# NSTIC National Program Office Discussion Draft
## TERMINOLOGY REPORT

# Contents



# Introduction

This document is a contribution from the NSTIC National Program Office to the Identity Ecosystem Steering Group. The document contains a list of terms and definitions obtained from review of standards, guidelines, policies, profiles and frameworks.

This is a work of research only. Selection of particular documents as sources of terminology does not reflect endorsement of those documents by the NSTIC National Program Office, likewise exclusion of documents as sources does not reflect non-endorsement.

# TERMS AND DEFINITIONS

## Terms Index

Name (1), Garbled (1), General Services Administration (1), Generate Key (1), Governance (1), Grant (of Rights Ofuse) (1), Grant Category (1), Grantee (1), Guessing Entropy (1), Guide (1), Handle (1), Handle Service (1), Handle Service Subject DN (1), Handle Service URL (1), Hardening (1), Hardware (1), Hash Function (2), Hash Value (1), Hash-based Message Authentication Code (1), High Assurance Guard (1), Higher Education Institution (1), Holder-of-key Assertion (3), Homeland Security Presidential Directive (1), Host (1), Human Resources (1), Hypertext Transfer Protocol (1), INCOMMON BRONZE IDENTITY ASSURANCE PROFILE (1), INCOMMON SILVER IDENTITY ASSURANCE PROFILE (1), Identification (3), Identifier (6), Identifying Information (1), Identity (7), Identity Assurance Assessment Framework (1), Identity Assurance Framework (1), Identity Assurance Profile (1), Identity Assurance Qualifier (1), Identity Assurance Work Group (1), Identity Attributes (1), Identity Authentication (1), Identity Binding (1), Identity Credential (1), Identity Database (1), Identity Defederation (1), Identity Ecosystem (1), Identity Ecosystem Framework (1), Identity Federation (1), Identity Management (1), Identity Management System (2), Identity Medium (1), Identity Proofing (4), Identity Proofing Policy (1), Identity Proofing Practice Statement (1), Identity Proofing Service Provider (1), Identity Provider (7), Identity Provider Security Token Service (1), Identity Registration (1), Identity Selector (1), Identity Verification (1), Identity, Credential, And Access Management (1), Identity, Credential, And Access Management Sub Committee (1), Idms Database (1), Idms Operations (1), Idp Operator (1), Immediately (1), Incommon CA Root Profile (1), Incommon Federation (1), Incommon Technical Advisory Committee (1), Indirect Assertion Model (1), Individual (1), Information Card (1), Information Card Model (1), Information Security And Identity Management Committee (1), Information Security Management Systems (ISMS) (1), Information System Security Officer (1), Information Technology (1), Initial SOAP Sender (1), Initialization Vector (1), Input Data (1), Inqueue (1), Inside Threat (1), Integrity (5), Intellectual Property (2), Interface (1), Interface Device (2), Intermediate CA (1), International Standard (2), Interoperability (2), Interoperability Test (1), Issuance (1), Issuer (3), Issuing Certification Authority (issuing CA) (1), Kantara Initiative Board Of Trustees (1), Kantara Initiative Mark (1), Kantara Trust Status List (1), Kantara-accredited Service (1), Kantara-approved Assessor (1), Kerberos (1), Key (1), Key Agreement (1), Key Confirmation (1), Key Encrypting Key (1), Key Entry (1), Key Escrow (2), Key Establishment (2), Key Exchange (1), Key Generation Material (1), Key Label (1), Key Life Cycle State (1), Key Loader (1), Key Management (1), Key Output (1), Key Owner (1), Key Pair (1), Key Reference (3), Key Split (1), Key State Transition (1), Key Transport (2), Key Update (1), Key Wrapping (1), Knowledge Based Authentication (1), LDAP Directory (1), Least Privilege (1), Level Of Assurance (1), Liberty Alliance (1), Lightweight Directory Access Protocol (1), Lightweight Directory Inter-exchange Format (1), Local Registration (1), Local Registration Authority (LRA) (1), Locale Identifier (1), Locally Unique Identifier (1), Login, Logon, Sign-on (1), Logout, Logoff, Sign-off (1), MSCUID (1), Malware (1), Man-in-the-middle Attack (1), Mandatory Element (1), Manual Key Entry (1), Manual Key Transport (1), Markup Language (1), Match (1), Matching (1), Memorandum Of Agreement (1), Message Authentication Code (1), Metadata (4), Metadata Authority (1), Metadata Element (1), Microcode (1), Min-entropy (2), Mission Support Information (1), Mode Of Operation (1), Model (1), Multi-factor (1), Multi-factor Authentication (1), Multi-token Authentication (1), Mutual Authentication (1), Name Qualifier (1), Namespace (2), Naming Authority (1), National Institute Of Standards And Technology (1), National Security System (1), Netid (1), Network (4), Non-person Entity (1), Non-repudiation (3), Nonce (2), Normative Element (1), OP Endpoint URL (1), OP Identifier (1), Object Identifier (4), Off-card (1), Off-line Attack (1), Office Of Governmentwide Policy (1), Office Of Management And Budget (1), Office Of Management And Budget (US Federal Government) (1), Offline Test (1), On-card (1), On-card Comparison (1), Online Attack (1), Online Certificate Status Protocol (1), Online Guessing Attack (1), Op-local Identifier (1), Openid Provider (1), Operational Test (1), Operator (1), Organization (1), Out Of Band (1), Out-of-band (2), Output Data (1), Outside Threat (1), PIV Assurance Level (1), PIV Key Type (1), PKI Disclosure Statement (1), PKI Sponsor (1), PKI-PIV Authentication Key (1), Parameters (1), Participant (2), Participant Agreement (1), Participant Operating Practices (1), Participants (1), Party (1), Passive Attack (1), Password (3), Path Validation (1), Permission (1), Persistent (1), Persistent Pseudonym (1), Person (1), Personal Identification Number (3), Personal Identifying Information (1), Personal Identity Verification Card (2), Personally Identifiable Information (2), Pharming (1), Phishing (1), Physical Protection (1), Physically Isolated Network (1), Pki-card Authentication Key (1), Plaintext Key (1), Policy Decision Point (1), Policy Enforcement Point (1), Policy Management Authority (1), Policy Qualifier (1), Port (1), Possession And Control Of A Token (1), Practice Statement (2), Pre-activation State (1), Preliminary Informative Element (1), Principal (1), Principal CA (2), Principal Identity (1), Privacy (3), Privacy Impact Assessment (1), Privacy Policy (1), Private Credentials (1), Private Key (4), Profile (2), Proof Of Possession Protocol (1), Proof-of-possession (1), Protected Channel (1), Protected Resource (3), Protected Session (2), Protection Profile (1), Provider (1), Proxy (1), Proxy Server (1), Pseudonym (2), Pseudonymous Identifier (1), Pseudonyms (1), Public Credentials (1), Public Key (5), Public Key (asymmetric) Cryptographic Algorithm (1), Public Key Certificate (3), Public Key Cryptography (1), Public Key Infrastructure (6), Publicly Available Specification (1), Pull (1), Push (1), Qubit (1), Random Number Generator (1), Re-key (a Certificate) (2), Recommendation (2), Recover (key/metadata) (1), Reference Data (2), Refresh Token (1), Registration (5), Registration Authority (5), Rekey (1), Relationship Identifier (1), Relying Parties (1), Relying Party (13), Relying Party Agent (1), Relying Party Agreement (1), Relying Party Security Token Service (1), Remote (1), Removable Cover (1), Renew (a Certificate) (2), Renewal (1), Replay Attack (1), Repository (2), Requester (1), Requester, SAML Requester (1), Requesting Party (1), Requirement (1), Resource (1), Resource Descriptor URL (1), Resource Owner (2), Resource Provider (1), Resource Server (1), Resource Set (1), Responder, SAML Responder (1), Responsible Individual (1), Restful (1), Revoke (a Certificate) (1), Revoke A Certificate (1), Revoked State (1), Risk (2), Risk Assessment (1), Risk Tolerance (1), Role (3), Root CA (1), Rootkit (1), Router (1), SAML Artifact (1), SAML Authentication Assertion (1), SAML Authority (1), Salt (2), Scalability (1), Scenario Test (1), Scheme (1), Scope (1), Secondary Authenticator (1), Secret Key (1), Secret Key (symmetric) Cryptographic Algorithm (1), Sector (1), Secure Sockets Layer (1), Security (2), Security Architecture (1), Security Assertion (1), Security Assertion Markup Language (4), Security Context (1), Security Domain (3), Security Policy (3), Security Policy Expression (1), Security Service (1), Security Strength (1), Security Token (1), Security Token Service (2), Seed Key (1), Semantics (1), Sensitive Information (1), Server (3), Service (1), Service Assessment Criteria (1), Service Provider (3), Service Provisioning Markup Language (1), Service Requester (1), Session Authority (1), Session Hijack Attack (1), Session Participant (1), Set Of Provisions (1), Shared BAE Broker (1), Shared Secret (2), Shibboleth (1), Signatory (1), Signature (1), Signature Certificate (2), Signature

Verification (1), Signed Security Token (1), Simple Object Access Protocol (1), Simple Power Analysis (1), Single Sign-on (1), Site (1), Social Engineering (1), Software (2), Special Publication (1), Specified Service (1), Split Knowledge (1), Sponsored Partner (1), Standard (2), State Of The Art (1), Statement (1), Status Information (1), Status Word (3), Steering Group (1), Store (key/metadata) (1), Strong Man In The Middle Resistance (1), Strongly Bound Credentials (2), Student Information System (1), Subject (4), Subject Certification Authority (subject CA) (1), Subordinate CA (2), Subscriber (6), Subscriber Agreement (1), Superior CA (2), Supplementary Informative Element (1), Support Contact (1), Suspended State (1), Symmetric Key (2), Syntax (1), Synthetic Identifier (1), System (1), System And Communications Protection (1), System Entity, Entity (1), System Equipment Configuration (1), System High (1), System Software (1), TEMPEST (1), TOE Security Functions (1), TOE Security Policy (1), Tamper Detection (1), Tamper Evidence (1), Tamper Response (1), Target Of Evaluation (1), Technical Contact (1), Technical Non-repudiation (1), Technical Report (1), Technical Specification (1), Template (2), Template Generator (1), Template Matcher (1), Threat (4), Time-out (1), Token (5), Token Authenticator (2), Token Endpoint (1), Token Secret (1), Transient Pseudonym (1), Transport Layer Security (1), Trust (1), Trust Anchor (3), Trust Anchor Store (1), Trust Criteria (1), Trust Framework (2), Trust Framework Adoption Process (1), Trust Framework Provider (1), Trust Framework Provider Adoption Process (1), Trust Identity (1), Trust List (1), Trusted Agent (1), Trusted Association (1), Trusted Certificate (1), Trusted Channel (1), Trusted Path (1), Trusted Timestamp (1), Trustmark (1), Trustmark Scheme (1), Trustworthy System (1), Two-person Control (1), URI Reference (1), Ultimate SOAP Receiver (1), Uniform Resource Identifier (2), Uniform Resource Locator (1), Uniform Resource Name (1), Unlinkability (1), Unobservability (1), Unsigned Security Token (1), Unverified Name (1), Update (a Certificate) (2), User (3), User Agent (1), User-agent (1), User-supplied Identifier (1), Valid (1), Validate (1), Validation (3), Validation Authorities (1), Validity Period (1), Verification (2), Verified Name (1), Verifier (3), Verifier Impersonation Attack (1), Weak Man In The Middle Resistance (1), Weakly Bound Credentials (2), Website (1), Where Are You From (1), XML Attribute (1), XML Element (1), XML Namespace (1), XML Schema (1), Yadis Document (1), Yadis ID (1), Yadis Resource (1), Yadis Resource Descriptor (1), Yadis Service (1), Yadis URL (1), Yadis User (1), Yadis User Agent (1), Zero-knowledge Password Protocol (1), Zeroization (1), Zeroize (3),

# Definitions of Terms

**Access**
Ability to make use of any information system (IS) resource. [NS4009] [FBCA CP 2.25]

Ability to make use of any information system (IS) resource. [SAFE-BioPharma CP 2.5]

To interact with a system entity in order to manipulate, use, gain knowledge of, and/or obtain a representation of some or all of a system entity's resources. [RFC2828] [OASIS SAML Glossary 2.0]

**Access Control**
Process of granting access to information system resources only to authorized users, programs, processes, or other systems. [NS4009] [FBCA CP 2.25]

The process of granting or denying specific requests: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities (e.g., Federal buildings, military establishments, border crossing entrances). [NIST FIPS 201-2]

Protection of resources against unauthorized access; a process by which use of resources is regulated according to a security policy and is permitted by only authorized system entities according to that policy. [RFC2828] [OASIS SAML Glossary 2.0]

**Access Control Information**
Any information used for access control purposes, including contextual information [X.812]. Contextual information might include source IP address, encryption strength, the type of operation being requested, time of day, etc. Portions of access control information may be specific to a request itself, some may be associated with the connection via which a request is transmitted, and others (for example, time of day) may be "environmental". [RFC2829] [OASIS SAML Glossary 2.0]

**Access Management System**
The collection of systems and services associated with specific on-line resources or services that together decide whether to grant a given individual access to those resources or services. [InCommon Glossary]

**Access Rights**
A description of the type of authorized interactions a subject can have with a resource. Examples include read, write, execute, add, modify, and delete. [Taxonomy] [OASIS SAML Glossary 2.0]

**Access Token**
Access tokens are credentials used to access protected resources. An access token is a string representing an authorization issued to the client. The string is usually opaque to the client. Tokens represent specific scopes and durations of access, granted by the resource owner, and enforced by the resource server and authorization server. The token may denote an identifier used to retrieve the authorization information, or self-contain the authorization information in a verifiable manner (i.e. a token string consisting of some data and a signature). Additional authentication credentials, which are beyond the scope of this specification, may be required in order for the client to use a token. The access token provides an abstraction layer, replacing different authorization constructs (e.g. username and password) with a single token understood by the resource server. This abstraction enables issuing access tokens more restrictive than the authorization grant used to obtain them, as well as removing the resource server's need to understand a wide range of authentication methods. Access tokens can have different formats, structures, and methods of utilization (e.g. cryptographic properties) based on the resource server security requirements. Access token attributes and the methods used to access protected resources are beyond the scope of this specification and are defined by companion specifications. [IETF ID OAuth 2.0]

**Account**
An account is used to associate transactional records with an end user or organization. Presence of an account does not necessarily mean that there are credentials (e.g., username and password) associated with the account. [ICAM SAML 2.0 WB SSO Profile 1.0.2]

Typically a formal business agreement for providing regular dealings and services between a principal and business service providers. [OASIS SAML Glossary 2.0]

**Account Linkage**
A method of relating accounts at two different providers that represent the same principal so that the providers can communicate about the principal. Account linkage can be established through the sharing of attributes or through identity federation. [OASIS SAML Glossary 2.0]

**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. [NS4009] [FBCA CP 2.25]

The process used to achieve formal recognition that an organization has agreed to the operating rules defined in the AAS (Assurance Assessment Scheme) and is competent to perform assessments using the Service Assessment Criteria. [Kantara IAF 1100]

**Accreditation Applicant**
An Audit Organization applying to Kantara Initiative for accreditation under the AAS. [Kantara IAF 1100]

**Accreditation Authority**
[entity that] assesses and validates identity providers, attribute providers, relying parties, and identity media, ensuring that they all adhere to an agreed-upon trust framework. Accreditation authorities can issue trustmarks to the participants that they validate. [NSTIC Strategy]

**Activation Data**
Private data, other than keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or decryption events). [FBCA CP 2.25]

Data values, other than keys, that are required to operate cryptographic modules and that need to be protected (e.g., a PIN, a passphrase, or a manually-held key share). [IETF RFC 3647]

Private data, other than keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or decryption events). [SAFE-BioPharma CP 2.5]

**Active Attack**
An attack on the authentication protocol where the Attacker transmits data to the Claimant, Credential Service Provider, Verifier, or Relying Party. Examples of active attacks include man-in-the-middle, impersonation, and session hijacking. [NIST SP 800-63-1]

**Active Role**
A role that a system entity has donned when performing some operation, for example accessing a resource. [OASIS SAML Glossary 2.0]

**Active State**
The key life cycle state in which a cryptographic key is available for use for a set of applications, algorithms, and security entities. [NIST SP 800-130]

**Address Of Record**
The official location where an individual can be found. The address of record always includes the residential street address of an individual and may also include the mailing address of the individual. In very limited circumstances, an Army Post Office box number, Fleet Post Office box number or the street address of next of kin or of another contact individual can be used when a residential street address for the individual is not available. [NIST SP 800-63-1]

A means of contacting the Subject. [InCommon IAAF 1.1]

**Administrative Domain**
An environment or context that is defined by some combination of one or more administrative policies, Internet Domain Name registrations, civil legal entities (for example, individuals, corporations, or other formally organized entities), plus a collection of hosts, network devices and the interconnecting networks (and possibly other traits), plus (often various) network services and applications running upon them. An administrative domain may contain or define one or more security domains. An administrative domain may encompass a single site or multiple sites. The traits defining an administrative domain may, and in many cases will, evolve over time. Administrative domains may interact and enter into agreements for providing and/or consuming services across administrative domain boundaries. [OASIS SAML Glossary 2.0]

**Administrator**
A person who installs or maintains a system (for example, a SAML-based security system) or who uses it to manage system entities, users, and/or content (as opposed to application purposes; see also End User). An administrator is typically affiliated with a particular administrative domain and may be affiliated with more than one administrative domain. [OASIS SAML Glossary 2.0]

**Adopted Authentication Scheme**
An open identity management standard that the ICAM assesses, approves, and scopes for government-wide use. An adopted scheme meets all applicable ICAM requirements, as well as other Federal statutes, regulations, and policies. In addition, the structured adoption process provides assurance to all ICAM participants that underlying identity assurance technologies are appropriate, robust, reliable, and secure. [FICAM TFPAP 1.0.1]

**Adopted Scheme**
(undefined) [FICAM TFPAP 1.0.1]

**Adoption**
Acceptance of a 3rd party Trust Framework by the Federal government after rigorous review and determination of comparability at a specified Level of Assurance. [FICAM TFPAP 1.0.1]

**Affiliate PKI**
An approved Applicant or Applicant Bridge PKI that has successfully completed all steps required to become cross-certified and has been issued a cross-certificate by the FBCA (or one of the other FPKI Trust Infrastructure CAs). [FBCA Cross-certification Methodology 3.0]

**Affiliated Organization**
Organizations that authorize affiliation with Subscribers of PIV-I certificates. [FBCA CP 2.25]

**Affiliation**
A set of system entities that share a single namespace (in thefederated sense) of identifiers for principals. Anonymity The quality or state of being anonymous, which is the condition of having a name or identity that is unknown or concealed. [RFC2828] [OASIS SAML Glossary 2.0]

**Agent**
A computer software process (or system of processes) acting on behalf of a party. [Yadis 1.0]

**Algorithm Identifier**
PIV algorithm identifier is a one-byte identifier that specifies a cryptographic algorithm and key size. For symmetric cryptographic operations, the algorithm identifier also specifies a mode of operation (ECB). [NIST SP 800-73-3 Part 1]

A PIV algorithm identifier is a one-byte identifier that specifies a cryptographic algorithm and key size. For symmetric cryptographic operations, the algorithm identifier also specifies a mode of oeration (i.e., ECB). [NIST SP 800-73-3 Part 2]

A PIV algorithm identifier is a one-byte identifier that specifies a cryptographic algorithm and key size. For symmetric cryptographic operations, the algorithm identifier also specifies a mode of oeration (i.e., ECB). [NIST SP 800-73-3 Part 3]

**Algorithm Transition**
The processes and procedures used to replace one cryptographic algorithm with another. Anonymity Assurance that public data cannot be associated with the owner in CKMS supported communications. [NIST SP 800-130]

**Annual Conformity Review**
Review undertaken annually by the ARB (Assurance Review Board) of all Grantees as a positive check and reminder that their conformity to the appropriate agreement, and therefore the requirements of the AAS, remains their obligation. [Kantara IAF 1100]

**Applicant**
A party undergoing the processes of registration and identity proofing. [NIST SP 800-63-1]

An entity requesting cross-certification with the FBCA. [FBCA Cross-certification Methodology 3.0]

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. [ABADSG footnote 32] [FBCA CP 2.25]

An individual applying for a PIV Card/credential. The applicant may be a current or prospective Federal hire, a Federal employee, a government affiliate, or a contractor.28 [NIST FIPS 201-2]

An individual or person acting as a proxy for a machine or corporate entity who is the subject of an identity proofing process. [Kantara IAF 1100]

**Application**
A hardware/software system implemented to satisfy a particular set of requirements. In this context, an application incorporates a system used to satisfy a subset of requirements related to the verification or identification of an end user's identity so that the end user's identifier can be used to facilitate the end user's interaction with the system. [NIST FIPS 201-2]

A computer program designed and operated to achieve a set of goals or provide a set of services. [NIST SP 800-130]

**Application Identifier**
The period of time within a card session between whena card application is selected and a different card application is selected or the card session ends. [NIST SP 800-73-3 Part 1]

A globally uniquie identifier of a card application as defined in ISO/IEC 7816-4. [NIST SP 800-73-3 Part 2]

A globally uniquie identifier of a card application as defined in ISO/IEC 7816-4. [NIST SP 800-73-3 Part 3]

**Application Session**
The period of time within a card session between whena card application is selected and a different card application is selected or the card session ends. [NIST SP 800-73-3 Part 3]

**Approval**
The process by which the ARB accepts the compliance of a certified service and the CSP responsible for that service commits to upholding the Rules as defined in the AAS. [Kantara IAF 1100]

**Approved**
Federal Information Processing Standard (FIPS) approved or NIST recommended. An algorithm or technique that is either 1) specified in a FIPS or NIST Recommendation, or 2) adopted in a FIPS or NIST Recommendation. [NIST SP 800-63-1]

FIPS-Approved and/or NIST-recommended. [NIST FIPS 140-2]

Acceptance by ICAM to technically interoperate with other ICAM members. [ICAM SAML 2.0 WB SSO Profile 1.0.2]

**Approved Encryption**
Any cryptographic algorithm or method specified in a FIPS or a NIST recommendation or equivalent, as established by a recognized national technical authority. Refer to http://csrc.nist.gov/cryptval/. [Kantara IAF 1100]

**Approved Encryption Method**
FIPS approved or NIST recommended. An algorithm or technique that is either 1) specified in a FIPS or NIST Recommendation, or 2) adopted in a FIPS or NIST Recommendation [FICAM TFPAP 1.0.1]

**Approved Mode Of Operation**
a mode of the cryptographic module that employs only Approved security functions (not to be confused with a specific mode of an Approved security function, e.g., DES CBC mode). [NIST FIPS 140-2]

**Approved Security Function**
for this standard, a security function (e.g., cryptographic algorithm, cryptographic key management technique, or authentication technique) that is either a) specified in an Approved standard, b) adopted in an Approved standard and specified either in an appendix of the Approved standard or in a document referenced by the Approved standard, or c) specified in the list of Approved security functions. [NIST FIPS 140-2]

**Approved Service**
A certified service which has been granted an approval by the Kantara Initiative Board of Trustees. [Kantara IAF 1100]

**Architecture**
A highly structured specification of an acceptable approach within a framework for solving a specific problem. An architecture contains descriptions of all the components of a selected, acceptable solution while allowing certain details of specific components to be variable to satisfy related constraints (e.g., costs, local environment, user acceptability). [NIST FIPS 201-2]

**Archive**
Long-term, physically separate storage. [FBCA CP 2.25]

**Archive (key/metadata)**
To place an electronic cryptographic key and/or metadata into a long-term storage medium that will be maintained even if the storage technology changes. Also, the location where archived keys and/or metadata are stored. [NIST SP 800-130]

**Artifact**
(undefined) [OASIS SAML Glossary 2.0]

**Assert**
To make a statement about the properties of a user or user's act of authentication. [ICAM SAML 2.0 WB SSO Profile 1.0.2]

**Asserting Party**
Formally, the administrative domain that hosts one or more SAML authorities. Informally, an instance of a SAML authority.Attribute A distinct characteristic of an object (in SAML, of a subject). An object's attributes are said to describe it. Attributes are often specified in terms of physical traits, such as size, shape, weight, and color, etc., for real-world objects. Objects in cyberspace might have attributes describing size, type of encoding, network address, and so on. Attributes are often represented as pairs of "attribute name" and "attribute value(s)", e.g. "foo" has the value 'bar', "count" has the value 1, "gizmo" has the values "frob" and "2", etc. Often, these are referred to as "attribute value pairs". Note that Identifiers are essentially "distinguished attributes". See also Identifier and XML attribute. [OASIS SAML Glossary 2.0]

**Assertion**
A statement from a Verifier to a Relying Party (RP) that contains identity information about a Subscriber. Assertions may also contain verified attributes. [NIST SP 800-63-1]

A statement from a Verifier to a Relying Party that contains identity information about a Subscriber. Assertions may also contain verified attributes. [FICAM TFPAP 1.0.1]

Structured data objects containing Identity information and other relevant data. Sometimes called Identity Assertions. [InCommon IAAF 1.1]

The identity information provided by an Identity Provider to a Service Provider. [InCommon Glossary]

A statement from a verifier to a relying party that contains identity or other information about a subscriber. [Kantara IAF 1100]

A piece of data produced by a SAML authority regarding either an act of authentication performed on a subject, attribute information about the subject, or authorization data applying to the subject with respect to a specified resource. [OASIS SAML Glossary 2.0]

**Assertion Reference**
A data object, created in conjunction with an assertion, which identifies the Verifier and includes a pointer to the full assertion held by the Verifier. [NIST SP 800-63-1]

Identifies the Verifier and includes a pointer to the full assertion held by the Verifier. [FICAM TFPAP 1.0.1]

