate that indicates how to access information and services for the subject of the certificate in which the extension appears. When the subject is a CA, information and services may include certificate validation services and CA policy data. When the subject is an end entity, the information describes the type of services offered and how to access them.
Subordinate CA	In a hierarchical PKI, a CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA. (See superior CA).
Subscriber Agreement	The subscriber agreement is a legally binding contract that provides terms and conditions applicable to a certificate that is applied for by an applicant and, if issued, is issued to that applicant as the subscriber of that certificate.
Subscriber	A subscriber is an end-entity individual or device to whom or to which a certificate is Issued. Subscribers may use certificates for purposes indicated by the certificate type.
Subscribing Organization Authorization Agreement	The Subscribing Organization Authorization Agreement is completed by and submitted in conjunction with registration for some types of certificates.
Subscribing Organization	A subscribing organization is an organization that authorizes affiliation with subscribers.
Superior CA	In a hierarchical PKI, a CA who has certified the certificate signature key of another CA, and who constrains the activities of that CA. (See subordinate CA).

2018-06-11-identrust-glossary-of-terms-and-acronyms-en

Glossary of Terms and Acronyms

Suspend (a certificate)	Suspension is the act of making a certificate ineffective temporarily from a specified time forward. Suspension is affected by notation or inclusion in a set of suspended certificates (e.g., inclusion in a CRL).
Symmetric Key	A key that can be used to encrypt and decrypt the same data.
System Equipment Configuration	A comprehensive accounting of all system hardware and software types and settings.
System High	The highest security level supported by an information system.
System Security Plan	Documentation of the management, technical, and operational security controls of an automated information system.
System Transaction	The successful execution of all of the following components and steps; a) creation of a digital signature; b) verification that the subscriber's digital signature was created by the private key corresponding to the public key in the certificate; and c) verification that the certificate was validated.
Technical non-repudiation	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 private signature key.
Threat	Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service.
Token	Object that a user possesses for the purpose of I&A. Tokens are generally characterized as USB tokens. USB tokens are typically secured through the use of a PIN or password.
Trust List	Collection of trusted certificates used by relying parties to authenticate other certificates.
Trusted Agent	A Trusted Agent is an individual who acts on behalf of the CA, RA, or LRA to collect and/or confirm information regarding applicants and/or subscribers, and where applicable to provide support regarding those activities to the applicants and/or subscribers.
Trusted Certificate	A certificate that is trusted by the relying party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a "trust anchor".

2018-06-11-identrust-glossary-of-terms-and-acronyms-en

Glossary of Terms and Acronyms

Trusted Role	A trusted role is a role involving functions that may introduce security problems if not carried out properly, whether accidentally or maliciously. The functions of trusted roles form the basis of trust for the entire PKI.
Trusted Timestamp	A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.
Trustworthy System	Computer hardware, software and procedures that: (a) are reasonably secure from intrusion and misuse; (b) provide a reasonable level of availability, reliability, and correct operation; (c) are reasonably suited to performing their intended functions; and (d) adhere to generally accepted security procedures.
Two-Person Control	Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and/or unauthorized procedures with respect to the task being performed and each familiar with established security and safety requirements.
Update (a certificate)	The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate.
User Principal Name	A User Principal Name is an attribute used in PKI, the format of such attribute being an Internet-style login name for a user based on an Internet standard.
Valid Certificate	A certificate that (a) an authorized CA has issued, (b) the subscriber listed in it has accepted, (c) has not expired, and (d) has not been revoked. Thus, a certificate is not "valid" until it is both issued by an authorized CA and has been accepted by the subscriber.
Validity Period	Validity period is the intended term of validity of a certificate, beginning with the "notBefore" date asserted in the certificate and ending with the "notAfter" date asserted in the certificate.
Vulnerability Assessment	An analysis of flaws or weaknesses in security procedures, technical controls, physical controls or other controls that may allow harm to occur to an automated information system.
Zeroize	A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data.

Acronyms and Abbreviations

2018-06-11-identrust-glossary-of-terms-and-acronyms-en

IdenTrust
part of HID Global

Glossary of Terms and Acronyms

AIA	Authority Information Access
AIS	Automated Information System
ASN.1	Abstract Syntax Notation (version 1)
CA	Certification Authority
CARL	Certificate Authority Revocation List
CHUID	Card Holder Unique Identifier
CIAO	Critical Infrastructure Assurance Office
CIS	Certificate Information System
CM	Configuration Management
CMA	Certificate Manufacturing Authority
CMS	Card Management System
CMS	Centers for Medicare and Medicaid Services
COMSEC	Communications Security
COOP	Continuity of Operations Plan
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSA	Certificate Status Authority
CSS	Certificate Status Server
CSOR	Computer Security Object Registry
DCID	Director of Central Intelligence Directive
DES	Data Encryption Standard
DITSCAP	Dept of Defense Information Technology Security Certification and Accreditation Process
DN	Distinguished Name
DNS	Domain Name System
DOD	Department of Defense