**Assessment**
A process used to evaluate an electronic trust service and the service provider using the requirements specified by one or more Service Assessment Criteria for compliance with all applicable requirements. [Kantara IAF 1100]

**Assessor**
A person or corporate entity who performs an assessment. [Kantara IAF 1100]

**Asset**
Anything that has value to an organization, including, but not limited to, another organization, person, computing device, information technology (IT) system, IT network, IT circuit, software (both an installed instance and a physical instance), virtual computing platform (common in cloud and virtualized computing), and related hardware (e.g., locks, cabinets, keyboards). [NIST IR 7693]

**Asset Identification**
The use of attributes and methods to uniquely identify an asset. [NIST IR 7693]

**Asset Identification Element**
A complete, bound expression of an asset identification using the constructs defined in this specification. [NIST IR 7693]

**Associated Metadata**
Metadata protected against unauthorized modification and disclosure by the CKMS using an association function. [NIST SP 800-130]

**Association Function**
In this document, a function that protects a key and metadata from unauthorized modification and disclosure and authenticates the source of the metadata. [NIST SP 800-130]

**Assurance**
In the context of OMB M-04-04 and this document, assurance is defined as 1) the degree of confidence in the vetting process used to establish the identity of an individual to whom the credential was issued, and 2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued. [NIST SP 800-63-1]

**Assurance Assessment Scheme**
A program which defines the process for assessing the operating standards of certain players in the Identity and Credential Assurance Management space against strict criteria, and grants to candidates of the Scheme the right to use the Kantara Initiative Mark, a symbol of trustworthy identity and credential management services, at specified Assurance Levels. [Kantara IAF 1100]

**Assurance Level**
A degree of certainty that a claimant has presented a credential that refers to the claimant's identity. Each assurance level expresses a degree of confidence in the process used to establish the identity of the individual to whom the credential was issued and a degree of confidence that the individual who uses the Kantara Initiative Identity Assurance credential is the individual to whom the credential was issued. The four assurance levels are: Level 1: Little or no confidence in the asserted identity's validity Level 2: Some confidence in the asserted identity's validity Level 3: High confidence in the asserted identity's validity Level 4: Very high confidence in the asserted identity's validity [Kantara IAF 1100]

Strength of the binding between a Public Key and the individual whose Subject name is cited in the Certificate Mechanisms used to control the use of the Private Key Security provided by the PKI itself. [SAFE-BioPharma CP 2.5]

**Assurance Review Board**
The Assurance Review Board (ARB) is a sub-committee of the Board of Trustees, and is the operational authoritative body of the Kantara Identity Assurance Framework Assurance Assessment Scheme (AAS) certification program. It has delegated authority from the Kantara Initiative Board of Trustees (KIBoT) to undertake assessments of all types of applications for a Grant of Rights of Use of the Kantara Initiative Mark and shall make recommendations to the KIBoT for the award or denial of such Grants. [Kantara IAF 1100]

**Asymmetric Keys**
Two related keys, a public key and a private key that are used to perform complementary operations, such as encryption and decryption or signature generation and signature verification. [NIST SP 800-63-1]

Two related keys, a public key and a private key, that are used to perform complementary operations, such as encryption and decryption or signature generation and signature verification. [NIST FIPS 201-2]

**Attack**
An attempt by an unauthorized individual to fool a Verifier or a Relying Party into believing that the unauthorized individual in question is the Subscriber. [NIST SP 800-63-1]

An attempt to obtain a subscriber's token or to fool a verifier into believing that an unauthorized individual possesses a claimant's token. [Kantara IAF 1100]

**Attacker**
A party who acts with malicious intent to compromise an information system. [NIST SP 800-63-1]

**Attribute**
A claim of a named quality or characteristic inherent in or ascribed to someone or something. (See term in [ICAM] for more information.) [NIST SP 800-63-1]

A single piece of information associated with an electronic identity database record. Some attributes are general; others are personal. Some subset of all attributes defines a unique individual. Examples of an attribute are name, phone number, and group affiliation. [InCommon Glossary]

A property associated with an individual. [Kantara IAF 1100]

**Attribute Assertion**
A mechanism for associating specific attributes with a user. [InCommon Glossary]

An assertion that conveys information about attributes of a subject. [OASIS SAML Glossary 2.0]

**Attribute Authority**
Entity providing Backend Attributes to the requesting BAE Relying Party. For this BAE release, the AA is the agency that issued the Credential to the Cardholder. The AA is the authoritative source of Backend Attributes for that Cardholder. [BAE Overview]

An entity, recognized by the FPKIPA or comparable Entity body as having the authority to verify the association of attributes to an identity. [FBCA CP 2.25]

The Shibboleth software service that asserts the requesting individual's attributes by creating an attribute assertion and then digitally signing it. The receiving online Service Provider must be able to validate this signature. [InCommon Glossary]

A system entity that produces attribute assertions. [SAMLAgree] [OASIS SAML Glossary 2.0]

**Attribute Authority Subject DN**
The distinguished name of the Attribute Authority. [InCommon Glossary]

**Attribute Authority URL**
The Internet address of the Attribute Authority. [InCommon Glossary]

**Attribute Provider**
[entity] responsible for the processes associated with establishing and maintaining identity attributes. Attribute maintenance includes validating, updating, and revoking the attribute claim. An attribute provider asserts trusted, validated attribute claims in response to attribute requests from relying parties In certain instances, a subject may self-assert attribute claims to relying parties. Trusted, validated attributes inform relying parties' decision to authorize subjects. [NSTIC Strategy]

**Attribute Release Policy**
Rules that an AA follows when deciding whether or not to release an attribute and its value(s) [InCommon Glossary]

**Attribute Service**
Provides Subject Attributes in response to queries from SPs. [InCommon IAAF 1.1]

**Attribute Subject**
Authentication Credential holder for whom an RP requires information (Backend Attributes) directly from the authoritative source (Attribute Authority), which is the agency that issued the Attribute Subject's Authentication Credential. [BAE Overview]

**Attributes**
Elements of an Identity. [InCommon IAAF 1.1]

a named quality or characteristic inherent in or ascribed to someone or something (for example, "this individual's age is at least 21 years"). [NSTIC Strategy]

**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. [NS4009] [FBCA CP 2.25]

An independent review and examination of a system's records and activities to determine the adequacy of system controls, ensure compliance with established security policy and procedures, detect breaches in security services, and recommend any changes that are indicated for countermeasures. [InCommon Glossary]

The procedures performed by an audit administrator to collect, analyze, and summarize the data required in a report to the system administrator regarding the security of the system. [NIST SP 800-130]

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. [SAFE-BioPharma CP 2.5]

**Audit Criteria**
TFP auditor qualifications, TFP identity provider audit processes, and ongoing TFP identity provider re-certification processes. [FICAM TFPAP 1.0.1]

**Audit Data**
Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. [NS4009, "audit trail"] [FBCA CP 2.25]

Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. [SAFE-BioPharma CP 2.5]

**Audit Organization**
An organization which undertakes assessments of entities and their services to establish their conformity to or compliance with specific standards or other widely-recognized criteria. Specifically, in the context of the AAS, entities providing credentialing or identity management services which are claiming conformance to the IAF. [Kantara IAF 1100]

**Authenticatable Entity**
An entity that can successfully participate in an authentication protocol with a card application. [NIST SP 800-73-3 Part 1]

An entity that can successfully participate in an authentication protocol with a card application. [NIST SP 800-73-3 Part 2]

**Authenticate**
To confirm the identity of an entity when that identity is presented. [FBCA CP 2.25]

**Authentication**
The process of establishing confidence in the identity of users or information systems. [NIST SP 800-63-1]

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. [NS4009] [FBCA CP 2.25]

The process of establishing confidence in the identity of users or information systems. [FICAM TFPAP 1.0.1]

The process of establishing confidence of authenticity; in this case, in the validity of a person's identity and the PIV Card. [NIST FIPS 201-2]

The security measure by which a person transmits and validates his or her association with an electronic identifier. An example of authentication is submitting a password that is associated with a user account name. [InCommon Glossary]

Authentication simply establishes identity, not what that identity is authorized to do or what access privileges he or she has. [Kantara IAF 1100]

The process of establishing that individuals, organizations, or things are who or what they claim to be. In the context of a PKI, authentication can be the process of establishing that an individual or organization applying for or seeking access to something under a certain name is, in fact, the proper individual or organization. This corresponds to the second process involved with identification, as shown in the definition of "identification" below. Authentication can also refer to a security service that provides assurances that individuals, organizations, or things are who or what they claim to be or that a message or other data originated from a specific individual, organization, or device. Thus, it is said that a digital signature of a message authenticates the message's sender. [IETF RFC 3647]

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. [SAFE-BioPharma CP 2.5]

To confirm a system entity's asserted principal identity with a specified, or understood, level of confidence. [CyberTrust] [SAMLAgree] [OASIS SAML Glossary 2.0]

**Authentication Assertion**
An assertion that conveys information about a successful act of authentication that took place for a subject. [OASIS SAML Glossary 2.0]

**Authentication Assurance Level**
A measure of trust or confidence in an authentication mechanism defined in [OMB0404] and [SP 800-63], in terms of four levels: Level 1: LITTLE OR NO confidence Level 2: SOME confidence Level 3: HIGH confidence Level 4: VERY HIGH confidence [NIST FIPS 201-2]

**Authentication Authority**
A system entity that produces authentication assertions. [SAMLAgree] [OASIS SAML Glossary 2.0]

**Authentication Code**
a cryptographic checksum based on an Approved security function (also known as a Message Authentication Code). [NIST FIPS 140-2]

**Authentication Protocol**
A defined sequence of messages between a Claimant and a Verifier that demonstrates that the Claimant has possession and control of a valid token to establish his/her identity, and optionally, demonstrates to the Claimant that he or she is communicating with the intended Verifier. [NIST SP 800-63-1]

A defined sequence of messages between a Claimant and a Verifier that demonstrates that the Claimant has control of a valid token to establish his/her identity, and optionally, demonstrates to the Claimant that he or she is communicating with the intended Verifier. [FICAM TFPAP 1.0.1]

A well-specified message exchange process that verifies possession of a token to remotely authenticate a claimant. Some authentication protocols also generate cryptographic keys that are used to protect an entire session, so that the data transferred in the session is cryptographically protected. [Kantara IAF 1100]

**Authentication Protocol Run**
An exchange of messages between a Claimant and a Verifier that results in authentication (or authentication failure) between the two parties. [NIST SP 800-63-1]

**Authentication Secret**
A generic term for any secret value that could be used by an Attacker to impersonate the Subscriber in an authentication protocol. These are further divided into short-term authentication secrets, which are only useful to an Attacker for a limited period of time, and long-term authentication secrets, which allow an Attacker to impersonate the Subscriber until they are manually reset. The token secret is the canonical example of a long term authentication secret, while the token authenticator, if it is different from the token secret, is usually a short term authentication secret. [NIST SP 800-63-1]

Used generically for passwords, passphrases, PINs, symmetric keys and other forms of secrets used for authentication [InCommon IAAF 1.1]

**Authentication Session**
Period of time that an end user remains trusted after the end user authenticates. That is because an IdP typically does not require an end user to re-authenticate for every page requested. Each IdP defines its own authentication session duration. If an end user returns to the IdP and an earlier authentication session has expired, the IdP re-authenticates the end user - even if single sign-on is in effect. [ICAM SAML 2.0 WB SSO Profile 1.0.2]

**Authenticity**
The property that data originated from its purported source. [NIST SP 800-63-1]

**Authoritative Source**
The Authoritative Source for a Backend Attribute is the entity that maintains the attested version of that Backend Attribute. When more than one entity (e.g., another Attribute Authority, a RP) has the same Backend Attribute, the Authoritative Source's value must be considered the correct value, and should take precedent over all other values. Only one Authoritative Source should exist per Backend Attribute. [BAE Overview]

**Authoritative Time Source**
A network entity that is relied upon to provide accurate time. [NIST SP 800-130]

**Authorization**
The process for determining a specific person's eligibility to gain access to a resource or service, a right or permission granted to access an online system [InCommon Glossary]

Process of deciding what an individual ought to be allowed to do. [Kantara IAF 1100]

The process of determining, by evaluating applicable access control information, whether a subject is allowed to have the specified types of access to a particular resource. Usually, authorization is in the context of authentication. Once a subject is authenticated, it may be authorized to perform different types of access. [Taxonomy] [OASIS SAML Glossary 2.0]

**Authorization Code**
Authorization codes operate as plaintext bearer credentials, used to verify that the resource owner who granted authorization at the authorization server is the same resource owner returning to the client to complete the process. Therefore, if the client relies on the authorization code for its own resource owner authentication, the client redirection endpoint MUST require the use of TLS. Authorization codes MUST be short lived and single use. If the authorization server observes multiple attempts to exchange an authorization code for an access token, the authorization server SHOULD attempt to revoke all access tokens already granted based on the compromised authorization code. If the client can be authenticated, the authorization servers MUST authenticate the client and ensure that the authorization code was issued to the same client. [IETF ID OAuth 2.0]

**Authorization Decision**
The result of an act of authorization. The result may be negative, that is, it may indicate that the subject is not allowed any access to the resource. [OASIS SAML Glossary 2.0]

**Authorization Decision Assertion**
An assertion that conveys information about an authorization decision. [OASIS SAML Glossary 2.0]

**Authorization Endpoint**
One of two defined authorization server endpoints, used by the client to obtain authorization from the resource owner via user-agent redirection. [IETF ID OAuth 2.0]

**Authorization Grant**
An authorization grant is a credential representing the resource owner's authorization (to access its protected resources) used by the client to obtain an access token. This specification defines four grant types: authorization code, implicit, resource owner password credentials, and client credentials, as well as an extensibility mechanism for defining additional types. [IETF ID OAuth 2.0]

**Authorization Manager**
An UMA-defined variant of an OAuth authorization server that carries out an authorizing user's policies governing access to a protected resource. [Kantara UMA]

**Authorization Server**
The server issuing access tokens to the client after successfully authenticating the resource owner and obtaining authorization. [IETF ID OAuth 2.0]

**Authorizing User**
The "user" in User-Managed Access. An UMA-defined variant of an OAuth resource owner, typically a web user who configures an authorization manager with policies that control how it assigns access permissions (or other authorization data) to requesters for a protected resource. The authorizing user can also be a corporation or other legal person. [Kantara UMA]

**Automated Key Transport**
the transport of cryptographic keys, usually in encrypted form, using electronic means such as a computer network (e.g., key transport/agreement protocols). [NIST FIPS 140-2]

**BAE Broker**
The Broker is the communications conduit between RPs and Attribute Authorities. [BAE Overview]

**BAE External Service**
Handles the exchange of Backend Attributes between trusted BAE partners. [BAE Overview]

**BAE Internal Service**
Handles the exchange of Backend Attribute data between local attribute authorities. [BAE Overview]

**BAE Relying Party**
Entity requesting Backend Attributes typically to support Cardholder authentication, authorization, or emergency events. [BAE Overview]

**BAE Requester**
BAE Broker that sends a request for Backend Attributes. [BAE Overview]

**BAE Responder**
BAE Broker that returns Backend Attribute values that were requested by a BAE Requester. [BAE Overview]

**BER-TLV Data Object**
A data object coded according to ISO/IEC 8825-2. [NIST SP 800-73-3 Part 1]

A data object coded according to ISO/IEC 8825-2. [NIST SP 800-73-3 Part 2]

A data object coded according to ISO/IEC 8825-2. [NIST SP 800-73-3 Part 3]

**Back Channel**
Back channel refers to direct communications between two system entities without "redirecting" messages through another system entity such as an HTTP client (e.g. A user agent). See also front channel. [OASIS SAML Glossary 2.0]

**Backend Attribute Exchange**
Process by which an RP obtains attribute information (Backend Attributes) about a claimant through a direct connection to an attribute source (attribute provider) - in contrast to a front-channel attribute delivery where the claimant is directly involved in the process, typically as part of the authentication event. [BAE Overview]

**Backend Attributes**
Cardholder information stored by an Attribute Authority available to Relying Parties typically to support Cardholder authentication, authorization, or emergency events. [BAE Overview]

**Backup**
Copy of files and programs made to facilitate recovery if necessary. [NS4009] [FBCA CP 2.25]

Copy of files and programs made to facilitate recovery if necessary. [SAFE-BioPharma CP 2.5]

**Backup (key/metadata)**
The process of placing at least one copy of a key and/or its metadata in one or more facilities so that the key and/or metadata can be recovered if the original values are lost or modified during operational usage. [NIST SP 800-130]

**Base URL**
The SCIM REST API is always relative to a Base URL. The Base URL MUST NOT contain a query string as Consumers may append additional path information and query parameters as part of forming the request. Example: https://example.com/scim/v1/ [IETF ID SCIM 1.0]

**Batch Processing**
A data processing operation and where related BAE transactions are grouped together and transmitted for processing in one group. [BAE Overview]

**Bearer Assertion**
An assertion that does not provide a mechanism for the Subscriber to prove that he or she is the rightful owner of the assertion. The RP has to assume that the assertion was issued to the Subscriber who presents the assertion or the corresponding assertion reference to the RP. [NIST SP 800-63-1]

An assertion that does not provide a mechanism for the Subscriber to prove that he or she is the rightful owner of the assertion. The Relying Party has to assume that the assertion was issued to the Subscriber who presents the assertion or the corresponding assertion reference to the Relying Party. [FICAM TFPAP 1.0.1]

**Billing Contact**
The Billing Contact is responsible for executing and maintaining all of the Participant's financial transactions associated with its InCommon federation participation, including any necessary communication with its internal Executive and Administrative Contacts, and externally with federation accounting staff. [InCommon Glossary]

**Binding**
Process of associating two related elements of information. [NS4009] [FBCA CP 2.25]

Process of associating two related elements of information. [SAFE-BioPharma CP 2.5]

Mappings of SAML request-response message exchanges onto standard messaging or communication protocols. [ICAM SAML 2.0 WB SSO Profile 1.0.2]

Generically, a specification of the mapping of some given protocol's messages, and perhaps message exchange patterns, onto another protocol, in a concrete fashion. For example, the mapping of the SAML message onto HTTP is one example of a binding. The mapping of that same SAML message onto SOAP is another binding. In the SAML context, each binding is given a name in the pattern "SAML xxx binding". [OASIS SAML Glossary 2.0]

**Biometric**
A physical or behavioral characteristic of a human being. [FBCA CP 2.25]

Automated recognition of individuals based on their behavioral and biological characteristics. In this document, biometrics may be used to unlock authentication tokens and prevent repudiation of registration. [FICAM TFPAP 1.0.1]

A measurable, physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an applicant. Facial images, fingerprints, and iris image samples are all examples of biometrics. [NIST FIPS 201-2]

**Biometric Information**
The stored electronic information pertaining to a biometric. This information can be in terms of raw or compressed pixels or in terms of some characteristic (e.g., patterns). [NIST FIPS 201-2]

**Biometrics**
Automated recognition of individuals based on their behavioral and biological characteristics. In this document, biometrics may be used to unlock authentication tokens and prevent repudiation of registration. [NIST SP 800-63-1]

**Bit**
A binary digit: 0 or 1. [NIST SP 800-63-1]

A binary digit: 0 or 1. [Kantara IAF 1100]

**Bona Fides**
Evidence that provides insight into an organization's maturity, legitimacy, stability, and reputation. [FICAM TFPAP 1.0.1]

**Bridge CA**
A CA that itself does not issue certificates to end entities (except those required for its own operations) but establishes unilateral or bilateral cross-certification with other CAs. [FBCA Cross-certification Methodology 3.0]

**CA Facility**
The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation. [FBCA CP 2.25]

**CA Software**
Key Management and cryptographic software used to manage certificates issued to subscribers. [SAFE-BioPharma CP 2.5]

**CKMS Component**
Any hardware, software, or firmware that is used to implement a CKMS. [NIST SP 800-130]

**CKMS Device**
Any combination of CKMS components that serve a specific purpose (e.g., firewalls, routers, transmission devices, cryptographic modules, and data storage devices). [NIST SP 800-130]

**CKMS Module**
A logical entity that performs all required CKMS functions at a given location. [NIST SP 800-130]

**CKMS Profile**
A document that provides an implementation independent specification of CKMS security requirements for use by a communityof-interest (e.g., U.S. Government; banking, health, and aerospace). [NIST SP 800-130]

**CPS Summary (or CPS Abstract)**
A subset of the provisions of a complete CPS that is made public by a CA. [IETF RFC 3647]

**Ca-certificate**
A certificate for one CA's public key issued by another CA. [IETF RFC 3647]

**Capture**
The method of taking a biometric sample from an end user. [INCITS/M1-040211] [NIST FIPS 201-2]

**Card**
An integrated circuit card. [NIST SP 800-73-3 Part 1]

An integrated circuit card. [NIST SP 800-73-3 Part 2]

An integrated circuit card. [NIST SP 800-73-3 Part 3]

An integrated circuit card. [NIST SP 800-73-3 Part 4]

**Card Application**
A set of data objects and card commands that can be selected using an application identifier. [NIST SP 800-73-3 Part 1]

A set of data objects and card commands that can be selected using an appliction identifier. [NIST SP 800-73-3 Part 2]

A set of data objects and card commands that can be selected using an appliction identifier. [NIST SP 800-73-3 Part 3]

A set of data objects and card commands that can be selected using an appliction identifier. [NIST SP 800-73-3 Part 4]

**Card Interface Device**
An electronic device that connects an integrated circuit card and the card applications therein to a client application. [NIST SP 800-73-3 Part 3]

**Card Issuer**
An authorized identity card creator that procures FIPS-approved blank identity cards, initializes them with appropriate software and data elements for the requested identity verification and access control application, personalizes the cards with the identity credentials of the authorized subjects, and delivers the personalized cards to the authorized subjects along with appropriate instructions for protection and use. [BAE Overview]

**Card Management System**
The card management system manages the lifecycle of a PIV Card Application. [NIST FIPS 201-2]

**Card Reader**
Synonym for card interface device. [NIST SP 800-73-3 Part 3]

**Cardholder**
An individual possessing an issued PIV Card. [NIST FIPS 201-2]

**Cardholder Unique Identifier**
The CHUID is defined to provide the basis for interoperable identification of individuals and to extend capabilities over magnetic stripe technology for Physical Access Control System applications. It contains a series of mandatory and optional tagged objects. Some of these include the Federal Agency Smart Credential Number (FASC-N), the Global Unique ID (GUID), and the Asymmetric Signature. [BAE Overview]

**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. [ABADSG]. As used in this CP, the term "Certificate" refers to certificates that expressly reference the OID of this CP in the "Certificate Policies" field of an X.509 v.3 certificate. [FBCA CP 2.25]

A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies it's Subscriber, (3) contains the Subscriber's public key, (4) identifies it's operational period, and (5) is digitally signed by the certification authority issuing it. [ABADSG] [FBCA CP 2.25]

refers to X.509 certificates unless otherwise qualified. Usage of certificates is dictated by the underlying protocols, e.g. HTTPS or WS-Security, except where noted [OASIS IMI 1.0]

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. [InCommon Glossary]

**Certificate Authority**
A trusted entity that issues and revokes public key certificates. [NIST SP 800-63-1]

A certificate authority (CA) is an authority in a network that issues and manages security credentials and public keys for message encryption. [InCommon Glossary]

**Certificate Management Authority**
A Certification Authority or a Registration Authority. [FBCA CP 2.25]

**Certificate Policy**
A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements [RFC 2828]. A PKI may adopt more than one CP. [FBCA Cross-certification Methodology 3.0]

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. [FBCA CP 2.25]

A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. http://www.ietf.org/rfc/rfc3647.txt [InCommon Glossary]

A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular CP might indicate applicability of a type of certificate to the authentication of parties engaging in business-to-business transactions for the trading of goods or services within a given price range. [IETF RFC 3647]

**Certificate Policy Working Group**
A subordinate committee of the FPKIPA that is responsible for reviewing Applicant CPs; for performing the policy mapping of the submitted policies to the [FBCA CP] on behalf of the FPKIPA; and, for advising the FPKIPA at which level of assurance the Applicant CP(s) would map to the [FBCA CP]. The CPWG also recommends changes to the [FBCA CP] to the FPKIPA for approval. [FBCA Cross-certification Methodology 3.0]

**Certificate Revocation List**
A list of revoked public key certificates created and digitally signed by a Certificate Authority. See [RFC 5280]. [NIST SP 800-63-1]

A data structure that enumerates digital certificates that have been invalidated by their issuer prior to when they were scheduled to expire [RFC 2828]. [FBCA Cross-certification Methodology 3.0]

A list maintained by a Certification Authority of the certificates which it has issued that are revoked prior to their stated expiration date. [FBCA CP 2.25]

A list of revoked public key certificates created and digitally signed by a certification authority. [RFC 5280] 28 See Page 2 of [OMB0524] for further details of individuals who are eligible to be issued PIV Cards. [NIST FIPS 201-2]

**Certificate Signing Request**
A digital file which contains a user's name and public key. The user sends the CSR to a Certificate Authority (CA) to be converted into a certificate. [InCommon Glossary]

**Certificate Status Authority**
A trusted entity that provides on-line verification to a Relying Party of a subject certificate's trustworthiness, and may also provide additional attribute information for the subject certificate. [FBCA CP 2.25]

A trusted entity that provides on-line verification to a Relying Party of a subject certificate's trustworthiness, and that may also provide additional attribute information for the subject certificate. [SAFE-BioPharma CP 2.5]

**Certificate-related Information**
Information, such as a subscriber's postal address, that is not included in a certificate. May be used by a CA managing certificates. [FBCA CP 2.25]

**Certification**
TFP certification of an identity provider is the determination that the identity provider's policies and practices are comparable to ICAM trust requirements. [FICAM TFPAP 1.0.1]

The process of verifying the correctness of a statement or claim and issuing a certificate as to its correctness. [NIST FIPS 201-2]

The ARB's affirmation that a particular credential service provider can provide a particular credential service at a particular assurance level based on a certification report from an accredited assessor. [Kantara IAF 1100]

**Certification Authority**
An entity that issues certificates (especially X.509 certificates) and vouches for the binding between the data items in a certificate [RFC 2828]. [FBCA Cross-certification Methodology 3.0]

An authority trusted by one or more users to issue and manage X.509 Public Key Certificates and CARLs or CRLs. [FBCA CP 2.25]

A trusted entity that issues and revokes public key certificates. [NIST FIPS 201-2]

**Certification Authority Revocation List**
(undefined) [FBCA CP 2.25]

**Certification Authority Software**
Key Management and cryptographic software used to manage certificates issued to subscribers. [FBCA CP 2.25]

**Certification Body**
An organization which has been deemed competent to perform assessments of a particular type. Such assessments may be formal evaluations or testing and be based upon some defined set of standards or other criteria. [Kantara IAF 1100]

**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. [IETF RFC 3647]

**Certification Practice Statement**
A declaration by a CA of the details of the system and practices it employs in its certificate management operations A CPS is usually more detailed and procedurally oriented than a CP [RFC 2828]. [FBCA Cross-certification Methodology 3.0]

A statement of the practices that a CA employs in issuing, suspending, revoking and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this CP, or requirements specified in a contract for services). [FBCA CP 2.25]

A statement of the practices that a certification authority employs in issuing, managing, revoking, and renewing or re-keying certificates. http://www.ietf.org/rfc/rfc3647.txt [InCommon Glossary]

A statement of the practices that a certification authority employs in issuing, managing, revoking, and renewing or re-keying certificates. [IETF RFC 3647]

**Certified Information System Auditor**
(undefined) [FICAM TFPAP 1.0.1]

**Certified Information Systems Auditor**
(undefined) [InCommon IAAF 1.1]

**Certified Service**
An electronic trust service which has been assessed by a Kantaraaccredited assessor and found to be compliant with the applicable SACs. [Kantara IAF 1100]

**Chain-of-trust**
The chain-of-trust is a sequence of related enrollment data sets that is created and maintained by PIV Card issuers. [NIST FIPS 201-2]

**Challenge-response Protocol**
An authentication protocol where the Verifier sends the Claimant a challenge (usually a random value or a nonce) that the Claimant combines with a secret (such as by hashing the challenge and a shared secret together, or by applying a private key operation to the challenge) to generate a response that is sent to the Verifier. The Verifier can independently verify the response generated by the Claimant (such as by re-computing the hash of the challenge and the shared secret and comparing to the response, or performing a public key operation on the response) and establish that the Claimant possesses and controls the secret. [NIST SP 800-63-1]

**Chief Information Officers**
(undefined) [FICAM TFPAP 1.0.1]

**Circuit**
A dedicated single connection between two endpoints on a network. [NIST IR 7693]

**Claim**
a piece of information about a Subject that an Identity Provider asserts about that Subject. [OASIS IMI 1.0]

A statement of the value or values of one or more identity attributes of a requesting party. A requesting party may need to provide claims to an authorization manager in order to satisfy policy and gain permission for access to a protected resource. [Kantara UMA]

**Claimant**
A party whose identity is to be verified using an authentication protocol. [NIST SP 800-63-1]

A party whose identity is to be verified using an authentication protocol. [BAE Overview]

A party whose identity is to be verified using an authentication protocol. [FICAM TFPAP 1.0.1]

A party whose identity is to be verified. [Kantara IAF 1100]

**Claimed Address**
The physical location asserted by an individual (e.g. an applicant) where he/she can be reached. It includes the residential street address of an individual and may also include the mailing address of the individual. For example, a person with a foreign passport, living in the U.S., will need to give an address when going through the identity proofing process. This address would not be an "address of record" but a "claimed address." [NIST SP 800-63-1]

**Claimed Identifier**
An Identifier that the end user claims to own; the overall aim of the protocol is verifying this claim. The Claimed Identifier is either: The Identifier obtained by normalizing the User-Supplied Identifier, if it was an URL. The CanonicalID, if it was an XRI. [OpenID Authentication 2.0]

**Client**
An application making protected resource requests on behalf of the resource owner and with its authorization. The term client does not imply any particular implementation characteristics (e.g. whether the application executes on a server, a desktop, or other devices). [IETF ID OAuth 2.0]

An HTTP client (per [RFC2616]) capable of making OAuth- authenticated requests (Section 3). [IETF RFC 5849]

**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. [FBCA CP 2.25]

A system entity, usually a computer process acting on behalf of a human user, that makes use of a service provided by a server. [SAFE-BioPharma CP 2.5]

**Client Application**
A computer program running on a computer in communication with a card interface device. [NIST SP 800-73-3 Part 1]

A computer program running on a computer in communication with a card interface device. [NIST SP 800-73-3 Part 2]

A computer program running on a computer in communication with a card interface device. [NIST SP 800-73-3 Part 3]

**Client Identifier**
The authorization server issues the registered client a client identifier - a unique string representing the registration information provided by the client. The client identifier is not a secret; it is exposed to the resource owner, and MUST NOT be used alone for client authentication. The client identifier is unique to the authorization server. The client identifier string size is left undefined by this specification. The client should avoid making assumptions about the identifier size. The authorization server SHOULD document the size of any identifier it issues. [IETF ID OAuth 2.0]

**Client Password**
A protocol field. [IETF ID OAuth 2.0]

**Client Secret**
A protocol field. [IETF ID OAuth 2.0]

**Commercial Off-the-shelf**
Technology and/or a product that is ready-made and available for sale, lease, or license to the general public. [NIST SP 800-130]

**Common Criteria**
A set of internationally accepted semantic tools and constructs for describing the security needs of customers and the security attributes of products. [FBCA CP 2.25]

A set of internationally accepted semantic tools and constructs for describing the security needs of customers and the security attributes of products. [SAFE-BioPharma CP 2.5]

**Comparability**
Equivalence of Trust Framework Provider criteria to ICAM trust criteria as determined by ICAM designated Assessment Teams. [FICAM TFPAP 1.0.1]

**Comparison**
The process of comparing a biometric with a previously stored reference. See also "Identification" and "Identity Verification". [INCITS/M1-040211] [NIST FIPS 201-2]

**Completely Automated Public Turing Test To Tell Computers And Humans Apart**
An interactive feature added to web-forms to distinguish use of the form by humans as opposed to automated agents. Typically, it requires entering text corresponding to a distorted image or from a sound stream. [NIST SP 800-63-1]

**Component**
An element of a large system, such as an identity card, issuer, card reader, or identity verification support, within the PIV system. [NIST FIPS 201-2]

**Components, PKI Components**
Collective name for Certification Authorities, Certificate Status Authorities (CSAs), Registration Authorities (RAs) and Trusted Agents [SAFE-BioPharma CP 2.5]

**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. [NS4009] [FBCA CP 2.25]

the unauthorized disclosure, modification, substitution, or use of sensitive data (including plaintext cryptographic keys and other CSPs). [NIST FIPS 140-2]

The unauthorized disclosure, modification, substitution or use of sensitive data (e.g., keys, metadata, and other security-related information). [NIST SP 800-130]

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. [SAFE-BioPharma CP 2.5]

**Compromised State**
A key life cycle state in which a key is designated as compromised and is not to be used to apply cryptographic protection to data. Under certain circumstances, the key may be used to process already-protected data. [NIST SP 800-130]

**Computer Security Objects Registry**
Computer Security Objects Registry operated by the National Institute of Standards and Technology. [FBCA CP 2.25]

**Computing Device**
A machine (real or virtual) for performing calculations automatically (including, but not limited to, computer, servers, routers, switches, etc.) [NIST IR 7693]

**Conditional Element**
element the presence of which in a document is dependant on the provisions of the particular document [ISO-IEC Directives Part 2]

**Confidentiality**
Assurance that information is not disclosed to unauthorized entities or processes. [NS4009] [FBCA CP 2.25]

The property that sensitive information is not disclosed to unauthorized individuals, entities or processes. [FICAM TFPAP 1.0.1]

the property that sensitive information is not disclosed to unauthorized individuals, entities, or processes. [NIST FIPS 140-2]

the process by which data is protected such that only authorized actors or security token owners can view the data [OASIS IMI 1.0]

Assurance that information is not disclosed to unauthorized entities or processes. [SAFE-BioPharma CP 2.5]

**Conformance Testing**
A process established by NIST within its responsibilities of developing, promulgating, and supporting FIPS for testing specific characteristics of components, products, and services, as well as people and organizations for compliance with a FIPS. [NIST FIPS 201-2]

**Consolidated Metadata**
Multiple or files into a single file. [ICAM SAML 2.0 WB SSO Profile 1.0.2]

**Control Information**
information that is entered into a cryptographic module for the purposes of directing the operation of the module. [NIST FIPS 140-2]

**Cookie**
A character string, placed in a web browser's memory, which is available to websites within the same Internet domain as the server that placed them in the web browser. Cookies are used for many purposes and may be assertions or may contain pointers to assertions. See Section 9.1.1 for more information. [NIST SP 800-63-1]

**Credential**
An object or data structure that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a Subscriber. While common usage often assumes that the credential is maintained by the Subscriber, this document also uses the term to refer to electronic records maintained by the CSP which establish a binding between the Subscriber's token and identity. [NIST SP 800-63-1]

Evidence attesting to one's right to credit or authority; in this Standard, it is the PIV Card and data elements associated with an individual that authoritatively binds an identity (and, optionally, additional attributes) to that individual. [NIST FIPS 201-2]

A unique identifier and authentication material. [InCommon IAAF 1.1]

An object to be verified when presented in an authentication transaction. A credential can be bound in some way to the individual to whom it was issued, or it can be a bearer credential. [Kantara IAF 1100]

**Credential Assessment Profile**
(undefined) [Kantara IAF 1100]

**Credential Management**
A service that supports the lifecycle of identity credentials from issuance to revocation, including renewal, status checks, and authentication services. [Kantara IAF 1100]

**Credential Service**
A type of electronic trust service that supports the verification of identities (identity proofing), the issuance of identity related assertions/credentials/tokens, and the subsequent management of those credentials (for example, renewal, revocation, and the provision of related status and authentication services). [Kantara IAF 1100]

**Credential Service Provider**
A trusted entity that issues or registers Subscriber tokens and issues electronic credentials to Subscribers. The CSP may encompass Registration Authorities (RAs) and Verifiers that it operates. A CSP may be an independent third party, or may issue credentials for its own use. [NIST SP 800-63-1]

An electronic trust service provider that operates one or more credential services. A CSP can include a Registration Authority. CSP See Credential Service Provider. [Kantara IAF 1100]

**Credential Store**
Contains Authentication Secrets for all Subjects [InCommon IAAF 1.1]

**Credentials**
information objects used during a transaction to provide evidence of the subject's identity. The credential may also provide a link to the subject's authority, roles, rights, privileges, and other attributes. The credential can be stored on an identity medium. [NSTIC Strategy]

Credentials are a pair of a unique identifier and a matching shared secret. OAuth defines three classes of credentials: client, temporary, and token, used to identify and authenticate the client making the request, the authorization request, and the access grant, respectively. [IETF RFC 5849]

Data that is transferred to establish a claimed principal identity. [X.800] [SAMLAgree] [OASIS SAML Glossary 2.0]

**Critical Security Parameter**
security-related information (e.g., secret and private cryptographic keys, and authentication data such as passwords and PINs) whose disclosure or modification can compromise the security of a cryptographic module. [NIST FIPS 140-2]

**Cross Site Request Forgery**
An attack in which a Subscriber who is currently authenticated to an RP and connected through a secure session, browses to an Attacker's website which causes the Subscriber to unknowingly invoke unwanted actions at the RP. For example, if a bank website is vulnerable to a CSRF attack, it may be possible for a Subscriber to unintentionally authorize a large money transfer, merely by viewing a malicious link in a webmail message while a connection to the bank is open in another browser window. [NIST SP 800-63-1]

**Cross Site Scripting**
A vulnerability that allows attackers to inject malicious code into an otherwise benign website. These scripts acquire the permissions of scripts generated by the target website and can therefore compromise the confidentiality and integrity of data transfers between the website and client. Websites are vulnerable if they display user supplied data from requests or forms without sanitizing the data so that it is not executable. [NIST SP 800-63-1]

**Cross-certificate**
A certificate issued by one CA to another CA for the purpose of establishing a trust relationship between the two CAs. [FBCA Cross-certification Methodology 3.0]

A certificate used to establish a trust relationship between two Certification Authorities. [FBCA CP 2.25]

A certificate used to establish a trust relationship between two Certification Authorities. [SAFE-BioPharma CP 2.5]

**Cross-certification**
The act or process by which two CAs each certify a public key of the other, issuing a public-key certificate to that other CA [RFC 2828]. [FBCA Cross-certification Methodology 3.0]

**Cross-certified**
A certificate used to establish a trust relationship between two Certification Authorities. [FICAM TFPAP 1.0.1]

**Cryptanalyze**
To defeat cryptographic mechanisms, and more generally, information security services by the application of mathematical techniques. [NIST SP 800-130]

**Crypto Officer**
an operator or process (subject), acting on behalf of the operator, performing cryptographic initialization or management functions. [NIST FIPS 140-2]

**Cryptographic**
A well-defined computational procedure that takes variable inputs, including a cryptographic key, and produces an output. [FICAM TFPAP 1.0.1]

**Cryptographic Binding (binding)**
The use of one or more cryptographic techniques by a CKMS to establish a trusted association between a key and selected metadata elements. [NIST SP 800-130]

**Cryptographic Boundary**
an explicitly defined continuous perimeter that establishes the physical bounds of a cryptographic module and contains all the hardware, software, and/or firmware components of a cryptographic module. [NIST FIPS 140-2]

An explicitly-defined perimeter that establishes the boundary of all components of a cryptographic module. [NIST SP 800-130]

**Cryptographic Key**
A value used to control cryptographic operations, such as decryption, encryption, signature generation or signature verification. For the purposes of this document, key requirements shall meet the minimum requirements stated in Table 2 of NIST SP 800-57 Part 1. See also Asymmetric keys, Symmetric key. [NIST SP 800-63-1]

A parameter used in conjunction with a cryptographic algorithm that determines the specific operation of that algorithm. [NIST FIPS 201-2]

a parameter used in conjunction with a cryptographic algorithm that determines the transformation of plaintext data into ciphertext data, the transformation of ciphertext data into plaintext data, a digital signature computed from data, the verification of a digital signature computed from data, an authentication code computed from data, or an exchange agreement of a shared secret. [NIST FIPS 140-2]

A string of bits, integers, or characters that constitute a parameter to a cryptographic algorithm. [NIST SP 800-130]

**Cryptographic Key Component**
a parameter used in conjunction with other key components in an Approved security function to form a plaintext cryptographic key or perform a cryptographic function. [NIST FIPS 140-2]

**Cryptographic Key Management System**
A set of policies, procedures and components that is designed to protect, manage, and distribute cryptographic keys and metadata. [NIST SP 800-130]

A system for the management (e.g., generation, distribution, storage, backup, archive, recovery, use, revocation, and destruction) of cryptographic keys and their metadata. [NIST SP 800-130]

**Cryptographic Module**
The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [FIPS1401] [FBCA CP 2.25]

the set of hardware, software, and/or firmware that implements Approved security functions (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary. [NIST FIPS 140-2]

A set of hardware, software and/or firmware that implements security functions (e.g. cryptographic algorithms and key establishment) and encompasses the cryptographic boundary. [NIST SP 800-130]

The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [FIPS1401] [SAFE-BioPharma CP 2.5]

**Cryptographic Module Security Policy**
a precise specification of the security rules under which a cryptographic module will operate, including the rules derived from the requirements of this standard and additional rules imposed by the vendor. (See Appendix C.) [NIST FIPS 140-2]

**Cryptographic Officer**
An individual authorized to perform cryptographic initialization and management functions on the cryptographic components and devices of a CKMS. [NIST SP 800-130]

**Cryptographic Token**
A token where the secret is a cryptographic key. [NIST SP 800-63-1]

A token for which the secret is a cryptographic key. [Kantara IAF 1100]

**Cryptography**
The use of mathematical techniques to provide security services, such as confidentiality, data integrity, entity authentication, and data origin authentication. [NIST SP 800-130]

**Cryptoperiod**
(undefined) [FBCA CP 2.25]

The time span during which a specific key is authorized for use or in which the keys for a given system or application may remain in effect. [NIST SP 800-130]

**Data**
Any piece of information suitable for use in a computer. [NIST IR 7693]

**Data Integrity**
The property that data has not been altered by an unauthorized entity. [NIST SP 800-63-1]

Assurance that the data are unchanged from creation to reception. [FBCA CP 2.25]

**Data Object**
An item of information seen at the card command interface for which is specified a name a description of logical content, a format, and a coding. [NIST SP 800-73-3 Part 1]

An item of information seen at the card command interface for which are a specified a name, a description of logical content, a format, and a coding. [NIST SP 800-73-3 Part 2]

An item of information seen at the card command interface for which are a specified a name, a description of logical content, a format, and a coding. [NIST SP 800-73-3 Part 3]

An item of information seen at the card command interface for which are a specified a name, a description of logical content, a format, and a coding. [NIST SP 800-73-3 Part 4]

**Data Path**
the physical or logical route over which data passes; a physical data path may be shared by multiple logical data paths. [NIST FIPS 140-2]

**Database**
A repository of information or data, which may or may not be a traditional relational database system. [NIST IR 7693]

**Date Of Birth**
(undefined) [FICAM TFPAP 1.0.1]

**Deactivated State**
The key life cycle state in which a key is not to be used to apply cryptographic protection to data. Under certain circumstances, the key may be used to process already-protected data. [NIST SP 800-130]

**Derived Credential**
A credential issued based on proof of possession and control of a token associated with a previously issued credential, so as not to duplicate the identity proofing process. [NIST SP 800-63-1]

**Designer**
The person or organization having the ability, responsibility, and authority for specifying the devices comprising a new system and how the devices will be structured, coordinated, and operated. [NIST SP 800-130]

**Destroyed Compromised State**
A key life cycle state in which a key cannot be recovered nor used and is marked as compromised. [NIST SP 800-130]

**Destroyed State**
A key life cycle state in which a key cannot be recovered or used. [NIST SP 800-130]

**Differential Power Analysis**
an analysis of the variations of the electrical power consumption of a cryptographic module, using advanced statistical methods and/or other techniques, for the purpose of extracting information correlated to cryptographic keys used in a cryptographic algorithm. [NIST FIPS 140-2]

**Digest**
a cryptographic checksum of an octet stream. [OASIS IMI 1.0]

**Digital Encryption**
Private key data encryption that converts data into a form that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood. In this Profile, encryption pertains to SSL v3 or TLS 1.1 (and higher), encryption and/or XML encryption, depending upon the Level of Assurance. [ICAM SAML 2.0 WB SSO Profile 1.0.2]

**Digital Identity**
a set of Claims made by one party about another party. [OASIS IMI 1.0]

a set of attributes that represent a subject in an online transaction. [NSTIC Strategy]

**Digital Signature**
An asymmetric key operation where the private key is used to digitally sign data and the public key is used to verify the signature. Digital signatures provide authenticity protection, integrity protection, and non-repudiation. [NIST SP 800-63-1]

A value computed with a cryptographic algorithm and appended to a data object in such a way that any recipient of the data can use the signature to verify the data's origin and integrity [RFC 2828]. [FBCA Cross-certification Methodology 3.0]

The result of a transformation of a message by means of a cryptographic system using keys such that a Relying Party can determine: (1) whether the transformation was created using the private key that corresponds to the public key in the signer's digital certificate; and (2) whether the message has been altered since the transformation was made. [FBCA CP 2.25]

1. origin authentication 2. data integrity, and 3. signer non-repudiation. [NIST FIPS 140-2]

A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message, or of the signer of a document. It can also be used to ensure that the original content of the message or document that has been conveyed is unchanged. [InCommon Glossary]

An asymmetric key operation where the private key is used to digitally sign an electronic document and the public key is used to verify the signature. Digital signatures provide authentication and integrity protection. [ICAM SAML 2.0 WB SSO Profile 1.0.2]

**Direct Assertion Model**
The Claimant uses his or her E-authentication token to authenticate to the Verifier. Following successful authentication of the Claimant, the Verifier creates an assertion, and sends it to the Subscriber to be forwarded to the Relying Party. The assertion is used by the Claimant/Subscriber to authenticate to the Relying Party. [FICAM TFPAP 1.0.1]

**Directory**
A database server or other system that provides information, such as a digital certificate or CRL, about an entity whose name is known [RFC 2828]. [FBCA Cross-certification Methodology 3.0]

A directory is a specialized database that may contain information about an institution's membership, groups, roles, devices, systems, services, locations, and other resources. [InCommon Glossary]

**Discovery**
Process of an end user finding a IdP and/or RP. [ICAM SAML 2.0 WB SSO Profile 1.0.2]

**Distinguished Name**
Distinguished names are string representations that uniquely identify users, systems, and organizations. In general, DNs are used in LDAP-compliant directories. In certificate management systems, DNs are used to identify the owner of a certificate and the authority that issued the certificate. [InCommon Glossary]

**Domain Name**
A domain name is that portion of an Internet Uniform Resource Locator (URL) that fully identifies the server program that an Internet request is addressed to. InCommonFederation.org is an example of a domain name. [InCommon Glossary]

**Domain Name Service**
An Internet service that translates domain names to and from IP addresses. [InCommon Glossary]

**Dual Use Certificate**
A certificate that is intended for use with both digital signature and data encryption services. [FBCA CP 2.25]

**Duration**
A field within a certificate which is composed of two subfields; "date of issue" and "date of next issue". [FBCA CP 2.25]

A field within a certificate that is composed of two subfields; "date of issue" and "date of next issue". [SAFE-BioPharma CP 2.5]

**E-authentication Credential**
An object that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a person. [FICAM TFPAP 1.0.1]

**E-commerce**
The use of network technology (especially the internet) to buy or sell goods and services. [FBCA CP 2.25]

The use of network technology (especially the internet) to buy or sell goods and services. [SAFE-BioPharma CP 2.5]

**E-governance Certification Authorities**
Established to support government-wide identity management initiatives. In accordance with EGCA Certificate Policy, the EGCA issues various certificates including certificates for signing metadata. [BAE Overview]

**E-governance Metadata Authority**
Government wide repository for SAML Metadata, representing both SAML and non-SAML endpoints (e.g., OpenID, BAE). EGMA collects, consolidates, validates and publishes metadata for identity and attribute providers that conduct authentication and attribute exchange in accordance with the Trust Framework Provider Adoption Process, ICAM adopted schemes, and this BAE document suite. Despite its role in facilitating metadata distribution, EGMA is not directly involved in authentication or attribute transaction processing. Furthermore, EGMA is not a replacement for Federation or Inter-Federation, but rather is a tool for supporting such activities. [BAE Overview]

**E-governance Trust Services**
E-Governance Trust Services (EGTS) facilitate the use of federated identity in a trusted manner throughout the Federal Government, and between the Federal Government and its partners (i.e., citizens, businesses, and other entities). EGTS includes two complimentary services: . E-Governance Certification Authority (EGCA); and . E-Governance Metadata Authority (EGMA). Both the EGCA and EGMA are technical tools that enable governance, convey trust, and facilitate secure communications within ICAM Federations. [BAE Overview]

**Eavesdropping Attack**
An attack in which an Attacker listens passively to the authentication protocol to capture information which can be used in a subsequent active attack to masquerade as the Claimant. [NIST SP 800-63-1]

**Eduorg**
An LDAP object class authored and promoted by the EDUCAUSE/Internet2 eduPerson Task Force to facilitate the development of inter-institutional applications. The eduOrg object class focuses on the attributes of organizations. Current documentation on the eduOrg object class is available at http://www.educause.edu/eduperson/. [InCommon Glossary]

**Eduperson**
An LDAP object class authored and promoted by the EDUCAUSE/Internet2 eduPerson Task Force to facilitate the development of inter-institutional applications. The eduPerson object class focuses on the attributes of individuals. Current documentation on the eduPerson object class is available at http://www.educause.edu/eduperson/. [InCommon Glossary]

**Electromagnetic Compatibility**
the ability of electronic devices to function satisfactorily in an electromagnetic environment without introducing intolerable electromagnetic disturbances to other devices in that environment. [NIST FIPS 140-2]

**Electromagnetic Interference**
electromagnetic emissions from a device, equipment, or system that interfere with the normal operation of another device, equipment, or system. [NIST FIPS 140-2]

**Electronic Authentication (e-authentication)**
The process of establishing confidence in user identities electronically presented to an information system. [NIST SP 800-63-1]

**Electronic Credentials**
are digital documents that bind an identity or an attribute to a subscriber's token. [Kantara IAF 1100]

Digital documents used in authentication that bind an identity or an attribute to a subscriber's token. [Kantara IAF 1100]

**Electronic Identifier**
A string of characters or structured data that may be used to reference an electronic identity. Examples include an email address, a user account name, a a campus NetID, an employee or student ID, or a PKI certificate. [InCommon Glossary]

**Electronic Identity**
A set of information that is maintained about an individual, typically in campus electronic identity databases. May include roles and privileges as well as personal information. The information must be authoritative to the applications for which it will be used. [InCommon Glossary]

**Electronic Identity Credential**
An electronic identifier and corresponding personal secret associated with an electronic identity. An electronic identity credential typically is issued to the person who is the subject of the information to enable that person to gain access to applications or other resources that need to control such access. [InCommon Glossary]

**Electronic Identity Database**
A structured collection of information pertaining to given individuals. Sometimes referred to as an "enterprise directory". Typically includes name, address, email address, affiliation, and electronic identifier(s). Many technologies can be used to create an identity database, for example LDAP or a set of linked relational databases. [InCommon Glossary]