2018-06-11-identrust-glossary-of-terms-and-acronyms-en

IdenTrust
part of HID Global

Glossary of Terms and Acronyms

DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
EAL	Evaluation Assurance Level
ECA	External Certificate Authority (certificate program)
ECDSA	Elliptic Curve Digital Signature Algorithm
EO	Executive Order
ERC	Enhanced Reliability Check
EWS	Enrollment Work Station
FASC-N	Federal Agency Smart Credential Number
FAR	Federal Acquisition Regulations
FBCA	Federal Bridge Certification Authority
FedCIRC	Federal Computer Incident Response Capability
FED-STD	Federal Standard
FIPS	Federal Information Processing Standards
FIPS PUB	Federal Information Processing Standard Publication (US)
FISCAM	Federal Information System Controls Audit Manual
FPKI	Federal Public Key Infrastructure
FPKIMA	Federal PKI Management Authority
FPKI-Prof	Federal PKI X.509 Certificate and CRL Extensions Profile
FPKIPA	Federal PKI Policy Authority
FQDN	Fully Qualified Domain Name
GAO	General Accounting Office (U.S.)
GPEA	Government Paperwork Elimination Act of 1998
HAG	High Assurance Guard
HE	Healthcare Entity
HIPAA	HIPAA is the federal Health Insurance Portability and Accountability Act of 1996.

2018-06-11 identrust-glossary-of-terms and acronyms-en

IdenTrust
part of HID Global

Glossary of Terms and Acronyms

HISP	Health Information Service Provider
I & A	Identification and Authentication
IATO	Interim Authority to Operate
IAW	In Accordance With
IETF	Internet Engineering Task Force
IGC	IdenTrust Global Common (certificate program)
IGC PIV-I	IdenTrust Global Common – Personal Identity Verification Interoperable
IS	Information System
ISO	International Organization for Standardization
ISSM	Information System Security Manager
ISSO	Information Systems Security Officer
IT	Information Technology
ITU	International Telecommunications Union
ITU-T	International Telecommunications Union – Telecommunications Sector
ITU-TSS	International Telecommunications Union – Telecommunications System Sector
IVP	Identity Verification Provider
KSM	Key Storage Module
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LRA	Local Registration Authority
MOA	Memorandum of Agreement
NAC	National Agency Check
NACIC	National Agency Check with Inquiries Credit
ND	Non-Declared Entity
NIACAP	National Information Assurance Certification and Accreditation Process
NIST	National Institute of Standards and Technology

2018-06-11 identrust-glossary-of-terms-and-acronyms-en

Glossary of Terms and Acronyms

NPI	National Provider Identifier
NSA	National Security Agency
NSTISSC	National Security Telecommunications and Information Systems Security Committee
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OMB	(US) Office of Management and Budget
OOB	Out-of-Band
OPM	(US) Office of Personnel Management
OTC	One Time Code
PAA	Policy Approval Authority
PCCIP	President's Commission on Critical Infrastructure Protection
PDD	Presidential Decision Directive
PIN	Personal Identification Number
PIV	Personal Identity Verification
PIV-I	Personal Identity Verification – Interoperable
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
PMA	Policy Management Authority
PPP	Privacy Practices and Procedures
RA	Registration Authority
RFC	Request For Comments
RPS	Registration Practices Statement
RSA	Rivest-Shamir-Adleman (encryption algorithm)
SBU	Sensitive But Unclassified

2018-06-11 identrust-glossary-of-terms and acronyms-en

Glossary of Terms and Acronyms

SHA-1	Secure Hash Algorithm, Version 1
SHS	Secure Hash Standard
SIA	Subject Information Access
S/MIME	Secure Multipurpose Internet Mail Extension
SO	System Owner
SPM	Security Program Manager
SSL/TLS	Secure Sockets Layer AND Transport Layer Security
SSP	System Security Plan
TA	Trusted Agent
TAISS	Telecommunications and Automated Information Systems Security
TrustID	TrustID (certificate program)
TSDM	Trusted Software Development Methodology
UPN	User Principal Name
UPS	Uninterrupted Power Supply
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
U.S.C.	United States Code
UUI	Universally Unique Identifier
WAN	Wide Area Network
WWW 88	World Wide Web
X.500	The ITU-T (International Telecommunication Union-T) standard that establishes a distributed, hierarchical directory protocol organized by country, region, organization, etc.
X.509, v.3	The ITU-T ("International Telecommunication Union-T") standard for certificates adopted as ISO/IEC 9594-8 (2001). X.509, version 3, refers to certificates containing or capable of containing extensions.
XKMS	XML Key Management Specification
XSMS	XML Subscriber Management Specification

IdenTrust
part of HID Global

Glossary of Terms and Acronyms

2018-06-11 identrust-glossary-of-terms and acronyms-en