**Electronic Key Entry**
the entry of cryptographic keys into a cryptographic module using electronic methods such as a smart card or a key-loading device. (The operator of the key may have no knowledge of the value of the key being entered.) [NIST FIPS 140-2]

**Electronic Trust Service**
A service that enhances trust and confidence in electronic transactions, typically but not necessarily using cryptographic techniques or involving confidential material such as PINs and passwords. [Kantara IAF 1100]

**Electronic Trust Service Provider**
An entity that provides one or more electronic trust services. [Kantara IAF 1100]

**Encrypted Key**
a cryptographic key that has been encrypted using an Approved security function with a key encrypting key, a PIN, or a password in order to disguise the value of the underlying plaintext key. [NIST FIPS 140-2]

**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. [FBCA CP 2.25]

**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. [FBCA CP 2.25]

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. [SAFE-BioPharma CP 2.5]

**End Entity**
Relying Parties and Subscribers. [SAFE-BioPharma CP 2.5]

**End User**
A natural person who makes use of resources for application purposes (as opposed to system management purposes; see Administrator, User). [OASIS SAML Glossary 2.0]

**End-entity**
Relying Parties and Subscribers. [FBCA CP 2.25]

**Endpoints**
Entities at each end of a BAE transaction. [BAE Overview]

**Enrolling Agent**
verification and enrollment provider alternate to the primary IDP. [NSTIC Strategy]

**Enrollment Data Set**
(undefined) [NIST FIPS 201-2]

**Enterprise Directory**
An enterprise directory is a core middleware architecture that may provide common authentication, authorization, and attribute services to electronic services offered by an institution. [InCommon Glossary]

**Enterprise Directory Infrastructure**
The infrastructure required to support and maintain an enterprise directory. This may include multiple directory hardware components as well as the processes by which data flows into and out of the directory service. [InCommon Glossary]

**Entity**
For the purposes of this document, "Entity" refers to an organization, corporation, community of interest, or government agency with operational control of a CA. [FBCA CP 2.25]

An individual (person), organization, device or process. An entity has an identifier to which it may be associated. [NIST SP 800-130]

**Entity CA**
A CA that acts on behalf of an Entity, and is under the operational control of an Entity. The Entity may be an organization, corporation, or community of interest. For the Federal Government, an Entity may be any department, subordinate element of a department, or independent organizational entity that is statutorily or constitutionally recognized as being part of the Federal Government. [FBCA CP 2.25]

**Entropy**
A measure of the amount of uncertainty that an Attacker faces to determine the value of a secret. Entropy is usually stated in bits. See Appendix A. [NIST SP 800-63-1]

A measure of the amount of uncertainty that an Attacker faces to determine the value of a secret. Entropy is usually stated in bits. See NIST SP 800-63 for additional information. [FICAM TFPAP 1.0.1]

**Environmental Failure Protection**
the use of features to protect against a compromise of the security of a cryptographic module due to environmental conditions or fluctuations outside of the module's normal operating range. [NIST FIPS 140-2]

**Environmental Failure Testing**
the use of testing to provide a reasonable assurance that the security of a cryptographic module will not be compromised by environmental conditions or fluctuations outside of the module's normal operating range. [NIST FIPS 140-2]

**Error Detection Code**
a code computed from data and comprised of redundant bits of information designed to detect, but not correct, unintentional changes in the data. [NIST FIPS 140-2]

**Extensibility**
A measure of the ease of increasing the capability of a system. [NIST SP 800-130]

**Extensible Markup Language**
Extensible Markup Language, abbreviated XML, describes a class of data objects called XML documents and partially describes the behavior of computer programs which process them. [NIST SP 800-63-1]

Specification developed by the W3C. XML is a pared-down version of SGML, designed especially for Web documents. It allows designers to create their own customized tags, enabling the definition, transmission, validation, and interpretation of data between applications and between organizations. [BAE Overview]

XML is a specification developed by the W3C that enables the definition, transmission, validation, and interpretation of data between applications and between organizations. In a nutshell, XML describes data and focuses on what data is. XML facilitates technical interoperability, and is used in identity management standards such as SAML (e.g., to convey information in a SAML assertion). [ICAM SAML 2.0 WB SSO Profile 1.0.2]

**Extension Identifier**
Any piece of identifying information provided in an asset identification element that is not explicitly defined in the Asset Identification schema. [NIST IR 7693]

**FBCA Management Authority**
The Federal Public Key Infrastructure Management Authority is the organization selected by the Federal Public Key Infrastructure Policy Authority to be responsible for operating the Federal Bridge Certification Authority. [FBCA CP 2.25]

**Federal Agency Smart Credential - Number**
The FASC-N is the primary identification string to be used on all government issued credentials. [BAE Overview]

**Federal Agency Smart Credential Number**
As required by FIPS 201, one of the primary identifiers on the PIV Card for physical access control. The FASC-N is a fixed length (25 byte) data object, specified in [SP 800-73], and included in several data objects on a PIV Card. [NIST FIPS 201-2]

**Federal Bridge Certification Authority**
The FBCA is the entity operated by the Federal Public Key Infrastructure (FPKI) Management Authority that is authorized by the Federal PKI Policy Authority to create, sign, and issue public key certificates to Principal CAs. [NIST SP 800-63-1]

the U.S. Federal Government's mechanism for enabling trust domain interoperability at a level of assurance satisfying E-Authentication levels 1 through 4 using public key certificates. [FBCA Cross-certification Methodology 3.0]

**Federal Chief Information Officers Council**
(undefined) [FICAM TFPAP 1.0.1]

**Federal Identity, Credentialing And Access Management**
Government-wide initiative whose goal is a consolidated approach for all government-wide identity, credential and access management activities to ensure alignment, clarity, and interoperability. FICAM provides a common segment architecture and implementation guidance for use by federal agencies as they continue to invest in ICAM programs. [BAE Overview]

**Federal Information Processing Standard**
Under the Information Technology Management Reform Act (Public Law 104-106), the Secretary of Commerce approves standards and guidelines that are developed by the National Institute of Standards and Technology (NIST) for Federal computer systems. These standards and guidelines are issued by NIST as Federal Information Processing Standards (FIPS) for use government-wide. NIST develops FIPS when there are compelling Federal government requirements such as for security and interoperability and there are no acceptable industry standards or solutions. See background information for more details. FIPS documents are available online through the FIPS home page: http://www.nist.gov/itl/fips.cfm [NIST SP 800-63-1]

**Federal Information Processing Standards**
(undefined) [FICAM TFPAP 1.0.1]

A standard for adoption and use by Federal departments and agencies that has been developed within the Information Technology Laboratory and published by NIST, a part of the U.S. Department of Commerce. A FIPS covers some topic in information technology to achieve a common level of quality or some level of interoperability. [NIST FIPS 201-2]

Standards and guidelines issued by the National Institute of Standards and Technology (NIST) for use government-wide in the United States. NIST develops FIPS when the U.S. Federal government has compelling requirements, such as for security and interoperability, for which no industry standards or solutions are acceptable. [Kantara IAF 1100]

**Federal Information Security Management Act**
Title III of the E-Government Act requiring each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. [NIST SP 800-63-1]

**Federal Public Key Infrastructure**
(undefined) [FICAM TFPAP 1.0.1]

**Federal Public Key Infrastructure Management Authority**
Provides the best and most cost-effective FPKI Trust Infrastructure services in support of organizations meeting their identity management and data security goals. The FPKIMA's primary focus is to ensure that common identity and access management policies for secure physical and logical access, document sharing, and communications across Federal agencies and between external business partners are realized through the execution and management of digital certificate policies and standards. [BAE Overview]

**Federal Public Key Infrastructure Policy Authority**
The FPKIPA is a federal government body responsible for setting, implementing, and administering policy decisions regarding inter Entity PKI interoperability that uses the FBCA. [FBCA CP 2.25]

**Federate**
To link or bind two or more entities together [Merriam]. Federation This term is used in two senses in SAML: a) The act of establishing a relationship between two entities [Merriam]. b) An association comprising any number of service providers and identity providers. [OASIS SAML Glossary 2.0]

**Federated Identity**
The management of identity information between members of a federation. [InCommon Glossary]

A principal's identity is said to be federated between a set of Providers when there is an agreement between the providers on a set of identifiers and/or attributes to use to refer to the Principal [OASIS SAML Glossary 2.0]

**Federated Identity Management**
A system that allows individuals to use the same user name, password, or other personal identification to sign on to the networks of more than one enterprise in order to conduct transactions. [Kantara IAF 1100]

**Federation**
A federation is an association of organizations that come together to exchange information as appropriate about their users and resources in order to enable collaborations and transactions. [InCommon Glossary]

**Federation Operating Policies And Practices**
(undefined) [InCommon IAAF 1.1]

**Federation Operation Policies And Practices**
The policies and practices the Federation operates under on a day-to-day basis. This document describes the activities of the Federation organization, the process of Participants applying and being accepted, etc., and how decisions are made. [InCommon Glossary]

**Federation Operator**
An individual or group that defines standards for its respective federation, or trust community and evaluates participation in the community or network to ensure compliance with policy, including the ability to request audits of participants for verification. FIPS See Federal Information Processing Standards. [Kantara IAF 1100]

**Finite State Model**
a mathematical model of a sequential machine that is comprised of a finite set of input events, a finite set of output events, a finite set of states, a function that maps states and input to output, a function that maps states and inputs to states (a state transition function), and a specification that describes the initial state. [NIST FIPS 140-2]

**Firewall**
Gateway that limits access between networks in accordance withlocal security policy. [NS4009] [FBCA CP 2.25]

The process integrated with a computer operating system that detects and prevents undesirable applications and remote users from accessing or performing operations on a secure computer. [NIST SP 800-130]

Gateway that limits access between networks in accordance with local security policy. [SAFE-BioPharma CP 2.5]

**Firmware**
the programs and data components of a cryptographic module that are stored in hardware (e.g., ROM, PROM, EPROM, EEPROM or FLASH) within the cryptographic boundary and cannot be dynamically written or modified during execution. [NIST FIPS 140-2]

**Formal Language**
A language whose syntax (i.e., rules for creating correct sentences with proper structure) is defined such that the rules are unambiguous and all syntactically correct sentences of the language can be recognized as being correct by an automaton (e.g., a computer running a syntax-analysis application program). [NIST SP 800-130]

**Framework**
A description of the policies, procedures, components, and devices that are used to create a CKMS. [NIST SP 800-130]

**Front Channel**
Front channel refers to the "communications channel" that can be effected between two HTTP-speaking servers by employing "HTTP redirect" messages and thus passing messages to each other via a user agent, e.g. a web browser, or any other HTTP client [RFC2616]. See also back channel. [OASIS SAML Glossary 2.0]

**Full Legal Name**
A person's name that is usually the name given at birth and recorded on the birth certificate but that may be a different name that is used by a person consistently and independently or that has been declared the person's name by a court. That is, the name one has for official purposes; not a nickname or pseudonym. [FICAM TFPAP 1.0.1]

**Garbled**
The modification of data (e.g., a cryptographic key) in which one or more of its elements (e.g., bit, digit, character) has been changed or destroyed. [NIST SP 800-130]

**General Services Administration**
(undefined) [FICAM TFPAP 1.0.1]

**Generate Key**
The key and metadata management function used to compute or create a cryptographic key. [NIST SP 800-130]

**Governance**
BAE governance ensures trust and reliable technical interoperation between all endpoints involved in a BAE transaction. Given the federated nature of BAE (i.e., inter-organization processing), governance is the responsibility of each participating community of interest. The essential governance functions are: 1. Managing Metadata; and 2. Issuing Certificates. [BAE Overview]

**Grant (of Rights Ofuse)**
The Granting, by the Kantara Initiative Board of Trustees (KIBoT) or another authoritative body to which the KIBoT has given a delegated authority (itself via a Grant), to use of the Kantara Initiative Mark for a specific Grant Category. [Kantara IAF 1100]

**Grant Category**
One of the specific purposes for which the Kantara Initiative Mark may be used by a third party, being one of: Approved Service; Accredited Assessor; Service Approval Authority (futurework focus); or Certified Federation Operator. [Kantara IAF 1100]

**Grantee**
An organization to which a Grant of Rights of Use of the Kantara Initiative Mark has been awarded. [Kantara IAF 1100]

**Guessing Entropy**
A measure of the difficulty that an Attacker has to guess the average password used in a system. In this document, entropy is stated in bits. When a password has n-bits of guessing entropy then an Attacker has as much difficulty guessing the average password as in guessing an n-bit random quantity. The Attacker is assumed to know the actual password frequency distribution. See Appendix A. [NIST SP 800-63-1]

**Guide**
document published by ISO or IEC giving rules, orientation, advice or recommendations relating to international standardization [ISO-IEC Directives Part 2]

**Handle**
A reference assigned to a user for the purpose of retrieving attributes about the user. The handle is not in any way linked to the identity of the user. [InCommon Glossary]

**Handle Service**
The Identity Provider component responsible for (indirectly) providing a handle to be used for making user attribute requests to an Identity Provider Attribute Authority. [InCommon Glossary]

**Handle Service Subject DN**
The distinguished name of the Handle Service. [InCommon Glossary]

**Handle Service URL**
The Internet address of the Handle Service. [InCommon Glossary]

**Hardening**
A process to eliminate a means of attack by patching vulnerabilities and turning off nonessential services. Hardening a computer involves several steps to form layers of protection. [NIST SP 800-130]

**Hardware**
the physical equipment within the cryptographic boundary used to process programs and data. [NIST FIPS 140-2]

**Hash Function**
A function that maps a bit string of arbitrary length to a fixed length bit string. Approved hash functions satisfy the following properties: 1. (One-way) It is computationally infeasible to find any input that maps to any pre-specified output, and 2. (Collision resistant) It is computationally infeasible to find any two distinct inputs that map to the same output. [NIST SP 800-63-1]

A function that maps a bit string of arbitrary length to a fixed length bit string. Secure hash functions [FIPS180] satisfy the following properties: One-Way It is computationally infeasible to find any input that maps to any pre-specified output. Collision Resistant It is computationally infeasible to find any two distinct inputs that map to the same output. [NIST FIPS 201-2]

**Hash Value**
The fixed-length bit string produced by a hash function [NIST SP 800-130]

**Hash-based Message Authentication Code**
a message authentication code that utilizes a keyed hash. [NIST FIPS 140-2]

**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. [FBCA CP 2.25]

**Higher Education Institution**
A two- or four-year post-secondary, degree-granting institution that is regionally accredited by an agency on the U.S. Department of Education's list of Regional Institutional Accrediting Agencies (see http://www.incommonfederation.org/accrediting.html). [InCommon Glossary]

**Holder-of-key Assertion**
An assertion that contains a reference to a symmetric key or a public key (corresponding to a private key) held by the Subscriber. The RP may authenticate the Subscriber by verifying that he or she can indeed prove possession and control of the referenced key. [NIST SP 800-63-1]

A holder-of-key assertion contains a reference to a symmetric key or a public key (corresponding to a private key) possessed by the Subscriber. The Relying Party may require the Subscriber to prove possession of the secret that is referenced in the assertion. In proving possession of the Subscriber's secret, the Subscriber also proves that he or she is the rightful owner of the assertion. It is therefore difficult for an Attacker to use a holder-of-key assertion issued to another Subscriber, since the former cannot prove possession of the secret referenced within the assertion [FICAM TFPAP 1.0.1]

A holder-of-key assertion contains a reference to a public key (corresponding to a private key) or a symmetric key possessed by the end user. The RP requires the end user to prove possession of the private key or secret that is referenced in the assertion. In proving possession, the end user also proves that he or she is the rightful owner of the assertion. [ICAM SAML 2.0 WB SSO Profile 1.0.2]

**Homeland Security Presidential Directive**
(undefined) [FICAM TFPAP 1.0.1]

**Host**
An UMA-defined variant of an OAuth resource server that enforces access to the protected resources it hosts, as governed by an authorization manager. [Kantara UMA]

**Human Resources**
(undefined) [InCommon IAAF 1.1]

**Hypertext Transfer Protocol**
Underlying protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. In the Federation, where appropriate, HTTP is used to redirect end users. [BAE Overview]

**INCOMMON BRONZE IDENTITY ASSURANCE PROFILE**
The InCommon Bronze identity assurance profile focuses on sequential identity, that is, reasonable assurance that the same person is authenticating each time with a particular Credential. Assertions under this profile are likely to represent the same Subject each time a Subject identifier is provided. While no identity proofing requirements are specified, it is expected that IdPOs use reasonable care when issuing Credentials to confirm that a single individual applies for and receives a given Credential and its Authentication Secret. InCommon Bronze qualified Assertions are typically usable by individuals seeking access to online information resources licensed to an organization and for which the Subject is an eligible user. They also may be usable for access to online services where the SP will invoke other methods for linking of the Subject identifier to information the SP already has regarding individuals who should have access to its services. [InCommon IAP 1.1]

**INCOMMON SILVER IDENTITY ASSURANCE PROFILE**
The InCommon Silver identity assurance profile builds on the Bronze profile requirements by adding criteria regarding individual Subject identity proofing and identity information records. Stronger Credential technology and Credential management are required as well. The Silver IAP intends to assure a reasonably strong binding between the physical Subject and that Subject's digital Credential, and reasonably accurate information in Assertions. Credentials must at a minimum make use of Authentication Secrets that are sufficiently difficult to guess or intercept. [InCommon IAP 1.1]

**Identification**
The process of discovering the identity (i.e., origin, initial history) of a person or item from the entire collection of similar persons or items. [NIST FIPS 201-2]

Process of using claimed or observed attributes of an individual to infer who the individual is. [Kantara IAF 1100]

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 the context of a PKI, identification refers to two processes: (1) establishing that a given name of an individual or organization corresponds to a real-world identity of an individual or organization, and (2) establishing that an individual or organization applying for or seeking access to something under that name is, in fact, the named individual or organization. A person seeking identification may be a certificate applicant, an applicant for employment in a trusted position within a PKI participant, or a person seeking access to a network or software application, such as a CA administrator seeking access to CA systems. [IETF RFC 3647]

**Identifier**
(undefined) [FICAM TFPAP 1.0.1]

Unique data used to represent a person's identity and associated attributes. A name or a card number are examples of identifiers. [NIST FIPS 201-2]

Something that points to an individual, such as a name, a serial number, or some other pointer to the party being identified. [Kantara IAF 1100]

A text string used to indicate an entity (e.g., one that is performing a key management function) and by the CKMS access control system to select a specific key from a collection of keys. [NIST SP 800-130]

An Identifier is either a "http" or "https" URI, (commonly referred to as a "URL" within this document), or an XRI [XRI_Syntax_2.0]. This document defines various kinds of Identifiers, designed for use in different contexts. [OpenID Authentication 2.0]

This term is used in two senses in SAML: c) One that identifies [Merriam]. d) A data object (for example, a string) mapped to a system entity that uniquely refers to the system entity. A system entity may have multiple distinct identifiers referring to it. An identifier is essentially a "distinguished attribute" of an entity. See also Attribute. [OASIS SAML Glossary 2.0]

**Identifying Information**
The set of an asset?s attributes that may be useful for identifying that asset, including discoverable information about the asset and identifiers assigned to the asset. [NIST IR 7693]

**Identity**
A set of attributes that uniquely describe a person within a given context. [NIST SP 800-63-1]

A unique name of an individual person. Since the legal names of persons are not necessarily unique, the identity of a person must include sufficient additional information (for example an address, or some unique identifier such as an employee or account number) to make the complete name unique. [FICAM TFPAP 1.0.1]

The set of physical and behavioral characteristics by which an individual is uniquely recognizable. [NIST FIPS 201-2]

Information that is true about a Subject. [InCommon IAAF 1.1]

Identity is the set of information associated with a specific physical person or other entity. Usually not all identity attributes are relevant in any given situation. Typically an Identity Provider will be authoritative for only a subset of a person's identity information. [InCommon Glossary]

A unique name for a single person. Because a person's legal name is not necessarily unique, identity must include enough additional information (for example, an address or some unique identifier such as an employee or account number) to make a unique name. [Kantara IAF 1100]

The essence of an entity [Merriam]. One's identity is often described by one's characteristics, among which may be any number of identifiers. See also Identifier, Attribute. [OASIS SAML Glossary 2.0]

**Identity Assurance Assessment Framework**
(undefined) [InCommon IAAF 1.1]

**Identity Assurance Framework**
The body of work that collectively defines the industry-led selfregulatory Framework for electronic trust services in the United States and around the globe, as operated by the Kantara Initiative. The Identity Assurance Framework includes documents which contain descriptions of criteria, rules, procedures, and processes. [Kantara IAF 1100]

**Identity Assurance Profile**
(undefined) [InCommon IAAF 1.1]

**Identity Assurance Qualifier**
(undefined) [InCommon IAAF 1.1]

**Identity Assurance Work Group**
The multi-industry Kantara Initiative partnership working on enabling interoperability among public and private electronic identity authentication systems to foster the adoption of trusted on-line identity services. [Kantara IAF 1100]

**Identity Attributes**
Information elements relevant to a Subject. [InCommon IAAF 1.1]

**Identity Authentication**
Process of establishing an understood level of confidence that an identifier refers to an identity. It may or may not be possible to link the authenticated identity to an individual. [Kantara IAF 1100]

**Identity Binding**
The extent to which an electronic credential can be trusted to be a proxy for the entity named in it. [Kantara IAF 1100]

**Identity Credential**
An electronic identifier and corresponding personal secret associated with an electronic identity. An identity credential typically is issued to the person who is the subject of the information to enable that person to gain access to applications or other resources that need to control such access. [InCommon Glossary]

**Identity Database**
A structured collection of information pertaining to a given individual. Sometimes referred to as an "enterprise directory." Typically includes name, address, email address, affiliation, and electronic identifier(s). Many technologies can be used to create an identity database or set of linked relational databases. [InCommon Glossary]

**Identity Defederation**
The action occurring when Providers agree to stop referring to a Principal via a certain set of identifiers and/or attributes. [OASIS SAML Glossary 2.0]

**Identity Ecosystem**
an online environment where individuals and organizations can trust each other because they follow agreed-upon standards and processes to identify and authenticate their digital identities-and the digital identities of organizations and devices. Similar to ecosystems that exist in nature, it will require disparate organizations and individuals to function together and fulfill unique roles and responsibilities, with an overarching set of standards and rules. The Identity Ecosystem will offer, but will not mandate, stronger identification and authentication while protecting privacy by limiting the amount of information that individuals must disclose. [NSTIC Strategy]

**Identity Ecosystem Framework**
the overarching set of interoperability standards, risk models, privacy and liability policies, requirements, and accountability mechanisms that structure the Identity Ecosystem. [NSTIC Strategy]

**Identity Federation**
The act of creating a federated identity on behalf of a Principal. . [OASIS SAML Glossary 2.0]

**Identity Management**
(undefined) [InCommon IAAF 1.1]

**Identity Management System**
A set of functions serving the Identity and access management needs of an enterprise. [InCommon IAAF 1.1]

A set of standards, procedures and technologies that provide electronic credentials to individuals and maintain authoritative information about the holders of those credentials. [InCommon Glossary]

**Identity Medium**
a device or object (physical or virtual) used for storing one or more credentials, claims, or attributes related to a subject. Identity media are available in many formats, such as smart cards, security chips embedded in personal computers, cell phones, software based certificates, and Universal Serial Bus (USB) devices. Selecting the appropriate identity medium and credential type is implementation-specific and depends on the risk tolerance of the participating entities. [NSTIC Strategy]

**Identity Proofing**
The process by which a CSP and a Registration Authority (RA) collect and verify information about a person for the purpose of issuing credentials to that person. [NIST SP 800-63-1]

The process by which a CSP and an RA validate sufficient information to uniquely identify a person. [FICAM TFPAP 1.0.1]

The process of providing sufficient information (e.g., identity history, credentials, documents) to establish an identity. [NIST FIPS 201-2]

The process by which identity related information is validated so as to identify a person with a degree of uniqueness and certitude sufficient for the purposes for which that identity is to be used. [Kantara IAF 1100]

**Identity Proofing Policy**
A set of rules that defines identity proofing requirements (required evidence, format, manner of presentation, validation), records actions required of the registrar, and describes any other salient aspects of the identity proofing function that are applicable to a particular community or class of applications with common security requirements. An identity proofing policy is designed to accomplish a stated assurance level. [Kantara IAF 1100]

**Identity Proofing Practice Statement**
A statement of the practices that an identity proofing service provider employs in providing its services in accordance with the applicable identity proofing policy. [Kantara IAF 1100]

**Identity Proofing Service Provider**
An electronic trust service provider which offers, as a standalone service, the specific electronic trust service of identity proofing. This service provider is sometimes referred to as a Registration Agent/Authority (RA). [Kantara IAF 1100]

**Identity Provider**
A trusted entity that issues or registers subscriber tokens and issues electronic credentials to subscribers. The Identity Provider may encompass Registration Authorities and verifiers that it operates. An Identity Provider may be an independent third party, or may issue credentials for its own use. [FICAM TFPAP 1.0.1]

The IdMS system component that issues Assertions. [InCommon IAAF 1.1]

a network entity providing the Digital Identity claims used by a Relying Party. [OASIS IMI 1.0]

The originating location for a user. Previously called the Origin Site in the Shibboleth software implementation. For InCommon, an IdP is a campus or other organization that manages and operates an identity management system and offers information about members of its community to other InCommon participants. [InCommon Glossary]

[organization] responsible for establishing, maintaining, and securing the digital identity associated with that subject. These processes include revoking, suspending, and restoring the subject's digital identity if necessary. The identity provider may also verify the identity of and sign up (enroll) a subject. IDPs issue credentials. [NSTIC Strategy]

A kind of service provider that creates, maintains, and manages identity information for principals and provides principal authentication to other service providers (relying parties) within a federation, such as with web browser profiles. [ICAM SAML 2.0 WB SSO Profile 1.0.2]

A kind of service provider that creates, maintains, and manages identity information for principals and provides principal authentication to other service providers within a federation, such as with web browser profiles. [OASIS SAML Glossary 2.0]

**Identity Provider Security Token Service**
the Security Token Service run by an Identity Provider to issue tokens. [OASIS IMI 1.0]

**Identity Registration**
The process of making a person's identity known to the PIV system, associating a unique identifier with that identity, and collecting and recording the person's relevant attributes into the system. [NIST FIPS 201-2]

**Identity Selector**
a software component available to the Service Requester through which the user controls and dispatches her Digital Identities. [OASIS IMI 1.0]

**Identity Verification**
The process of confirming or denying that a claimed identity is correct by comparing the credentials (something you know, something you have, something you are) of a person requesting access with those previously proven and stored in the PIV Card or system and associated with the identity being claimed. [NIST FIPS 201-2]

**Identity, Credential, And Access Management**
(undefined) [FICAM TFPAP 1.0.1]

**Identity, Credential, And Access Management Sub Committee**
(undefined) [FICAM TFPAP 1.0.1]

**Idms Database**
A database of IdMS Subjects. [InCommon IAAF 1.1]

**Idms Operations**
The technical environment supporting the IdMS. [InCommon IAAF 1.1]

**Idp Operator**
The organization operating an IdP is an IdP Operator. [InCommon IAAF 1.1]

**Immediately**
In accordance with an expedient and well defined process. [SAFE-BioPharma CP 2.5]

**Incommon CA Root Profile**
The description of attributes and the data required to authenticate under the InCommon Certificate Authority (CA). [InCommon Glossary]

**Incommon Federation**
InCommon is a formal federation of organizations focused on creating a common framework for trust in support of research and education. The primary purpose of the InCommon federation is to facilitate collaboration through the sharing of protected network-accessible resources by means of an agreed-upon common trust fabric. InCommon participation is separate from membership in Internet2. [InCommon Glossary]

**Incommon Technical Advisory Committee**
Group of individuals that provide technical guidance and direction for InCommon. [InCommon Glossary]

**Indirect Assertion Model**
In the indirect model, the Claimant uses his or her token to authenticate to the Verifier. Following successful authentication, the Verifier creates an assertion as well as an assertion reference (which identifies the Verifier and includes a pointer to the full assertion held by the Verifier). The assertion reference is sent to the Subscriber to be forwarded to the Relying Party. In this model, the assertion reference is used by the Claimant/Subscriber to authenticate to the Relying Party. The Relying Party then uses the assertion reference to explicitly request the assertion from the Verifier. [FICAM TFPAP 1.0.1]

**Individual**
a person engaged in an online transaction. Individuals are the first priority of the Strategy [NSTIC Strategy]

**Information Card**
provides a visual representation of a Digital Identity for the end user. Information Cards contain a reference to an IP/STS that issues Security Tokens containing the Claims for that Digital Identity. [OASIS IMI 1.0]

**Information Card Model**
refers to the use of Information Cards containing metadata for obtaining Digital Identity claims from Identity Providers and then conveying them to Relying Parties under user control. [OASIS IMI 1.0]

**Information Security And Identity Management Committee**
(undefined) [FICAM TFPAP 1.0.1]

**Information Security Management Systems (ISMS)**
A system of management concerned with information security.The key concept of ISMS is the design, implement, and maintain a coherent suite of processes and systems for effectively managing information security, thus ensuring the confidentiality, integrity, and availability of information assets and minimizing information security risks. [Kantara IAF 1100]

**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. [NS4009] [FBCA CP 2.25]

**Information Technology**
(undefined) [FICAM TFPAP 1.0.1]

**Initial SOAP Sender**
The SOAP sender that originates a SOAP message at the starting point of a SOAP message path. [WSGloss] [OASIS SAML Glossary 2.0]

**Initialization Vector**
a vector used in defining the starting point of an encryption process within a cryptographic algorithm. [NIST FIPS 140-2]

**Input Data**
information that is entered into a cryptographic module for the purposes of transformation or computation using an Approved security function. [NIST FIPS 140-2]

**Inqueue**
InQueue is a federation of organizations who are interested in using the Shibboleth technology and exploring how federations work prior to joining a production federation such as InCommon. Participation in InQueue is open to any technically qualifying organization. http://inqueue.internet2.edu/ [InCommon Glossary]

**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. [FBCA CP 2.25]

**Integrity**
Protection against unauthorized modification or destruction of information. [NS4009]. 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. [FBCA CP 2.25]

The property that data has not been altered by an unauthorized entity. [FICAM TFPAP 1.0.1]

the property that sensitive data has not been modified or deleted in an unauthorized and undetected manner. [NIST FIPS 140-2]

the process by which it is guaranteed that information is not modified in transit. [OASIS IMI 1.0]

Protection against unauthorized modification or destruction of information. [NS4009]. 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. [SAFE-BioPharma CP 2.5]

**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. [FBCA CP 2.25]

Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation. [SAFE-BioPharma CP 2.5]

**Interface**
a logical entry or exit point of a cryptographic module that provides access to the module for logical information flows representing physical signals. [NIST FIPS 140-2]

**Interface Device**
Synonym for card interface device. [NIST SP 800-73-3 Part 1]

Synonym for card interface device. [NIST SP 800-73-3 Part 3]

**Intermediate CA**
A CA that is subordinate to another CA, and has a CA subordinate to itself. [FBCA CP 2.25]

**International Standard**
standard that is adopted by an international standardizing/standards organization and made available to the public [ISO-IEC Directives Part 2]

international standard where the international standards organization is ISO or IEC [ISO-IEC Directives Part 2]

**Interoperability**
For the purposes of this Standard, interoperability allows any government facility or information system, regardless of the issuer, to verify a cardholder's identity using the credentials on the PIV Card. [NIST FIPS 201-2]

A measure of the ability of one set of entities to physically connect to and logically communicate with another set of entities. [NIST SP 800-130]

**Interoperability Test**
Interoperability tests measure the performance associated with the use of standardized biometric data records ina multiple vendor environment. It involves the production of the templates by N enrollment products and authentication of the against images processed by M others. [NIST SP 800-85B]

**Issuance**
Delivery of token or credential to the subscriber of an Identity Provider. [FICAM TFPAP 1.0.1]

**Issuer**
The organization that is issuing the PIV Card to an applicant. Typically this is an organization for which the applicant is working. [NIST FIPS 201-2]

The CA that issues a certificate. [InCommon Glossary]

Somebody or something that supplies or distributes something officially. [Kantara IAF 1100]

**Issuing Certification Authority (issuing CA)**
In the context of a particular certificate, the issuing CA is the CA that issued the certificate (see also Subject certification authority). [IETF RFC 3647]

**Kantara Initiative Board Of Trustees**
The Kantara Initiative Board of Trustees (KIBoT) is comprised of trustee-level members of the Kantara Initiative, who have the responsibility of reviewing ARB recommendations and awarding the Kantara Initiative Mark to applying assessors and CSPs. [Kantara IAF 1100]

**Kantara Initiative Mark**
A symbol of trustworthy identity and credential management services at specified Assurance Levels, awarded by the Kantara Initiative Board of Trustees. [Kantara IAF 1100]

**Kantara Trust Status List**
Online record of Accredited Assessors and Certified Services, maintained on the Kantara Initiative website, listing organizations and services that have received the Kantara Initiative Mark and the associated assurance levels achieved. [Kantara IAF 1100]

**Kantara-accredited Service**
A service which has applied for accreditation and completed a certified assessment at the specified assurance level(s). [Kantara IAF 1100]

**Kantara-approved Assessor**
A body that has been granted an accreditation to perform assessments against Service Assessment Criteria, at the specified assurance level(s). [Kantara IAF 1100]

**Kerberos**
A widely used authentication protocol developed at MIT. In "classic" Kerberos, users share a secret password with a Key Distribution Center (KDC). The user, Alice, who wishes to communicate with another user, Bob, authenticates to the KDC and is furnished a "ticket" by the KDC to use to authenticate with Bob. When Kerberos authentication is based on passwords, the protocol is known to be vulnerable to off-line dictionary attacks by eavesdroppers who capture the initial user-to- KDC exchange. Longer password length and complexity provide some mitigation to this vulnerability, although sufficiently long passwords tend to be cumbersome for users. [NIST SP 800-63-1]

**Key**
(undefined) [NIST FIPS 201-2]

**Key Agreement**
A key establishment procedure where the resultant keying material is a function of information contributed by two or more participants, so that no entity can predetermine the resulting value of the keying material independently of any other entity's contribution. [NIST SP 800-130]

**Key Confirmation**
A procedure to provide assurance to one entity (the key confirmation recipient) that another entity (the key confirmation provider) actually possesses the correct secret keying material and/or shared secret. [NIST SP 800-130]

**Key Encrypting Key**
a cryptographic key that is used for the encryption or decryption of other keys. [NIST FIPS 140-2]

**Key Entry**
The process by which a key (and perhaps its metadata) is entered into a cryptographic module in preparation for active use. [NIST SP 800-130]

**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. [adapted from ABADSG, "Commercial key escrow service"] [FBCA CP 2.25]

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. [adapted from ABADSG, "Commercial key escrow service"] [SAFE-BioPharma CP 2.5]

**Key Establishment**
the process by which cryptographic keys are securely distributed among cryptographic modules using manual transport methods (e.g., key loaders), automated methods (e.g., key transport and/or key agreement protocols), or a combination of automated and manual methods (consists of key transport plus key agreement). [NIST FIPS 140-2]

The process by which a key is securely shared between two or more entities, either by transporting a key from one entity to another (key transport) or deriving a key from information shared by the entities (key agreement). [NIST SP 800-130]

**Key Exchange**
The process of exchanging public keys in order to establish secure communications. [FBCA CP 2.25]

**Key Generation Material**
Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys. [FBCA CP 2.25]

**Key Label**
A key label is a text string that provides a human-readable and perhaps machine-readable set of descriptors for the key. Hypothetical examples of key labels include: "Root CA Private Key 2009-29"; "Maintenance Secret Key 2005." [NIST SP 800-130]

**Key Life Cycle State**
One of the set of finite states that describes the accepted use of a cryptographic key at a given point in its lifetime, including: Pre-Activation; Active; Suspended; Deactivated; Revoked; Compromised; Destroyed; Destroyed Compromised. [NIST SP 800-130]

**Key Loader**
a self-contained unit that is capable of storing at least one plaintext or encrypted cryptographic key or key component that can be transferred, upon request, into a cryptographic module. [NIST FIPS 140-2]

**Key Management**
the activities involving the handling of cryptographic keys and other related security parameters (e.g., IVs and passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and zeroization. [NIST FIPS 140-2]

**Key Output**
The process by which a key (and perhaps its metadata) are extracted from a cryptographic module (usually for extermal storage). [NIST SP 800-130]

**Key Owner**
An entity (e.g., person, group, organization, device, or module) authorized to use a cryptographic key or key pair. [NIST SP 800-130]

**Key Pair**
Two mathematically related keys having the properties that (1) one key can be used to encrypt a message that can only be decrypted using the other key, and (ii) even knowing one key, it is computationally infeasible to discover the other key. [FBCA CP 2.25]

**Key Reference**
A key reference is a one-byte identifier that specifies a cryptographic key according to its PIV Key Type. The identifier is part of the cryptographic material used ina cryptographic protocol, such as an authentication or signing protocol. [NIST SP 800-73-3 Part 1]

A PIV key reference is a one-byte identifier that specifies a cryptographic key according to its PIV Key Type. The identifier is part of cryptographic material used ina cryptographic protocol such as an authentication or a signing protocol. [NIST SP 800-73-3 Part 2]

A PIV key reference is a one-byte identifier that specifies a cryptographic key according to its PIV Key Type. The identifier is part of cryptographic material used ina cryptographic protocol such as an authentication or a signing protocol. [NIST SP 800-73-3 Part 3]

**Key Split**
A parameter that, when properly combined with one or more other key splits, forms a cryptographic key. [NIST SP 800-130]

**Key State Transition**
The process of moving from one key life cycle state to another. [NIST SP 800-130]

**Key Transport**
secure transport of cryptographic keys from one cryptographic module to another module. [NIST FIPS 140-2]

A key establishment procedure whereby one entity (the sender) selects and encrypts the keying material and then distributes the material to another entity (the receiver). [NIST SP 800-130]

**Key Update**
The process used to replace a previously active key with a new key that is related to the old key. [NIST SP 800-130]

**Key Wrapping**
A method of encrypting keys (along with associated integrity information) that provides both confidentiality and integrity protection using a symmetric key. [NIST SP 800-130]

**Knowledge Based Authentication**
Authentication of an individual based on knowledge of information associated with his or her claimed identity in public databases. Knowledge of such information is considered to be private rather than secret, because it may be used in contexts other than authentication to a Verifier, thereby reducing the overall assurance associated with the authentication process. [NIST SP 800-63-1]

**LDAP Directory**
An LDAP directory is one that supports the Lightweight Directory Access Protocol (LDAP). LDAP is a widely adopted IETF standard directory access protocol well suited to the authentication and authorization needs of modern application architectures. [InCommon Glossary]

**Least Privilege**
The principle that each entity has access only to the information and resources necessary for legitimate use. [NIST SP 800-130]

**Level Of Assurance**
In the context of OMB M-04-04 and this document, assurance is defined as 1) the degree of confidence in the vetting process used to establish the identity of an individual to whom the credential was issued, and 2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued. [FICAM TFPAP 1.0.1]

**Liberty Alliance**
A consortium of technology and consumer-facing organizations, formed in September 2001 to establish an open standard for federated network identity. http://www.projectliberty.org/ [InCommon Glossary]

**Lightweight Directory Access Protocol**
An IETF standard for directory services. [InCommon Glossary]

**Lightweight Directory Inter-exchange Format**
A protocol for exchange of information among LDAP directories. [InCommon Glossary]

**Local Registration**
A Registration Authority with responsibility for a local community.Authority (LRA) [FBCA CP 2.25]

**Local Registration Authority (LRA)**
A Registration Authority with responsibility for a local community. [SAFE-BioPharma CP 2.5]

**Locale Identifier**
The BAE Architecture supports both Direct and Brokered Attribute Exchange Models. In order to retrieve the attributes of subjects who are in remote domains, it is critical that sufficient information be made available to the Requesting BAE Broker to enable it to route the query to a BAE Broker that is authoritative for the attributes of the Subject. The BAE specification uses the term Locale Identifier (LI) to define the routing information that is embedded within the unique identifier assigned to a BAE Requester and/or Responder. [BAE Overview]

**Locally Unique Identifier**
In order to query an attribute service to retrieve the information about a Subject, it is necessary to utilize an identifier that is unique across the domain in which the Subject exists. The BAE specification uses the term Locally Unique Identifier (LUID) to define this identifier. The BAE architecture has the ability to support multiple LUID formats. [BAE Overview]

**Login, Logon, Sign-on**
The process whereby a user presents credentials to an authentication authority, establishes a simple session, and optionally establishes a rich session. [OASIS SAML Glossary 2.0]

**Logout, Logoff, Sign-off**
The process whereby a user signifies desire to terminate a simple session or rich session. [OASIS SAML Glossary 2.0]

**MSCUID**
An optional legacy identifier included for compatibility with Common Access Card and Government Smart Card Interoperability Specifications. [NIST SP 800-73-3 Part 1]

**Malware**
Software designed and operated by an adversary to violate the security of a computer (includes spyware, virus programs, root kits, and Trojan horses) [NIST SP 800-130]

**Man-in-the-middle Attack**
An attack on the authentication protocol run in which the Attacker positions himself or herself in between the Claimant and Verifier so that he can intercept and alter data traveling between them. [NIST SP 800-63-1]

**Mandatory Element**
element the presence of which in a document is obligatory [ISO-IEC Directives Part 2]

**Manual Key Entry**
the entry of cryptographic keys into a cryptographic module, using devices such as a keyboard. [NIST FIPS 140-2]

**Manual Key Transport**
a non-electronic means of transporting cryptographic keys. [NIST FIPS 140-2]

**Markup Language**
A set of XML elements and XML attributes to be applied to the structure of an XML document for a specific purpose. A markup language is typically defined by means of a set of XML schemas and accompanying documentation. For example, the Security Assertion Markup Language (SAML) is defined by two schemas and a set of normative SAML specification text. [OASIS SAML Glossary 2.0]

**Match**
The process of comparing biometric information against a previously stored biometric data and scoring the level of similarity. [NIST FIPS 201-2]

**Matching**
The process of determining whether two or more asset identification expressions refer to the same asset. [NIST IR 7693]

**Memorandum Of Agreement**
Agreement between the FPKIPA and an Entity allowing interoperability between the Entity Principal CA and the FBCA. [FBCA CP 2.25]

**Message Authentication Code**
A cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of the data. MACs provide authenticity and integrity protection, but not non-repudiation protection. [NIST SP 800-63-1]

**Metadata**
Message exchange between two BAE entities requires each to have specific knowledge about the other. One example is the URL of each entity a BAE Broker technically interoperates. Without such knowledge, a BAE Broker does not know where to send messages for processing. Metadata describes and conveys such information. Metadata is the primary means of trust within Federal ICAM. Signed metadata is used to bind ICAM members to their digital signature and encryption keys. [BAE Overview]

Data about data, or information known about an object in order to provide access to the object. Usually includes information about intellectual content, digital representation data, and security or rights management information. [InCommon Glossary]

In the Framework, information used to describe specific characteristics, constraints, acceptable uses, and parameters associated with a cryptographic key that is explicitly recorded and managed by the CKMS. [NIST SP 800-130]

Information shared between endpoints (e.g., RP, IdP) necessary for technical interoperation. [ICAM SAML 2.0 WB SSO Profile 1.0.2]

**Metadata Authority**
Entity that oversees and facilitates the overall metadata exchange process, including but not limited to metadata collection, validation, and distribution in a secure, confidential manner. See also E-Governance Trust Services (EGTS) and E-Governance Metadata Authority (EGMA). [BAE Overview]

**Metadata Element**
One unit of metadata that is associated with a key and explicitly recorded and managed by the CKMS. [NIST SP 800-130]

**Microcode**
the elementary processor instructions that correspond to an executable program instruction. [NIST FIPS 140-2]

**Min-entropy**
A measure of the difficulty that an Attacker has to guess the most commonly chosen password used in a system. In this document, entropy is stated in bits. When a password has n-bits of min-entropy then an Attacker requires as many trials to find a user with that password as is needed to guess an n-bit random quantity. The Attacker is assumed to know the most commonly used password(s). See Appendix A. [NIST SP 800-63-1]

A measure of the difficulty that an Attacker has to guess the most commonly chosen password used in a system. In this document, entropy is stated in bits. When a password has n-bits of min-entropy then an Attacker requires as many trials to find a user with that password as is needed to guess an n-bit random quantity. The Attacker is assumed to know the most commonly used password(s). See NIST SP 800-63 for additional information. [FICAM TFPAP 1.0.1]

**Mission Support Information**
Information that is important to the support of deployed and contingency forces. [FBCA CP 2.25]

**Mode Of Operation**
A set of rules for operating on data with a cryptographic algorithm and a key; often includes feeding all or part of the output of the algorithm back into the input of the next iteration of the algorithm, either with or without additional data being processed. Examples are: Cipher Feedback, Output Feedback, and Cipher Block Chaining. [NIST SP 800-130]

**Model**
A very detailed description or scaled representation of one component of a larger system that can be created, operated, and analyzed to predict actual operational characteristics of the final produced component. [NIST FIPS 201-2]

**Multi-factor**
A characteristic of an authentication system or a token that uses more than one authentication factor. The three types of authentication factors are something you know, something you have, and something you are. [NIST SP 800-63-1]

**Multi-factor Authentication**
Use of two or more of he following: 1. Something you know (for example, a password) 2. Something you have (for example, an ID badge or a cryptographic key) 3. Something you are (for example, a thumb print or other biometric data) Authentication systems that incorporate all three factors are stronger than systems that only incorporate one or two of the factors. [FICAM TFPAP 1.0.1]

**Multi-token Authentication**
Two or more tokens are required to verify the identity of the Claimant. [FICAM TFPAP 1.0.1]

**Mutual Authentication**
Occurs when parties at both ends of a communication activity authenticate each other (see authentication). [FBCA CP 2.25]

**Name Qualifier**
A string that disambiguates an identifier that may be used in more than one namespace (in the federated sense) to represent different principals. [OASIS SAML Glossary 2.0]

**Namespace**
A set of names in which all names are unique. [InCommon Glossary]

This term is used in several senses in SAML: e) (In discussing federated names) A domain in which an identifier is unique in representing a single principal. f) (With respect to authorization decision actions) A URI that identifies the set of action values from which the supplied action comes. g) (In XML) See XML namespace. [OASIS SAML Glossary 2.0]

**Naming Authority**
An organizational entity responsible for assigning distinguished names (DNs) and for assuring that each DN is meaningful and unique within its domain. [FBCA CP 2.25]

**National Institute Of Standards And Technology**
(undefined) [FICAM TFPAP 1.0.1]

**National Security System**
(undefined) [FBCA CP 2.25]

**Netid**
An electronic identifier created specifically for use with on-line applications, often an integer and typically with no other meaning. [InCommon Glossary]

**Network**
An open communications medium, typically the Internet, that is used to transport messages between the Claimant and other parties. Unless otherwise stated, no assumptions are made about the security of the network; it is assumed to be open and subject to active (i.e., impersonation, man-in-the-middle, session hijacking) and passive (i.e., eavesdropping) attack at any point between the parties (e.g., Claimant, Verifier, CSP or RP). [NIST SP 800-63-1]

An open communications medium, typically the Internet, that is used to transport messages between the Claimant and other parties. [FICAM TFPAP 1.0.1]

An open communications medium, typically the Internet, that is used to transport messages between the claimant and other parties. [Kantara IAF 1100]

An information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices. [NIST IR 7693]

**Non-person Entity**
[entities that] may also require authentication in the Identity Ecosystem. NPEs can be organizations, hardware, networks, software, or services and are treated much like individuals within the Identity Ecosystem NPEs may engage in or support a transaction. [NSTIC Strategy]

**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. [NS4009] 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 private signature key. Legal non-repudiation refers to how well possession or control of the private signature key can be established. [FBCA CP 2.25]

Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information. [FICAM TFPAP 1.0.1]

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. [SAFE-BioPharma CP 2.5]

**Nonce**
A value used in security protocols that is never repeated with the same key. For example, nonces used as challenges in challenge-response authentication protocols must not be repeated until authentication keys are changed. Otherwise, there is a possibility of a replay attack. Using a nonce as a challenge is a different requirement than a random challenge, because a nonce is not necessarily unpredictable. [NIST SP 800-63-1]

A value used in security protocols that is never repeated with the same key. For example, challenges used in challenge-response authentication protocols generally must not be repeated until authentication keys are changed, or there is a possibility of a replay attack. Using a nonce as a challenge is a different requirement than a random challenge, because a nonce is not necessarily unpredictable. [FICAM TFPAP 1.0.1]

**Normative Element**
element that describes the scope of the document or sets out provisions [ISO-IEC Directives Part 2]

**OP Endpoint URL**
The URL which accepts OpenID Authentication protocol messages, obtained by performing discovery on the User-Supplied Identifier. This value MUST be an absolute HTTP or HTTPS URL. [OpenID Authentication 2.0]

**OP Identifier**
An Identifier for an OpenID Provider. [OpenID Authentication 2.0]

**Object Identifier**
A specialized formatted number that is registered with an internationally recognized standards organization. The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the federal government PKI they are used to uniquely identify each of the seven policies and cryptographic algorithms supported. [FBCA CP 2.25]

A globally unique identifier of a data object as defined in ISO/IEC 8824-2. [NIST SP 800-73-3 Part 1]

A globally unique identifier of a data object as defined in ISO/IEC 8824-2. [NIST SP 800-73-3 Part 2]

A globally unique identifier of a data object as defined in ISO/IEC 8824-2. [NIST SP 800-73-3 Part 3]

**Off-card**
Refers to data that is not stored within the PIV Card or to a computation that is not performed by the Integrated Circuit Chip (ICC) of the PIV Card. [NIST FIPS 201-2]

**Off-line Attack**
An attack where the Attacker obtains some data (typically by eavesdropping on an authentication protocol run or by penetrating a system and stealing security files) that he/she is able to analyze in a system of his/her own choosing. [NIST SP 800-63-1]

**Office Of Governmentwide Policy**
(undefined) [FICAM TFPAP 1.0.1]

**Office Of Management And Budget**
(undefined) [FICAM TFPAP 1.0.1]

**Office Of Management And Budget (US Federal Government)**
(undefined) [InCommon IAAF 1.1]

**Offline Test**
Offline tests use previously captured images as inputs to core biometric implementations. Such tests are repeatable and can readily be scaled to very large populations and large numbers of competing products. They institue a level-playing field and produce robust estimates of the core biometric power of an algorithm. This style of testing is particularly suited to interoperability testing of a fingerprint template. [NIST SP 800-85B]

**On-card**
Refers to data that is stored within the PIV Card or to a computation that is performed by the Integrated Circuit Chip (ICC) of the PIV Card. [NIST FIPS 201-2]

**On-card Comparison**
Comparison of fingerprint data transmitted to the card with reference data previously stored on the card. [NIST FIPS 201-2]

**Online Attack**
An attack against an authentication protocol where the Attacker either assumes the role of a Claimant with a genuine Verifier or actively alters the authentication channel. [NIST SP 800-63-1]

**Online Certificate Status Protocol**
An online protocol used to determine the status of a public key certificate. [NIST FIPS 201-2]

**Online Guessing Attack**
An attack in which an Attacker performs repeated logon trials by guessing possible values of the token authenticator. [NIST SP 800-63-1]

**Op-local Identifier**
An alternate Identifier for an end user that is local to a particular OP and thus not necessarily under the end user's control [OpenID Authentication 2.0]

**Openid Provider**
An OpenID Authentication server on which a Relying Party relies for an assertion that the end user controls an Identifier. [OpenID Authentication 2.0]

**Operational Test**
Operational tests involve a deployed system and are usually conducted to measure in-the-field performance and user-system interaction effects. Such tests require the members of human test population to transact with biometric sensors. False acceptance rates may not be measurable, depending on the controls instituted. [NIST SP 800-85B]

**Operator**
an individual accessing a cryptographic module or a process (subject) operating on behalf of the individual, regardless of the assumed role. [NIST FIPS 140-2]

**Organization**
An entity of any size, complexity, or positioning within an organizational structure (e.g., a federal agency, or, as appropriate, any of its operational elements). [NIST IR 7693]

**Out Of Band**
Communications which occur outside of a previously established communication method or channel. [FICAM TFPAP 1.0.1]

**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). [FBCA CP 2.25]

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). [SAFE-BioPharma CP 2.5]

**Output Data**
information that is produced from a cryptographic module. [NIST FIPS 140-2]

**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. [FBCA CP 2.25]

**PIV Assurance Level**
A degree of confidence established in the identity of the holder of the PIV Card. [NIST FIPS 201-2]

**PIV Key Type**
The type of a key. the PIV KEY Types are 1) PIV Authentication KEY, 2) PIV Card Authenticaiton Key, 3) PIV Digital Signauture Key, 4) PIV Key Management Key, and 5) Card Application Administration Key. [NIST SP 800-73-3 Part 1]

**PKI Disclosure Statement**
An instrument that supplements a CP or CPS by disclosing critical information about the policies and practices of a CA/PKI. A PDS is a vehicle for disclosing and emphasizing information normally covered in detail by associated CP and/or CPS documents. Consequently, a PDS is not intended to replace a CP or CPS. [IETF RFC 3647]

**PKI Sponsor**
Fills the role of a Subscriber for non-human system components that are named as public key certificate subjects, and is responsible for meeting the obligations of Subscribers as defined throughout this CP. [FBCA CP 2.25]

**PKI-PIV Authentication Key**
A PIV authentication mechanism that is implemented by an asymmetric key challenge/response protocol using the PIV Authentication key of the PIV Card and a contact reader, or a contactless card reader that supports the virtual contact interface. [NIST FIPS 201-2]

**Parameters**
Specific variables and their values that are used with a cryptographic algorithm to compute outputs useful to achieve specific security goals. [NIST SP 800-130]

**Participant**
An organization accepted into the InCommon Federation that has met all the criteria for participation as either a higher education institution or a Sponsored Partner. [InCommon Glossary]

An individual or organization that plays a role within a given PKI as a subscriber, relying party, CA, RA, certificate manufacturing authority, repository service provider, or similar entity. [IETF RFC 3647]

**Participant Agreement**
This is the "contract" that a potential Participant signs when they are accepted by the Federation. This document outlines information such as fees, and responsibilities to participate in InCommon. [InCommon Glossary]

**Participant Operating Practices**
This document describes how InCommon Participants need to describe their credential and identity management system. [InCommon Glossary]

**Participants**
the collective subjects, identity providers, attribute providers, relying parties and identity media taking part in a given transaction. [NSTIC Strategy]

**Party**
Informally, one or more principals participating in some process or communication, such as receiving an assertion or accessing a resource. [OASIS SAML Glossary 2.0]

**Passive Attack**
An attack against an authentication protocol where the Attacker intercepts data traveling along the network between the Claimant and Verifier, but does not alter the data (i.e., eavesdropping). [NIST SP 800-63-1]

**Password**
A secret that a Claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings. [NIST SP 800-63-1]

a string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization. [NIST FIPS 140-2]

A shared secret character string used in authentication protocols. In many cases the claimant is expected to memorize the password. [Kantara IAF 1100]

**Path Validation**
The process of verifying the binding between the subject identifier and subject public key in a certificate, based on the public key of a trust anchor, through the validation of a chain of certificates that begins with a certificate issued by the trust anchor and ends with the target certificate. Successful path validation provides strong evidence that the information in the target certificate is trustworthy. [NIST FIPS 201-2]

**Permission**
A scope of access over a particular resource set at a particular host that is being asked for by, or being granted to, a requester. In authorization policy terminology, a permission includes a "subject" (requesting party), "verbs" (one or more scopes of access), and an "object" (resource set). The UMA "bearer" token profile uses permissions directly. Other UMA token profiles might define other forms of authorization data, such as authorization decisions or resource-specific policies. [Kantara UMA]

**Persistent**
Ability to maintain data. [ICAM SAML 2.0 WB SSO Profile 1.0.2]

**Persistent Pseudonym**
A privacy-preserving name identifier assigned by a provider to identify a principal to a given relying party for an extended period of time that spans multiple sessions; can be used to represent an identity federation. [OASIS SAML Glossary 2.0]

**Person**
Any person considered as an asset by the management domain. [NIST IR 7693]

**Personal Identification Number**
A password consisting only of decimal digits. [NIST SP 800-63-1]

A secret that a cardholder memorizes and uses to authenticate his or her identity. [NIST FIPS 201-2]

an alphanumeric code or password used to authenticate an identity. [NIST FIPS 140-2]

**Personal Identifying Information**
Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. Possession and Control of a Token The ability to activate and use the token in an authentication protocol. [FICAM TFPAP 1.0.1]

**Personal Identity Verification Card**
Defined by [FIPS 201] as a physical artifact (e.g., identity card, smart card) issued to federal employees and contractors that contains stored credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable). [NIST SP 800-63-1]

A physical artifact (e.g., identity card, "smart" card) issued to an individual that contains stored identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable). [NIST FIPS 201-2]

**Personally Identifiable Information**
Defined by GAO Report 08-536 as "Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information." [NIST SP 800-63-1]

Information that can be used to distinguish or trace an individual's identity, such as name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. [OMB0716] [NIST FIPS 201-2]

**Pharming**
An attack in which an Attacker corrupts an infrastructure service such as DNS (Domain Name Service) causing the Subscriber to be misdirected to a forged Verifier/RP, which could cause the Subscriber to reveal sensitive information, download harmful software or contribute to a fraudulent act. [NIST SP 800-63-1]

**Phishing**
An attack in which the Subscriber is lured (usually through an email) to interact with a counterfeit Verifier/RP and tricked into revealing information that can be used to masquerade as that Subscriber to the real Verifier/RP. [NIST SP 800-63-1]

**Physical Protection**
the safeguarding of a cryptographic module, cryptographic keys, or CSPs using physical means. [NIST FIPS 140-2]

**Physically Isolated Network**
A network that is not connected to entities or systems outside a physically controlled space. [FBCA CP 2.25]

**Pki-card Authentication Key**
A PIV authentication mechanism that is implemented by an asymmetric key challenge/response protocol using the Card Authentication key of the PIV Card and a contact or contactless reader. [NIST FIPS 201-2]

**Plaintext Key**
an unencrypted cryptographic key. [NIST FIPS 140-2]

**Policy Decision Point**
A system entity that makes authorization decisions for itself or for other system entities that request such decisions. [PolicyTerm] For example, a SAML PDP consumes authorization decision requests, and produces authorization decision assertions in response. A PDP is an "authorization decision authority". [OASIS SAML Glossary 2.0]

**Policy Enforcement Point**
A system entity that requests and subsequently enforces authorization decisions. [PolicyTerm] For example, a SAML PEP sends authorization decision requests to a PDP, and consumes the authorization decision assertions sent in response. [OASIS SAML Glossary 2.0]

**Policy Management Authority**
Body established to oversee the creation and update of Certificate Policies, review Certification Practice Statements, 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. For the FBCA, the PMA is the FPKIPA. [FBCA CP 2.25]

**Policy Qualifier**
Policy-dependent information that may accompany a CP identifier in an X.509 certificate. Such information can include a pointer to the URL of the applicable CPS or relying party agreement. It may also include text (or number causing the appearance of text) that contains terms of the use of the certificate or other legal information. [IETF RFC 3647]

**Port**
a physical entry or exit point of a cryptographic module that provides access to the module for physical signals, represented by logical information flows (physically separated ports do not share the same physical pin or wire). [NIST FIPS 140-2]

**Possession And Control Of A Token**
The ability to activate and use the token in an authentication protocol. [NIST SP 800-63-1]

**Practice Statement**
A formal statement of the practices followed by the parties to an authentication process (i.e., RA, CSP, or Verifier). It usually describes the policies and practices of the parties and can become legally binding. [NIST SP 800-63-1]

A formal statement of the practices followed by an authentication entity (e.g., RP, CSP, or verifier) that typically defines the specific steps taken to register and verify identities, issue credentials, and authenticate claimants. [Kantara IAF 1100]

**Pre-activation State**
A key life cycle state in which a key has not yet been authorized for use. [NIST SP 800-130]

**Preliminary Informative Element**
element that identifies the document, introduces its content and explains its background, its development and it relationship with other documents [ISO-IEC Directives Part 2]

**Principal**
A system entity whose identity can be authenticated. [X.811] [OASIS SAML Glossary 2.0]

**Principal CA**
The Principal CA is a CA designated by an Entity to interoperate with the FBCA. An Entity may designate multiple Principal CAs to interoperate with the FBCA. [FBCA CP 2.25]

The Principal CA is a CA designated by an Issuer to interoperate with the SBCA. An Issuer may designate multiple Principal CAs to interoperate with the SBCA. [SAFE-BioPharma CP 2.5]

**Principal Identity**
A representation of a principal's identity, typically an identifier. Profile A set of rules for one of several purposes; each set is given a name in the pattern "xxx profile of SAML" or "xxx SAML profile". a) Rules for how to embed assertions into and extract them from a protocol or other context of use. b) Rules for using SAML protocol messages in a particular context of use. c) Rules for mapping attributes expressed in SAML to another attribute representation system. Such a set of rules is known as an "attribute profile". [OASIS SAML Glossary 2.0]

**Privacy**
Restricting access to subscriber or Relying Party information in accordance with Federal law and Entity policy. [FBCA CP 2.25]

Assurance that the confidentiality of, and access to, certain information about an entity is protected. [NIST SP 800-130]

Restricting access to subscriber or Relying Party information in accordance with Federal law and Issuer policy. [SAFE-BioPharma CP 2.5]

**Privacy Impact Assessment**
(undefined) [FICAM TFPAP 1.0.1]

**Privacy Policy**
A statement to users of what information is collected and what will be done with the information after it has been collected. [InCommon Glossary]

**Private Credentials**
Credentials that cannot be disclosed by the CSP because the contents can be used to compromise the token. (For more discussion, see Section 7.1.1.) [NIST SP 800-63-1]

**Private Key**
The secret part of an asymmetric key pair that is used to digitally sign or decrypt data. [NIST SP 800-63-1]

(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. [FBCA CP 2.25]

The secret part of an asymmetric key pair that is typically used to digitally sign or decrypt data. [NIST FIPS 201-2]

a cryptographic key, used with a public key cryptographic algorithm, that is uniquely associated with an entity and is not made public. [NIST FIPS 140-2]

**Profile**
Data comprising the broad set of attributes that may be maintained for an identity, and the data required to authenticate under that identity. [InCommon Glossary]

A specification of the policies, procedures, components and devices that are used to create a CKMS that conforms to the standards of a customer sector (e.g., Federal, Private, or International). [NIST SP 800-130]

**Proof Of Possession Protocol**
A protocol where a Claimant proves to a Verifier that he/she possesses and controls a token (e.g., a key or password) [FICAM TFPAP 1.0.1]

**Proof-of-possession**
data that is used in a proof process to demonstrate the sender's knowledge of information that should only be known to the claiming sender of a security token. [OASIS IMI 1.0]

**Protected Channel**
A communication mechanism that provides message integrity and confidentiality protection. [InCommon IAAF 1.1]

**Protected Resource**
Definition is referenced elsewhere, term is used often in this document but not defined. [IETF ID OAuth 2.0]

An access-restricted resource at a host, which is being policy-protected by an AM. [Kantara UMA]

An access-restricted resource that can be obtained from the server using an OAuth-authenticated request (Section 3). [IETF RFC 5849]

**Protected Session**
A session wherein messages between two participants are encrypted and integrity is protected using a set of shared secrets called session keys. A participant is said to be authenticated if, during the session, he, she or it proves possession of a long term token in addition to the session keys, and if the other party can verify the identity associated with that token. If both participants are authenticated, the protected session is said to be mutually authenticated. [NIST SP 800-63-1]

A session wherein messages between two participants are encrypted and integrity is protected using a set of shared secrets called session keys. A participant is said to be authenticated if, during the session, he, she or it proves possession of a long term token in addition to the session keys, and if the other party can verify the identity associated with that token. If both participants are authenticated, the protected session is said to be mutually authenticated. One way to implement a protected session is SSL/TLS, which is required for this Profile. [ICAM SAML 2.0 WB SSO Profile 1.0.2]

**Protection Profile**
an implementation-independent set of security requirements for a category of Targets of Evaluation (TOEs) that meet specific consumer needs. [NIST FIPS 140-2]

**Provider**
A generic way to refer to both identity providers and service providers. [OASIS SAML Glossary 2.0]

**Proxy**
An entity authorized to act for another. a) Authority or power to act for another. b) A document giving such authority. [Merriam] [OASIS SAML Glossary 2.0]

**Proxy Server**
A computer process that relays a protocol between client and server computer systems, by appearing to the client to be the server and appearing to the server to be the client. [RFC2828] [OASIS SAML Glossary 2.0]

**Pseudonym**
A false name. In this document, all unverified names are assumed to be pseudonyms. [NIST SP 800-63-1]

A Subscriber name that has been chosen by the Subscriber that is not verified as meaningful by identity proofing. [FICAM TFPAP 1.0.1]

**Pseudonymous Identifier**
Private end user pseudonym that will only be used with one site. The site will always know it's you when you come back, but it won't be able to look up any other information about you, or correlate your profile with other sites. [ICAM SAML 2.0 WB SSO Profile 1.0.2]

**Pseudonyms**
a name assigned by a Federal department or agency through a formal process to a Federal employee for the purpose of the employee's protection (i.e., the employee might be placed at risk if his or her actual name were known) or for other purposes. [NIST FIPS 201-2]

**Public Credentials**
Credentials that describe the binding in a way that does not compromise the token. (For more discussion, see Section 7.1.1.) [NIST SP 800-63-1]

**Public Key**
The public part of an asymmetric key pair that is used to verify signatures or encrypt data. [NIST SP 800-63-1]

(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. [FBCA CP 2.25]

The public part of an asymmetric key pair that is typically used to verify signatures or encrypt data. [NIST FIPS 201-2]

a cryptographic key used with a public key cryptographic algorithm that is uniquely associated with an entity and that may be made public. (Public keys are not considered CSPs.) [NIST FIPS 140-2]

The public part of the asymmetric key pair that is typically used to verify signatures or encrypt data. [Kantara IAF 1100]

**Public Key (asymmetric) Cryptographic Algorithm**
a cryptographic algorithm that uses two related keys, a public key and a private key. The two keys have the property that deriving the private key from the public key is computationally infeasible. [NIST FIPS 140-2]

**Public Key Certificate**
A digital document issued and digitally signed by the private key of a Certificate authority that binds the name of a Subscriber to a public key. The certificate indicates that the Subscriber identified in the certificate has sole control and access to the private key. See also [RFC 5280]. [NIST SP 800-63-1]

A digital certificate that binds a system entity's identity to a public key value, and possibly to additional data items; a digitally-signed data structure that attests to the ownership of a public key [RFC 2828]. [FBCA Cross-certification Methodology 3.0]

a set of data that uniquely identifies an entity, contains the entity's public key, and is digitally signed by a trusted party, thereby binding the public key to the entity. [NIST FIPS 140-2]

**Public Key Cryptography**
A cryptographic technique that uses two keys: the first key is always kept secret by an entity, and the second key, which is uniquely linked to the first one, is made public. Messages created with the first key can be uniquely verified with the second key. [InCommon Glossary]

**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. [NIST SP 800-63-1]

A system of CAs that perform some set of certificate management, archive management, key management, and token management functions for a community of users in an application of asymmetric cryptography [RFC 2828]. As used in this document, PKI also includes the entire set of policies, processes, and CAs used for the purpose of administering certificates and keys. The term also designates the person or organizational unit within an entity responsible for the following (a) Operation of a Certification Authority trusted by one or more users to issue and manage public key certificates and certificate revocation mechanisms; or (b) Management of (i) Any arrangement under which an entity contracts for the provision of services relating to the issuance and management of public key certificates and certificate revocation lists on its behalf; and (ii) Policies and procedures within the entity for managing public key certificates issued on its behalf. Note- A PKI remains at all times responsible and accountable for managing the public key certificates it issues or arranges to be issued on behalf of its organization. [FBCA Cross-certification Methodology 3.0]

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. [FBCA CP 2.25]

A support service to the PIV system that provides the cryptographic keys needed to perform digital signature-based identity verification and to protect communications and storage of sensitive verification system data within identity cards and the verification system. [NIST FIPS 201-2]

The set of standards and services that facilitate the use of public-key cryptography in a networked environment. [InCommon Glossary]

A set of technical and procedural measures used to manage public keys embedded in digital certificates. The keys in such certificates can be used to safeguard communication and data exchange over potentially unsecure networks. [Kantara IAF 1100]

**Publicly Available Specification**
document published by ISO or IEC to respond to an urgent market need, representing either a) a consensus in an organization external to ISO or IEC, or b) a consensus of the experts within a working group [ISO-IEC Directives Part 2]

**Pull**
To actively request information from a system entity. [OASIS SAML Glossary 2.0]

**Push**
To provide information to a system entity that did not actively request it. [OASIS SAML Glossary 2.0]

**Qubit**
In quantum computing, a unit of quantum information - the quantum analogue of the classical bit. [NIST SP 800-130]

**Random Number Generator**
Random Number Generators used for cryptographic applications typically produce a sequence of zero and one bits that may be combined into sub-sequences or blocks of random numbers. There are two basic classes deterministic and nondeterministic. A deterministic RNG consists of an algorithm that produces a sequence of bits from an initial value called a seed. A nondeterministic RNG produces output that is dependent on some unpredictable physical source that is outside human control. [NIST FIPS 140-2]

**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. [FBCA CP 2.25]

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. [SAFE-BioPharma CP 2.5]

**Recommendation**
A special publication of the ITL stipulating specific characteristics of technology to use or procedures to follow to achieve a common level of quality or level of interoperability. [NIST FIPS 201-2]

expression in the content of a document conveying that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred by not necessarily required, or that (in the negative form) a certain possibility or course of action is deprecated but not prohibited [ISO-IEC Directives Part 2]

**Recover (key/metadata)**
To obtain or reconstruct a key/metadata from backup or archive storage. [NIST SP 800-130]

**Reference Data**
Cryptographic material used in the performance of a cryptographic protocol such as an authentication or a signing protocol. The reference data lenght is the maximum length of a password or PIN. For algorithms, the reference data length is the length of a key. [NIST SP 800-73-3 Part 2]

Cryptographic material used in the performance of a cryptographic protocol such as an authentication or a signing protocol. The reference data lenght is the maximum length of a password or PIN. For algorithms, the reference data length is the length of a key. [NIST SP 800-73-3 Part 3]

**Refresh Token**
Refresh tokens are credentials used to obtain access tokens. Refresh tokens are issued to the client by the authorization server and are used to obtain a new access token when the current access token becomes invalid or expires, or to obtain additional access tokens with identical or narrower scope (access tokens may have a shorter lifetime and fewer permissions than authorized by the resource owner). Issuing a refresh token is optional at the discretion of the authorization server. If the authorization server issues a refresh token, it is included when issuing an access token (i.e. step (D) in Figure 1). A refresh token is a string representing the authorization granted to the client by the resource owner. The string is usually opaque to the client. The token denotes an identifier used to retrieve the authorization information. Unlike access tokens, refresh tokens are intended for use only with authorization servers and are never sent to resource servers. [IETF ID OAuth 2.0]

**Registration**
The process through which an Applicant applies to become a Subscriber of a CSP and an RA validates the identity of the Applicant on behalf of the CSP. [NIST SP 800-63-1]

The process through which a party applies to become a Subscriber of a CSP and an RA validates the identity of that party on behalf of the CSP. [FICAM TFPAP 1.0.1]

The process of creating a record of a Subject's Identity information. [InCommon IAAF 1.1]

An entry in a register, or somebody or something whose name or designation is entered in a register. [Kantara IAF 1100]

The collection of procedures performed by a registration agent for verifying the identity and authorizations of an entity and establishing a trusted association of the entity's key(s) to the entity's identifier and possibly other metadata. [NIST SP 800-130]

**Registration Authority**
A trusted entity that establishes and vouches for the identity or attributes of a Subscriber to a CSP. The RA may be an integral part of a CSP, or it may be independent of a CSP, but it has a relationship to the CSP(s). [NIST SP 800-63-1]

An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a Registration Authority is delegated certain tasks on behalf of an authorized CA). [FBCA CP 2.25]

A trusted entity that establishes and vouches for the identity of a Subscriber to a CSP. The RA may be an integral part of a CSP, or it may be independent of a CSP, but it has a relationship to the CSP(s). [FICAM TFPAP 1.0.1]

A trusted entity entitled to perform Registrations. [InCommon IAAF 1.1]

An entity that is responsible for one or more of the following functions: the identification and authentication of certificate applicants, the approval or rejection of certificate applications, initiating certificate revocations or suspensions under certain circumstances, processing subscriber requests to revoke or suspend their certificates, and approving or rejecting requests by subscribers to renew or re-key their certificates. RAs, however, do not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of a CA). [Note: The term Local Registration Authority (LRA) is sometimes used in other documents for the same concept.] [IETF RFC 3647]

**Rekey**
The process used to replace a previously active key with a new key that was created completely independently of the old key. [NIST SP 800-130]

**Relationship Identifier**
Identifying information where the value is a relationship to another asset. [NIST IR 7693]

**Relying Parties**
A synonym for Service Provider. [InCommon IAAF 1.1]

**Relying Party**
An entity that relies upon the Subscriber's token and credentials or a Verifier's assertion of a Claimant's identity, typically to process a transaction or grant access to information or a system. [NIST SP 800-63-1]

Entity requesting Backend Attributes typically to support PIV Cardholder authentication, authorization, or emergency events. [BAE Overview]

A person or Entity who has received information that includes a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them. [FBCA CP 2.25]

An entity that relies upon the Subscriber's credentials or Verifier's assertion of an identity, typically to process a transaction or grant access to information or a system. [FICAM TFPAP 1.0.1]

a network entity providing the desired service, and relying upon Digital Identity. [OASIS IMI 1.0]

A recipient of a certificate who acts in reliance on that certificate and/or any digital signatures verified using that certificate. http://www.ietf.org/rfc/rfc3647.txt [InCommon Glossary]

An entity that relies upon a subscriber's credentials, typically to process a transaction or grant access to information or a system. [Kantara IAF 1100]

An entity that relies upon the subscriber's credentials, typically to process a transaction or grant access to informaiton or a system. [NIST SP 800-73-3 Part 1]

[entity that] makes transaction decisions based upon its receipt, validation, and acceptance of a subject's authenticated credentials and attributes. Within the Identity Ecosystem, a relying party selects and trusts the identity and attribute providers of their choice, based on risk and functional requirements. Relying parties are not required to integrate with all permutations of credential types and identity media. Rather, they can trust an identity provider's assertion of a valid subject credential, as appropriate. Relying parties also typically need to identify and authenticate themselves to the subject as part of transactions in the Identity Ecosystem. Relying parties can choose the strength of the authentication and attributes required to access their services. [NSTIC Strategy]

A Web application that wants proof that the end user controls an Identifier. [OpenID Authentication 2.0]

A recipient of a certificate who acts in reliance on that certificate and/or any digital signatures verified using that certificate. In this document, the terms "certificate user" and "relying party" are used interchangeably. [IETF RFC 3647]

A system entity that decides to take an action based on information from another system entity. For example, a SAML relying party depends on receiving assertions from an asserting party (a SAML authority) about a subject. [OASIS SAML Glossary 2.0]

A party responsible for a Relying Party Agent and on whose behalf that Agent acts. A Relying Party is relying on the services provided by a Yadis Resource, in particular on data provided by that service concerning the person identified by a Yadis ID. [Yadis 1.0]

**Relying Party Agent**
A role to be fulfilled by an agent that uses a Yadis ID (and the data accessible using that Yadis ID) provided by a Yadis User Agent. The Relying Party Agent discovers the services available for a Yadis ID using the Yadis Protocol, and may modify its own behavior accordingly. [Yadis 1.0]

**Relying Party Agreement**
An agreement between a certification authority and relying party that typically establishes the rights and responsibilities between those parties regarding the verification of digital signatures or other uses of certificates. [IETF RFC 3647]

**Relying Party Security Token Service**
a Security Token Service run by a Relying Party to accept and issue tokens. [OASIS IMI 1.0]

**Remote**
(As in remote authentication or remote transaction) An information exchange between network-connected devices where the information cannot be reliably protected end-to-end by a single organization's security controls. Note: Any information exchange across the Internet is considered remote. [NIST SP 800-63-1]

**Removable Cover**
a cover designed to permit physical access to the contents of a cryptographic module. [NIST FIPS 140-2]

**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. [FBCA CP 2.25]

The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate. [SAFE-BioPharma CP 2.5]

**Renewal**
The process used to extend the validity period of a public key so that it can be used for an additional time period. [NIST SP 800-130]

**Replay Attack**
An attack in which the Attacker is able to replay previously captured messages (between a legitimate Claimant and a Verifier) to masquerade as that Claimant to the Verifier or vice versa. [NIST SP 800-63-1]

**Repository**
A system for storing and distributing digital certificates and related information (including CRLs, CPSs, and certificate policies) to certificate users [RFC 2828]. [FBCA Cross-certification Methodology 3.0]

A database containing information and data relating to certificates as specified in this CP; may also be referred to as a directory. [FBCA CP 2.25]

**Requester**
An UMA-defined variant of an OAuth client that seeks access to a protected resource. [Kantara UMA]

**Requester, SAML Requester**
A system entity that utilizes the SAML protocol to request services from another system entity (a SAML authority, a responder). The term "client" for this notion is not used because many system entities simultaneously or serially act as both clients and servers. In cases where the SOAP binding for SAML is being used, the SAML requester is architecturally distinct from the initial SOAP sender. [OASIS SAML Glossary 2.0]

**Requesting Party**
A web user, or a corporation or other legal person, that uses a requester to seek access to a protected resource. The requesting party may or may not be the same person as the authorizing user. [Kantara UMA]

**Requirement**
expression in the content of a document conveying critera to be fulfilled if compliance with the document is to be claimed and from which no deviation is permitted [ISO-IEC Directives Part 2]

**Resource**
Data contained in an information system (for example, in the form of files, information in memory, etc), as well as: a) A service provided by a system. b) An item of system equipment (in other words, a system component such as hardware, firmware, software, or documentation). c) A facility that houses system operations and equipment. [RFC2828] SAML uses resource in the first two senses, and refers to resources by means of URI references. [OASIS SAML Glossary 2.0]

**Resource Descriptor URL**
A URL that locates a Yadis document. [Yadis 1.0]

**Resource Owner**
An entity capable of granting access to a protected resource. When the resource owner is a person, it is referred to as an end- user. [IETF ID OAuth 2.0]

An entity capable of accessing and controlling protected resources by using credentials to authenticate with the server. [IETF RFC 5849]

**Resource Provider**
For the InCommon Federation, the term Resource Provider has been superseded by the term Service Provider. [InCommon Glossary]

**Resource Server**
The server hosting the protected resources, capable of accepting and responding to protected resource requests using access tokens. [IETF ID OAuth 2.0]

**Resource Set**
A host-managed set of one or more resources to be AM-protected. In authorization policy terminology, a resource set is the "object" being protected. [Kantara UMA]

**Responder, SAML Responder**
A system entity (a SAML authority) that utilizes the SAML protocol to respond to a request for services from another system entity (a requester). The term "server" for this notion is not used because many system entities simultaneously or serially act as both clients and servers. In cases where the SOAP binding for SAML is being used, the SAML responder is architecturally distinct from the ultimate SOAP receiver. [OASIS SAML Glossary 2.0]

**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. [FBCA CP 2.25]

**Restful**
Having the REST architectural style [Yadis 1.0]

**Revoke (a Certificate)**
To prematurely end the operational period of a certificate effective at a specific date and time. [SAFE-BioPharma CP 2.5]

**Revoke A Certificate**
To prematurely end the operational period of a certificate effective at a specific date and time. [FBCA CP 2.25]

**Revoked State**
The key life cycle state in which a previously active cryptographic key is no longer to be used to apply cryptographic protection to data. [NIST SP 800-130]

**Risk**
An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result. [FBCA CP 2.25]

An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result. [SAFE-BioPharma CP 2.5]

**Risk Assessment**
The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact. Part of Risk Management and synonymous with Risk Analysis. [NIST SP 800-63-1]

**Risk Tolerance**
The level of risk an entity is willing to assume in order to achieve a potential desired result. [FBCA CP 2.25]

**Role**
The usual or expected function of somebody or something, or the part somebody or something plays in a particular action or event. [Kantara IAF 1100]

The set of acceptable functions, services, and tasks that a person or organization is authorized to perform within an environment or context. [NIST SP 800-130]

Dictionaries define a role as "a character or part played by a performer" or "a function or position." System entities don various types of roles serially and/or simultaneously, for example, active roles and passive roles. The notion of an Administrator is often an example of a role. [OASIS SAML Glossary 2.0]

**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. [FBCA CP 2.25]

**Rootkit**
Malware that enables unauthorized, privileged access to a computer while actively hiding its presence from administrators by subverting standard operating-system functionality or other applications. [NIST SP 800-130]

**Router**
A physical or logical entity that receives and transmits data packets or establishes logical connections among a diverse set of communicating entities (usually supports both hardwired and wireless communication devices simultaneously). [NIST SP 800-130]

**SAML Artifact**
A small, fixed-size, structured data object pointing to a typically larger,variably-sized SAML protocol message. SAML artifacts are designed to be embedded in URLs and conveyed in HTTP messages, such as HTTP response messages with "3xx Redirection" status codes, and subsequent HTTP GET messages. In this way, a service provider may indirectly, via a user agent, convey a SAML artifact to another provider, who may subsequently dereference the SAML artifact via a direct interaction with the supplying provider, and obtain the SAML protocol message. Various characteristics of the HTTP protocol and user agent implementations provided the impetus for concocting this approach. The HTTP Artifact binding section of [SAMLBind] defines both the SAML Artifact format and the SAML HTTP protocol binding incorporating it. [OASIS SAML Glossary 2.0]

**SAML Authentication Assertion**
A SAML assertion that conveys information from a Verifier to an RP about a successful act of authentication that took place between the Verifier and a Subscriber. [NIST SP 800-63-1]

**SAML Authority**
An abstract system entity in the SAML domain model that issues assertions. See also attribute authority, authentication authority, and policy decision point (PDP). [OASIS SAML Glossary 2.0]

**Salt**
A non-secret value that is used in a cryptographic process, usually to ensure that the results of computations for one instance cannot be reused by an Attacker. [NIST SP 800-63-1]

A non-secret value that is used in a cryptographic process, usually to ensure that the results of computations for one instance cannot be reused by an Attacker. [FICAM TFPAP 1.0.1]

**Scalability**
The ability of a system to handle a growing amount of work in a capable manner or its ability to be enlarged to accommodate that growth. [NIST SP 800-130]

**Scenario Test**
Scenario testing is intended to mimic an operational application and simultaneously institute controls on the procedures. Scenario testing requires members of human test population to transact with biometric sensors. Scenario tests are appropriate for capturing and assessing the effects of interactions human users have with biometric sensors and interfaces. [NIST SP 800-85B]

**Scheme**
An unambiguous specification of a set of transformations that is capable of providing a (cryptographic) service when properly implemented and maintained. A scheme is a higher-level construct than a primitive and a lower level construct than a protocol. [NIST SP 800-130]

**Scope**
A bounded extent of access that is possible to perform on a resource set. In authorization policy terminology, a scope is one of the "verbs" that can apply to a resource set. Whereas OAuth scopes apply to resource sets that are implicitly defined in protocol terms, UMA associates scopes with explicitly labeled resource sets ("objects"). [Kantara UMA]

**Secondary Authenticator**
A temporary secret, issued by the Verifier to a successfully authenticated Subscriber as part of an assertion protocol. This secret is subsequently used, by the Subscriber, to authenticate to the RP. Examples of secondary authenticators include bearer assertions, assertion references, and Kerberos session keys. [NIST SP 800-63-1]

**Secret Key**
a cryptographic key, used with a secret key cryptographic algorithm, that is uniquely associated with one or more entities and should not be made public. [NIST FIPS 140-2]

**Secret Key (symmetric) Cryptographic Algorithm**
a cryptographic algorithm that uses a single secret key for both encryption and decryption. [NIST FIPS 140-2]

**Sector**
A group of organizations (e.g., Federal agencies, private organizations, international consortia) that have common goals, standards, and requirements for a product, system, or service. [NIST SP 800-130]

**Secure Sockets Layer**
An authentication and security protocol widely implemented in browsers and web servers. SSL has been superseded by the newer Transport Layer Security (TLS) protocol; TLS 1.0 is effectively SSL version 3.1. [NIST SP 800-63-1]

**Security**
A collection of safeguards that ensures the confidentiality of information, protects the integrity of information, ensures the availability of information, accounts for use of the system, and protects the system(s) and/or network(s) used to process the information. [Kantara IAF 1100]

A collection of safeguards that ensure the confidentiality of information, protect the systems or networks used to process it, and control access to them. Security typically encompasses the concepts of secrecy, confidentiality, integrity, and availability. It is intended to ensure that a system resists potentially correlated attacks. [CyberTrust] [OASIS SAML Glossary 2.0]

**Security Architecture**
A plan and set of principles for an administrative domain and its security domains that describe the security services that a system is required to provide to meet the needs of its users, the system elements required to implement the services, and the performance levels required in the elements to deal with the threat environment. A complete security architecture for a system addresses administrative security, communication security, computer security, emanations security, personnel security, and physical security, and prescribes security policies for each. A complete security architecture needs to deal with both intentional, intelligent threats and accidental threats. A security architecture should explicitly evolve over time as an integral part of its administrative domain's evolution. [RFC2828] [OASIS SAML Glossary 2.0]

**Security Assertion**
An assertion that is scrutinized in the context of a security architecture. [OASIS SAML Glossary 2.0]

**Security Assertion Markup Language**
An XML-based security specification developed by the Organization for the Advancement of Structured Information Standards (OASIS) for exchanging authentication (and authorization) information between trusted entities over the Internet. See [SAML]. [NIST SP 800-63-1]

The set of specifications describing security assertions that are encoded in XML, profiles for attaching the assertions to various protocols and frameworks, the request/response protocol used to obtain the assertions, and bindings of this protocol to various transfer protocols (for example, SOAP and HTTP). SAML addresses web single sign-on, web services authentication, attribute exchange, authorization, non-repudiation, and secure communications. SAML defines assertion message formats that are referenced in Liberty Alliance, Shibboleth, WS-Security, and other specifications. SAML has become the standard web SSO identity management solution. Several versions have been released to date, including SAML 1.0, SAML 1.1, and SAML 2.0. The Organization for the Advancement of Structured Information Standards (OASIS) oversees SAML. [BAE Overview]

The set of specifications describing security assertions that are encoded in XML, profiles for attaching the assertions to various protocols and frameworks, the request/response protocol used to obtain the assertions, and bindings of this protocol to various transfer protocols (for example, SOAP and HTTP). SAML addresses web single sign-on, web services authentication, attribute exchange, authorization, non-repudiation, and secure communications. SAML defines assertion message formats that are referenced in Liberty Alliance, Shibboleth, WS-Security, and other specifications. SAML has become the standard web SSO identity management solution. Several versions have been released to date, including SAML 1.0, SAML 1.1, and SAML 2.0. The Organization for the Advancement of Structured Information Standards (OASIS) oversees SAML. [ICAM SAML 2.0 WB SSO Profile 1.0.2]

The set of specifications describing security assertions that are encoded in XML, profiles for attaching the assertions to various protocols and frameworks, the request/response protocol used to obtain the assertions, and bindings of this protocol to various transfer protocols (for example, SOAP and HTTP). [OASIS SAML Glossary 2.0]

**Security Context**
With respect to an individual SAML protocol message, the message's security context is the semantic union of the message's security header blocks (if any) along with other security mechanisms that may be employed in the message's delivery to a recipient. With respect to the latter, an examples are security mechanisms employed at lower network stack layers such as HTTP, TLS/SSL, IPSEC, etc. With respect to a system entity, "Alice", interacting with another system entity, "Bob", a security context is nominally the semantic union of all employed security mechanisms across all network connections between Alice and Bob. Alice and Bob may each individually be, for example, a provider or a user agent. This notion of security context is similar to the notion of "security contexts" as employed in [RFC2743], and in the Distributed Computing Environment [DCE], for example. [OASIS SAML Glossary 2.0]

**Security Domain**
A logical entity that contains a group of elements (e.g., people, organizations, information systems) that have common goals and requirements. [NIST SP 800-130]

A group of entities that have common goals and requirements (including security considerations) that have been specified in a common security policy. [NIST SP 800-130]

An environment or context that is defined by security models and a security architecture, including a set of resources and set of system entities that are authorized to access the resources. One or more security domains may reside in a single administrative domain. The traits defining a given security domain typically evolve over time. [Taxonomy] [OASIS SAML Glossary 2.0]

**Security Policy**
(undefined) [NIST FIPS 140-2]

The rules and requirements established by an organization that govern the acceptable use of its information and services, and the level and means for protecting the confidentiality, integrity, and availability of its information. [NIST SP 800-130]

A set of rules and practices that specify or regulate how a system or organization provides security services to protect resources. Security policies are components of security architectures. Significant portions of security policies are implemented via security services, using security policy expressions. [RFC2828] [Taxonomy] [OASIS SAML Glossary 2.0]

**Security Policy Expression**
A mapping of principal identities and/or attributes thereof with allowable actions. Security policy expressions are often essentially access control lists. [Taxonomy] [OASIS SAML Glossary 2.0]

**Security Service**
A processing or communication service that is provided by a system to give a specific kind of protection to resources, where said resources may reside with said system or reside with other systems, for example, an authentication service or a PKI-based document attribution and authentication service. A security service is a superset of AAA services. Security services typically implement portions of security policies and are implemented via security mechanisms. [RFC2828] [Taxonomy] [OASIS SAML Glossary 2.0]

**Security Strength**
A number associated with the amount of work (that is, the base 2 logarithm of the minimum number of operations) that is required to cryptanalyze a cryptographic algorithm or system. [NIST SP 800-130]

**Security Token**
a collection of claims. [OASIS IMI 1.0]

**Security Token Service**
a WS-Trust endpoint. [OASIS IMI 1.0]

An STS provides a standards-based method of converting security tokens across different formats. [ICAM SAML 2.0 WB SSO Profile 1.0.2]

**Seed Key**
a secret value used to initialize a cryptographic function or operation. [NIST FIPS 140-2]

**Semantics**
The intended meaning of acceptable sentences of a language. [NIST SP 800-130]

**Sensitive Information**
Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. [FICAM TFPAP 1.0.1]

**Server**
A system entity that provides a service in response to requests from clients. [FBCA CP 2.25]

An HTTP server (per [RFC2616]) capable of accepting OAuth- authenticated requests (Section 3). [IETF RFC 5849]

A system entity that provides a service in response to requests from clients. [SAFE-BioPharma CP 2.5]

**Service**
A set of related IT components provided in support of one or more business processes. [NIST IR 7693]

**Service Assessment Criteria**
A set of requirements levied upon specific organizational and other functions performed by electronic trust services and service providers. Services and service providers must comply with all applicable criteria to qualify for Kantara Initiative approval and earn the Kantara Initiative Mark. [Kantara IAF 1100]

**Service Provider**
Uses an Identity Assertion as part of managing access to its services. [InCommon IAAF 1.1]

Previously called the Target Site in the Shibboleth software implementation. For InCommon, an SP is a campus or other organization that makes online resources available to users based in part on information about them that it receives from other InCommon participants. [InCommon Glossary]

A role donned by a system entity where the system entity provides services to principals or other system entities. Session A lasting interaction between system entities, often involving a Principal, typified by the maintenance of some state of the interaction for the duration of the interaction. [OASIS SAML Glossary 2.0]

**Service Provisioning Markup Language**
An XML-based framework, developed by OASIS, for exchanging user, resource and service provisioning information between cooperating organizations. SPML relies on SAML for the exchange of authorization data. Several versions have been released including version 1.0 in 2003 and version 2.0 in 2006. [BAE Overview]

**Service Requester**
software acting on behalf of a party who wants to obtain a service through a digital network. [OASIS IMI 1.0]

**Session Authority**
A role donned by a system entity when it maintains state related to sessions. Identity providers often fulfill this role. [OASIS SAML Glossary 2.0]

**Session Hijack Attack**
An attack in which the Attacker is able to insert himself or herself between a Claimant and a Verifier subsequent to a successful authentication exchange between the latter two parties. The Attacker is able to pose as a Subscriber to the Verifier or vice versa to control session data exchange. Sessions between the Claimant and the Relying Party can also be similarly compromised. [NIST SP 800-63-1]

**Session Participant**
A role donned by a system entity when it participates in a session with at least a session authority. [OASIS SAML Glossary 2.0]

**Set Of Provisions**
A collection of practice and/or policy statements, spanning a range of standard topics, for use in expressing a CP or CPS employing the approach described in this framework. [IETF RFC 3647]

**Shared BAE Broker**
A BAE broker used by multiple departments or agencies to participate in Backend Attribute exchanges. [BAE Overview]

**Shared Secret**
A secret used in authentication that is known to the Claimant and the Verifier. [NIST SP 800-63-1]

A secret used in authentication that is known to the Claimant and the Verifier. [FICAM TFPAP 1.0.1]

**Shibboleth**
Software developed by Internet2 to enable the sharing of web resources that are subject to access controls such as user IDs and passwords. Shibboleth leverages institutional sign-on and directory systems to work among organizations by locally authenticating users and then passing information about them to the resource site to enable that site to make an informed authorization decision. The Shibboleth architecture protects privacy by letting institutions and individuals set policies that control what information about a user can be released to each destination. For more information on Shibboleth please visit http://shibboleth.internet2.edu/uses.html. [InCommon Glossary]

**Signatory**
A party that opts into and agrees to be bound by the AAS-defined agreements according to the specified procedures. [Kantara IAF 1100]

**Signature**
a cryptographic binding of a proof-of-possession and a digest. This covers both symmetric key-based and public key-based signatures. Consequently, non-repudiation is not always achieved. [OASIS IMI 1.0]

**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. [FBCA CP 2.25]

A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions. [SAFE-BioPharma CP 2.5]

**Signature Verification**
The process of checking the digital signature by reference to the original message and a given public key, thereby determining whether the digital signature was created for that same message using the private key that corresponds to the referenced public key. [ICAM SAML 2.0 WB SSO Profile 1.0.2]

**Signed Security Token**
a security token that is asserted and cryptographically endorsed by a specific authority (e.g. an X.509 certificate, a Kerberos ticket, or a self-issued Information Card). [OASIS IMI 1.0]

**Simple Object Access Protocol**
Lightweight XML-based messaging protocol used to encode the information in Web service request and response messages before sending them over a network. It consists of three parts: an envelope that defines a framework for describing what is in a message and how to process it, a set of encoding rules for expressing instances of application-defined data types, and a convention for representing remote procedure calls and responses. SOAP messages are independent of any operating system or protocol and may be transported using a variety of Internet protocols, including MIME and HTTP. [BAE Overview]

**Simple Power Analysis**
a direct (primarily visual) analysis of patterns of instruction execution (or execution of individual instructions), obtained through monitoring the variations in electrical power consumption of a cryptographic module, for the purpose of revealing the features and implementations of cryptographic algorithms and subsequently the values of cryptographic keys. [NIST FIPS 140-2]

**Single Sign-on**
Once an end user has authenticated their identity at an IdP, he or she may, by their choice, move among RPs that interoperate with the IdP without re-authenticating. In other words, the end user is seamlessly logged into any other RP that interoperates with the IdP. For privacy considerations, end users must take explicit actions to opt-in to SSO. SSO applies to assertion based ICAM member systems only. In addition, SSO is in effect only for the duration of the end user's current browser session and authentication session. An end user must opt-in to SSO each time he or she opens a new web browser session [ICAM SAML 2.0 WB SSO Profile 1.0.2]

**Site**
An informal term for an administrative domain in geographical or DNS name sense. It may refer to a particular geographical or topological portion of an administrative domain, or it may encompass multiple administrative domains, as may be the case at an ASP site. [OASIS SAML Glossary 2.0]

**Social Engineering**
The act of deceiving an individual into revealing sensitive information by associating with the individual to gain confidence and trust. [NIST SP 800-63-1]

**Software**
the programs and data components within the cryptographic boundary, usually stored on erasable media (e.g., disk), that can be dynamically written and modified during execution. [NIST FIPS 140-2]

Computer programs and associated data that may be dynamically written or modified during execution. [NIST IR 7693]

**Special Publication**
A type of publication issued by NIST. Specifically, the Special Publication 800-series reports on the Information Technology Laboratory's research, guidelines, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations. [NIST SP 800-63-1]

**Specified Service**
The electronic trust service which, for the purposes of an AAS assessment, is the subject of criteria set out in a particular SAC, or in an application for assessment, in a grant of an approval or other similar usage as may be found in various IAWG documentation. [Kantara IAF 1100]

**Split Knowledge**
a process by which a cryptographic key is split into multiple key components, individually sharing no knowledge of the original key, that can be subsequently input into, or output from, a cryptographic module by separate entities and combined to recreate the original cryptographic key. [NIST FIPS 140-2]

**Sponsored Partner**
A business partner that provides resources to a higher education institution, and is sponsored for participation in InCommon by a participating higher education institution. [InCommon Glossary]

**Standard**
document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines or charactersitics for activities or their results, aimed at the achievement of the optimum degreee of order in a given context [ISO-IEC Directives Part 2]

Something established by authority, custom, or general consent as a model or example. [NIST SP 800-130]

**State Of The Art**
developed stage of technical capability at a given time as regards products, processes and services, based on the relevant consolidated findings of science, technology and experienc [ISO-IEC Directives Part 2]

**Statement**
expression in the content of a document conveying information [ISO-IEC Directives Part 2]

**Status Information**
information that is output from a cryptographic module for the purposes of indicating certain operational characteristics or states of the module. [NIST FIPS 140-2]

**Status Word**
Two bytes returned by an integrated circuit card after processing any command that signify the success of or errors encountered during said processing. [NIST SP 800-73-3 Part 1]

Two bytes returned by an integrated circuit card after processing any command that signify the success of or errors encountered during said processing. [NIST SP 800-73-3 Part 2]

Two bytes returned by an integrated circuit card after processing any command that signify the success of or errors encountered during said processing. [NIST SP 800-73-3 Part 3]

**Steering Group**
[entity to] administer the process for policy and standards development for the Identity Ecosystem Framework in accordance with the Guiding Principles in this Strategy. The steering group will also ensure that accreditation authorities validate participants' adherence to the requirements of the Identity Ecosystem Framework [NSTIC Strategy]

**Store (key/metadata)**
To place a key/metadata into a medium (without making a copy) from which the key/metadata may be recovered. [NIST SP 800-130]

**Strong Man In The Middle Resistance**
A protocol is said to be strongly resistant to man-in-the-middle attack if it does not allow the Claimant to reveal, to an attacker masquerading as the Verifier, information (token secrets, authenticators) that can be used by the latter to masquerade as the true Claimant to the real Verifier. [FICAM TFPAP 1.0.1]

**Strongly Bound Credentials**
Credentials that describe the binding between a user and token in a tamper-evident fashion. (For more discussion, see Section 7.1.1.) [NIST SP 800-63-1]

The association between the identity and the token within strongly bound credentials cannot be easily undone. For example, a digital signature binds the identity to the public key in a public key certificate; tampering of this signature can be easily detected through signature validation. [FICAM TFPAP 1.0.1]

**Student Information System**
(undefined) [InCommon IAAF 1.1]

**Subject**
A person who is (or will be) registered with the IdP Operator [InCommon IAAF 1.1]

an individual or entity about whom claims are made by an Identity Provider. [OASIS IMI 1.0]

An entity that is able to use an electronic trust service subject to agreement with an associated subscriber. A subject and a subscriber can be the same entity. [Kantara IAF 1100]

A principal in the context of a security domain. SAML assertions make declarations about subjects. [OASIS SAML Glossary 2.0]

**Subject Certification Authority (subject CA)**
In the context of a particular CA-certificate, the subject CA is the CA whose public key is certified in the certificate (see also Issuing certification authority). [IETF RFC 3647]

**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). [FBCA CP 2.25]

In a hierarchical PKI, a CA whose certificate Signing Key is certified by another CA, and whose activities are constrained by that other CA (see superior CA). [SAFE-BioPharma CP 2.5]

**Subscriber**
A party who has received a credential or token from a CSP. [NIST SP 800-63-1]

An entity whose public key is contained in a certificate bound to the entity. [FBCA Cross-certification Methodology 3.0]

A Subscriber is an entity that (1) is the subject named or identified in a certificate issued to that entity, (2) holds a private key that corresponds to the public key listed in the certificate, and (3) does not itself issue certificates to another party. This includes, but is not limited to, an individual or network device [FBCA CP 2.25]

A party who has received a credential or token from a CSP. [FICAM TFPAP 1.0.1]

A party that has entered into an agreement to use an electronic trust service. A subscriber and a subject can be the same entity. [Kantara IAF 1100]

A subject of a certificate who is issued a certificate. [IETF RFC 3647]

**Subscriber Agreement**
An agreement between a CA and a subscriber that establishes the right and responsibilities of the parties regarding the issuance and management of certificates. [IETF RFC 3647]

**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). [FBCA CP 2.25]

In a hierarchical PKI, a CA who has certified the certificate Signing Key of another CA, and who constrains the activities of that CA. (See subordinate CA). [SAFE-BioPharma CP 2.5]

**Supplementary Informative Element**
element that provides additional information intended to assist the understanding or use of the document [ISO-IEC Directives Part 2]

**Support Contact**
The Support Contact is the primary contact for error handling. The Support Contact may be a help desk or a designated support person. [InCommon Glossary]

**Suspended State**
The key life cycle state used to temporarily remove a previously active key from that status, but making provisions for later returning the key to active status, if appropriate. [NIST SP 800-130]

**Symmetric Key**
A cryptographic key that is used to perform both the cryptographic operation and its inverse, for example to encrypt and decrypt, or create a message authentication code and to verify the code. [NIST SP 800-63-1]

A cryptographic key that is used to perform both the cryptographic operation and its inverse, for example to encrypt and decrypt, or create a message authentication code and to verify the code. [NIST FIPS 201-2]

**Syntax**
The rules for constructing acceptable sentences of a language. [NIST SP 800-130]

**Synthetic Identifier**
An identifier that is assigned to an asset in the context of some management domain. [NIST IR 7693]

**System**
A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. [NIST IR 7693]

**System And Communications Protection**
(undefined) [FICAM TFPAP 1.0.1]

**System Entity, Entity**
An active element of a computer/network system. For example, an automated process or set of processes, a subsystem, a person or group of persons that incorporates a distinct set of functionality. [RFC2828] [SAMLAgree] [OASIS SAML Glossary 2.0]

**System Equipment Configuration**
A comprehensive accounting of all system hardware and software types and settings. [FBCA CP 2.25]

**System High**
The highest security level supported by an information system. [NS4009] [FBCA CP 2.25]

**System Software**
the special software within the cryptographic boundary (e.g., operating system, compilers or utility programs) designed for a specific computer system or family of computer systems to facilitate the operation and maintenance of the computer system, and associated programs, and data. [NIST FIPS 140-2]

**TEMPEST**
a name referring to the investigation, study, and control of unintentional compromising emanations from telecommunications and automated information systems equipment. [NIST FIPS 140-2]

**TOE Security Functions**
used in the Common Criteria, a set of the TOE consisting of all hardware, software, and firmware that must be relied upon for the correct enforcement of the TOE Security Policy. [NIST FIPS 140-2]

**TOE Security Policy**
used in the Common Criteria, a set of rules that regulate how assets are managed, protected, and distributed within a Target of Evaluation. [NIST FIPS 140-2]

**Tamper Detection**
the automatic determination by a cryptographic module that an attempt has been made to compromise the physical security of the module. [NIST FIPS 140-2]

**Tamper Evidence**
the external indication that an attempt has been made to compromise the physical security of a cryptographic module. (The evidence of the tamper attempt should be observable by an operator subsequent to the attempt.) [NIST FIPS 140-2]

**Tamper Response**
the automatic action taken by a cryptographic module when a tamper detection has occurred (the minimum response action is the zeroization of plaintext keys and CSPs). [NIST FIPS 140-2]

**Target Of Evaluation**
an information technology product or system and associated administrator and user guidance documentation that is the subject of an evaluation. [NIST FIPS 140-2]

**Technical Contact**
The Technical Contact for InCommon serves as the primary point of contact for all technical issues for the organization participating in InCommon. The technical contact communicates with federation technical staff to ensure smooth operation of the federation's infrastructure. [InCommon Glossary]

**Technical Non-repudiation**
The contribution public key mechanisms to the provision of technical evidence supporting a non-repudiation security service. [FBCA CP 2.25]

**Technical Report**
document published by ISO or IEC containing collected data of a different kind from that normally published as an International Standard or Technical Specification [ISO-IEC Directives Part 2]

**Technical Specification**
document published by ISO or IEC for which there is the future possibility of agreement on an International Standard, but for which at present the required support for approval as an International Standard cannot be established, there is doubt on whether consensus has been achieved, the subject matter is still under technical development, or there is another reason precluding immidiate publicaiton as an International Standard [ISO-IEC Directives Part 2]

**Template**
A (constructed) BER-TLV data object whose value field contains specific BER-TLV data objects. [NIST SP 800-73-3 Part 2]

A (constructed) BER-TLV data object whose value field contains specific BER-TLV data objects. [NIST SP 800-73-3 Part 3]

**Template Generator**
In the PIV context a template generator is a software library providing facilities for the conversion of images conformant to FINGSTD to templates conformant to MINUSTD for storage on the PIV card. [NIST SP 800-85B]

**Template Matcher**
In the PIV context a matcher is a software library providing for the comparison of images conformant to FINGSTD and templates conformant to MINUSTD. The ouput of the mathcer, a similarity score, will be the basis of accept or reject decision. [NIST SP 800-85B]

**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. [NS4009] [FBCA CP 2.25]

Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. [FICAM TFPAP 1.0.1]

An adversary that is motivated and capable to violate the security of a target and has the capability to mount attacks that will exploit the target's vulnerabilities. [Kantara IAF 1100]

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. [SAFE-BioPharma CP 2.5]

**Time-out**
A period of time after which some condition becomes true if some event has not occurred. For example, a session that is terminated because its state has been inactive for a specified period of time is said to "time out". [OASIS SAML Glossary 2.0]

**Token**
Something that the Claimant possesses and controls (typically a cryptographic module or password) that is used to authenticate the Claimant's identity. [NIST SP 800-63-1]

Something that the Claimant possesses and controls (typically a key or password) used to authenticate the Claimant's identity. [FICAM TFPAP 1.0.1]

A physical device (or specialized software on a device such as a mobile phone) used in authentication. [InCommon IAAF 1.1]

Something that a claimant possesses and controls (typically a key or password) that is used to authenticate the claimant's identity. [Kantara IAF 1100]

A unique identifier issued by the server and used by the client to associate authenticated requests with the resource owner whose authorization is requested or has been obtained by the client. Tokens have a matching shared-secret that is used by the client to establish its ownership of the token, and its authority to represent the resource owner. [IETF RFC 5849]

**Token Authenticator**
The output value generated by a token. The ability to generate valid token authenticators on demand proves that the Claimant possesses and controls the token. Protocol messages sent to the Verifier are dependent upon the token authenticator, but they may or may not explicitly contain it. [NIST SP 800-63-1]

The value that is provided to the protocol stack to prove that the Claimant possesses and controls the token. Protocol messages sent to the Verifier are dependant upon the token authenticator, but they may or may not explicitly contain it. [FICAM TFPAP 1.0.1]

**Token Endpoint**
One of two defined authorization server endpoints, used by the client to exchange an authorization grant for an access token, typically with client authentication. [IETF ID OAuth 2.0]

**Token Secret**
The secret value, contained within a token, which is used to derive token authenticators. [NIST SP 800-63-1]

**Transient Pseudonym**
A privacy-preserving identifier assigned by an identity provider to identify a principal to a given relying party for a relatively short period of time that need not span multiple sessions. [OASIS SAML Glossary 2.0]

**Transport Layer Security**
An authentication and security protocol widely implemented in browsers and web servers. TLS is defined by [RFC 2246], [RFC 3546], and [RFC 5246]. TLS is similar to the older Secure Sockets Layer (SSL) protocol, and TLS 1.0 is effectively SSL version 3.1. NIST SP 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations specifies how TLS is to be used in government applications. [NIST SP 800-63-1]

**Trust**
A characteristic of an entity that indicates its ability to perform certain functions or services correctly, fairly, and impartially, along with assurance that the entity and its identifier are genuine. [NIST SP 800-130]

**Trust Anchor**
A public or symmetric key that is trusted because it is directly built into hardware or software, or securely provisioned via out-of-band means, rather than because it is vouched for by another trusted entity (e.g. in a public key certificate). [NIST SP 800-63-1]

One or more trusted public keys that exist at the base of a tree of trust or as the strongest link in a chain of trust and upon which a Public Key Infrastructure is constructed in a CKMS. [NIST SP 800-130]

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. [SAFE-BioPharma CP 2.5]

**Trust Anchor Store**
The location where trust anchor information is stored. [NIST SP 800-130]

**Trust Criteria**
Set of benchmarks used to measure an identity provider's technical and operational controls with respect to registration and issuance, tokens, token and credential management, the authentication process, and assertions. [FICAM TFPAP 1.0.1]

**Trust Framework**
Trust Framework Provider processes and controls for determining an identity provider's compliance to OMB M-04-04 Levels of Assurance. [FICAM TFPAP 1.0.1]

developed by a community whose members have similar goals and perspectives. It defines the rights and responsibilities of that community's participants in the Identity Ecosystem; specifies the policies and standards specific to the community; and defines the community-specific processes and procedures that provide assurance. A trust framework considers the level of risk associated with the transaction types of its participants; for example, for regulated industries, it could incorporate the requirements particular to that industry. Different trust frameworks can exist within the Identity Ecosystem, and sets of participants can tailor trust frameworks to meet their particular needs. In order to be a part of the Identity Ecosystem, all trust frameworks must still meet the baseline standards established by the Identity Ecosystem Framework. [NSTIC Strategy]

**Trust Framework Adoption Process**
(undefined) [FICAM TFPAP 1.0.1]

**Trust Framework Provider**
A TFP is an organization that defines or adopts an on-line identity trust model and then, certifies identity providers that are in compliance with that model. [FICAM TFPAP 1.0.1]

**Trust Framework Provider Adoption Process**
(undefined) [InCommon IAAF 1.1]

**Trust Identity**
a verifiable claim about a principal (e.g. name, identity, key, group, privilege, capability, etc). [OASIS IMI 1.0]

**Trust List**
Collection of trusted certificates used by Relying Parties to authenticate other certificates. [FBCA CP 2.25]

**Trusted Agent**
Entity authorized to act as a representative of an Entity in confirming Subscriber identification during the registration process. Trusted Agents do not have automated interfaces with Certification Authorities. [FBCA CP 2.25]

**Trusted Association**
The linking of a key with selected metadata elements so as to provide assurance that the key and its metadata are properly associated, originate from a particular source, have not been modified, and have been protected from unauthorized disclosure. [NIST SP 800-130]

**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". [FBCA CP 2.25]

**Trusted Channel**
A trusted and safe communication channel used to share sensitive information between two entities that are not collocated in a secure facility. [NIST SP 800-130]

**Trusted Path**
a means by which an operator and a TOE Security Function can communicate with the necessary confidence to support the TOE Security Policy. [NIST FIPS 140-2]

**Trusted Timestamp**
A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time. [FBCA CP 2.25]

**Trustmark**
[something] used to indicate that a product or service provider has met the requirements of the Identity Ecosystem, as determined by an accreditation authority. The trustmark itself, and the way it is presented, will be resistant to tampering and forgery; participants should be able to both visually and electronically validate its authenticity. The trustmark helps individuals and organizations make informed choices about the Identity Ecosystem-related practices of the service providers and identity media they select. [NSTIC Strategy]

**Trustmark Scheme**
the combination of criteria that is measured to determine service provider compliance with the Identity Ecosystem Framework. [NSTIC Strategy]

**Trustworthy System**
Computer hardware, software and procedures that: (1) are reasonably secure from intrusion and misuse; (2) provide a reasonable level of availability, reliability, and correct operation; (3) are reasonably suited to performing their intended functions; and (4) adhere to generally accepted security procedures. [FBCA CP 2.25]

**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. [NS4009] [FBCA CP 2.25]

**URI Reference**
A URI that is allowed to have an appended number sign (#) and fragment identifier. [RFC2396] Fragment identifiers address particular locations or regions within the identified resource. XML Extensible Markup Language, abbreviated XML, describes a class of data objects called XML documents and partially describes the behavior of computer programs which process them. [XML] [OASIS SAML Glossary 2.0]

**Ultimate SOAP Receiver**
The SOAP receiver that is a final destination of a SOAP message. It is responsible for processing the contents of the SOAP body and any SOAP header blocks targeted at it. In some circumstances, a SOAP message might not reach an ultimate SOAP receiver, for example because of a problem at a SOAP intermediary. An ultimate SOAP receiver cannot also be a SOAP intermediary for the same SOAP message. [WSGloss] [OASIS SAML Glossary 2.0]

**Uniform Resource Identifier**
The name for identifying an abstract or physical resource. [InCommon Glossary]

A compact string of characters for identifying an abstract or physical resource. [RFC2396] URIs are the universal addressing mechanism for resources on the World Wide Web. Uniform Resource Locators (URLs) are a subset of URIs that use an addressing scheme tied to the resource's primary access mechanism, for example, their network "location". [OASIS SAML Glossary 2.0]

**Uniform Resource Locator**
The address of a resource accessible on the Internet. URLs are a subset of URIs. [InCommon Glossary]

**Uniform Resource Name**
Refers to the subset of URIs that are required to remain globally unique and persistent even when the resource ceases to exist or becomes unavailable. [InCommon Glossary]

**Unlinkability**
Assurance that two or more related events in an information processing system cannot be associated with each other in CKMS-supported communications. [NIST SP 800-130]

**Unobservability**
Assurance that an observer is unable to identify or make inferences about the parties involved in a transaction in CKMS-supported communications. [NIST SP 800-130]

**Unsigned Security Token**
Aa security token that is not cryptographically endorsed by a specific authority (e.g. a security token backed by shared secrets such as usernames and passwords). [OASIS IMI 1.0]

**Unverified Name**
A Subscriber name that is not verified as meaningful by identity proofing. [NIST SP 800-63-1]

**Update (a Certificate)**
The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, arechanged by issuing a new certificate. [FBCA CP 2.25]

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. [SAFE-BioPharma CP 2.5]

**User**
an individual or a process (subject) acting on behalf of the individual that accesses a cryptographic module in order to obtain cryptographic services. [NIST FIPS 140-2]

An individual authorized by an organization and its policies to use an information system, one or more of its applications, its security procedures and services, and a supporting CKMS. [NIST SP 800-130]

A natural person who makes use of a system and its resources for any purpose [SAMLAgree] [OASIS SAML Glossary 2.0]

**User Agent**
Typically a web browser, used by the Subject to authenticate to the IdP and convey the assertion to the SP. [InCommon IAAF 1.1]

**User-agent**
The end user's Web browser which implements HTTP/1.1 [RFC2616]. [OpenID Authentication 2.0]

**User-supplied Identifier**
An Identifier that was presented by the end user to the Relying Party, or selected by the user at the OpenID Provider. During the initiation phase of the protocol, an end user may enter either their own Identifier or an OP Identifier. If an OP Identifier is used, the OP may then assist the end user in selecting an Identifier to share with the Relying Party. [OpenID Authentication 2.0]

**Valid**
In reference to an ID, the quality of not being expired or revoked. [NIST SP 800-63-1]

**Validate**
To test cryptographic parameters or modules and confirm the test results to obtain assurance that the tested implementation is appropriate for use. [NIST SP 800-130]

**Validation**
The process of demonstrating that the system under consideration meets in all respects the specification of that system. [INCITS/M1-040211] [NIST FIPS 201-2]

The process of identification of certificate applicants. [InCommon Glossary]

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. [IETF RFC 3647]

**Validation Authorities**
NIST and CSE. [NIST FIPS 140-2]

**Validity Period**
The lifespan of a public key certificate [NIST SP 800-130]

**Verification**
(undefined) [NIST FIPS 201-2]

Establishment of the truth or correctness of something by investigation of evidence [Kantara IAF 1100]

**Verified Name**
A Subscriber name that has been verified by identity proofing. [NIST SP 800-63-1]

**Verifier**
An entity that verifies the Claimant's identity by verifying the Claimant's possession and control of a token using an authentication protocol. To do this, the Verifier may also need to validate credentials that link the token and identity and check their status. [NIST SP 800-63-1]

An entity that verifies the Claimant's identity by verifying the Claimant's possession of a token using an authentication protocol. To do this, the Verifier may also need to validate credentials that link the token and identity and check their status. [FICAM TFPAP 1.0.1]

Validates the correctness of offered authentication material. [InCommon IAAF 1.1]

**Verifier Impersonation Attack**
A scenario where the Attacker impersonates the Verifier in an authentication protocol, usually to capture information that can be used to masquerade as a Claimant to the real Verifier. [NIST SP 800-63-1]

**Weak Man In The Middle Resistance**
A protocol is said to be weakly resistant to man-in-the-middle attacks if it provides a mechanism for the Claimant to determine whether he or she is interacting with the real Verifier, but still leaves the opportunity for the non-vigilant Claimant to reveal a token authenticator (to an unauthorized party) that can be used to masquerade as the Claimant to the real Verifier. [FICAM TFPAP 1.0.1]

**Weakly Bound Credentials**
Credentials that describe the binding between a user and token in a manner than can be modified without invalidating the credential. (For more discussion, see Section 7.1.1.) [NIST SP 800-63-1]

The association between the identity and the token within a weakly bound credential can be readily undone and a new association can be readily created. For example, a password file is a weakly bound credential since anyone who has "write" access to [FICAM TFPAP 1.0.1]

**Website**
A set of related web pages that are prepared and maintained as a collection in support of a single purpose [NIST IR 7693]

**Where Are You From**
A server used by the Shibboleth software to determine what a user's home organization is. [InCommon Glossary]

**XML Attribute**
An XML data structure that is embedded in the start-tag of an XML element and that has a name and a value. (example removed) See also attribute. [OASIS SAML Glossary 2.0]

**XML Element**
An XML data structure that is hierarchically arranged among other such structures in an XML document and is indicated by either a start-tag and end-tag or an empty tag. (example removed) [OASIS SAML Glossary 2.0]

**XML Namespace**
A collection of names, identified by a URI reference, which are used in XML documents as element types and attribute names. An XML namespace is often associated with an XML schema. For example, SAML defines two schemas, and each has a unique XML namespace. [OASIS SAML Glossary 2.0]

**XML Schema**
The format developed by the World Wide Web Consortium (W3C) for describing rules for a markup language to be used in a set of XML documents. In the lowercase, a "schema" or "XML schema" is an individual instance of this format. For example, SAML defines two schemas, one containing the rules for XML documents that encode security assertions and one containing the rules for XML documents that encode request/response protocol messages. Schemas define not only XML elements and XML attributes, but also datatypes that apply to these constructs. [OASIS SAML Glossary 2.0]

**Yadis Document**
A document containing a Yadis Resource Descriptor [Yadis 1.0]

**Yadis ID**
A identifier used with one or more Yadis Services. A Yadis ID may be a URL; it may be any other identifier, such as an XRI, that can be resolved to a URL. [Yadis 1.0]

**Yadis Resource**
A computer software process (or system of processes) that provides one or more services located using the Yadis Protocol. [Yadis 1.0]

**Yadis Resource Descriptor**
An element of a Yadis document identifying the services that are available using a Yadis ID. [Yadis 1.0]

**Yadis Service**
A service provided by a Yadis Resource. [Yadis 1.0]

**Yadis URL**
A Yadis ID, if it is a URL, otherwise the URL to which that Yadis ID resolves. A Yadis URL may be used in the Yadis Protocol to obtain a Yadis Resource Descriptor. [Yadis 1.0]

**Yadis User**
An entity using a Yadis ID as an identifier. [Yadis 1.0]

**Yadis User Agent**
An agent acting on behalf of a Yadis User (for example, a regular web browser). [Yadis 1.0]

**Zero-knowledge Password Protocol**
A password based authentication protocol that allows a claimant to authenticate to a Verifier without revealing the password to the Verifier. Examples of such protocols are EKE, SPEKE and SRP [NIST SP 800-63-1]

**Zeroization**
a method of erasing electronically stored data, cryptographic keys, and CSPs by altering or deleting the contents of the data storage to prevent recovery of the data. [NIST FIPS 140-2]

**Zeroize**
Overwrite a memory location with data consisting entirely of bits with the value zero so that the data is destroyed and not recoverable. This is often contrasted with deletion methods that merely destroy reference to data within a file system rather than the data itself. [NIST SP 800-63-1]

A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data. [FIPS1401 [FBCA CP 2.25]

A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data. [FIPS1401] [SAFE-BioPharma CP 2.5]

# ACRONYMS

| | |
|---|---|
| A | Application |
| AA | Attribute Authority |
| AAS | Assurance Assessment Scheme |
| ABA | American Bar Association |
| ABAC | Attribute Based Access Control |
| ACL | Access Control List |
| ACR | Annual Conformity Review, Access Control Rule |
| ACS | Access Control System |
| AES | Advanced Encryption Standard |
| AID | Application Identifier, Application IDentifier |
| AIM | Association for Automatic Identification and Mobility |
| AL | Assurance Level |
| AM | Authorization Manager |
| AMI | Attribute Management Interface |
| ANS | American National Standard |
| ANSI | American National Standards Institute |
| AP | Attribute Provider |
| APDU | Application Protocol Data Unit |
| API | Application Programming Interface, Application Program Interface |
| APT | Application Property Template |
| ARB | Assurance Review Board |
| ARC | Automated Record Checks |
| ARP | Attribute Release Policy |
| ASCII | American Standard Code for Information Interchange |
| ASI | Attribute Service Interface |
| ASN.1 | Abstract Syntax Notation One |
| ASTM | American Society for Testing and Materials |
| AWG | Architecture Working Group |
| BAE | Backend Attribute Exchange |
| BDB | Biometric Data Block |
| BER | Basic Encoding Rules |
| BER-TLV | Basic Encoding Rules Tag-Length-Value |
| BIOS | Basic Input/Output System |
| BSI | Basic Services Interface |
| C&A | Certification and Accreditation |
| CA | Certificate Authority, Certification Authority, Certificate (Certification) Authority |
| CAK | Card Authentication Key |
| CAP | Credential Assessment Profile |
| CAPP | Controlled Access Protection Profile |
| CAPTCHA | Completely Automated Public Turing Test To Tell Computers And Humans Apart |
| CARL | Certification Authority Revocation List, Certificate Authority Revocation List |
| CBC | Cipher Block Chaining |
| CBEFF | Common Biometric Exchange Formats Framework |
| CC | Common Criteria |
| CCC | Card Capability Container |
| CCM | Counter with Cipher Block Chaining-Message Authentication Code |
| CHUID | Cardholder Unique Identifier, Card Holder Unique Identifier |
| CIDR | Classless Inter-Domain Routing |
| CIO | Chief Information Officers |
| CISA | Certified Information System Auditor, Certified Information Systems Auditor |
| CKMS | Cryptographic Key Management System, Cryptographic Key Management System(s) |
| CLA | Class (first) byte of a card command |
| cm | Centimeter |

| | |
|---|---|
| CMA | Certificate Management Authority |
| CMS | Cryptographic Message Syntax, Certificate Management System, Card Management System |
| CMTC | Card Management System to the Card |
| CMVP | Cryptographic Module Validation Program |
| COMSEC | Communications Security |
| COTS | Commercial Off-the-shelf, Commercial Off-the-Shelf, Commercial Off-The-Shelf, Commercial Off the Shelf |
| CP | Certificate Policy |
| CPE | Common Platform Enumeration |
| CPS | Certification Practice Statement |
| CPWG | Certificate Policy Working Group |
| CRL | Certificate Revocation List, Certificate revocation List |
| CSE | Communications Security Establishment, Communications Security Establishment of the Government of Canada |
| CSOR | Computer Security Objects Registry, Computer Security Object Registry |
| CSP | Credential Service Provider, Critical Security Parameter |
| CSR | Certificate Signing Request |
| CSRF | Cross Site Request Forgery |
| CTC | Cardholder to Card |
| CTE | Cardholder to External System |
| D | Domain |
| DAM | Draft Amendment |
| DER | Distinguished Encoding Rules |
| DES | Data Encryption Standard |
| DG | Data Group |
| DHS | Department of Homeland Security |
| DN | Distinguished Name |
| DNS | Domain Name Service |
| DNSSEC | Domain Name System Security Extensions |
| DOB | Date of Birth |
| DoB | Date Of Birth, Date of Birth |
| DOD | Departmentof Defense |
| DPA | Differential Power Analysis |
| dpi | Dots Per Inch |
| DSA | Digital Signature Algorithm |
| DSS | Digital Signature Standard |
| DTR | Derived Test Requirement, Derived Test Requirements |
| E-Mail | Electronic Mail |
| EAL | Common Criteria Evaluation Assurance Level |
| EAP | Extensible Authentication Protocol |
| EC | CDH Elliptic Curve Cryptography Cofactor Diffie-Hellman, Elliptic Curve |
| ECB | Electronic Codebook |
| ECC | Elliptic Curve Cryptography |
| ECDH | Elliptic Curve Diffie-Hellman |
| ECDSA | Elliptic Curve Digital Signature Algorithm , Elliptic Curve Digital Signature Algorithm |
| EDC | Error Detection Code |
| EEPROM | Electronically-Erasable Programmable Read-Only Memory |
| EFP | Environmental Failure Protection |
| EFS | Electronic File System |
| EFT | Environmental Failure Testing |
| EGCA | E-governance Certification Authorities |
| EGMA | E-governance Metadata Authority |
| EGTS | E-governance Trust Services, E-Governance Trust Services |
| EMC | Electromagnetic Compatibility |
| EMI | Electromagnetic Interference |
| EPROM | ErasableProgrammable Read-Only Memory |
| ERC | Enhanced Reliability Check |
| ERT | Emergency Response Team |

| | |
|---|---|
| ETS | Electronic Trust Service |
| ETSP | Electronic Trust Service Provider |
| EU | European Union |
| FAR | Federal Acquisition Regulations |
| FASC-N | Federal Agency Smart Credential - Number, Federal Agency Smart Credential Number |
| FBCA | Federal Bridge Certification Authority |
| FBI | Federal Bureau of Investigation |
| FCC | Federal Communications Commission |
| FCIOC | Federal Chief Information Officers Council |
| FED-STD | Federal Standard |
| FICAM | Federal Identity, Credentialing And Access Management, Federal Identity, Credentialing and Access Management |
| FICC | Federal Identity Credentialing Committee |
| FIPS | Federal Information Processing Standard, Federal Information Processing Standards, PUB FIPS Publication, Federal Information Processing Standard Publication, (US) Federal Information Processing Standard Publication |
| FISMA | Federal Information Security Management Act |
| FOPP | Federation Operating Policies And Practices, Federation Operation Policies And Practices, Federation Operating Policies and Practices |
| FPKI | Federal Public Key Infrastructure |
| FPKI MA | FBCA Management Authority |
| FPKI PA | Federal Public Key Infrastructure Policy Authority |
| FPKI-E | Federal PKI Version 1 Technical Specifications: Part E – X.509 Certificate and CRL Extensions Profile |
| FPKIMA | Federal Public Key Infrastructure Management Authority |
| FPKIPA | Federal Public Key Infrastructure Policy Authority, Federal PKI Policy Authority |
| FPKISC | Federal PKI Steering Committee |
| FQDN | Fully-Qualified Domain Name |
| FR | Framework Requirement |
| fr | Framework Response |
| FSM | Finite State Model |
| FT | Framework Topic |
| GPEA | Government Paperwork Elimination Act of 1998 |
| GSA | General Services Administration, U.S. General Services Administration |
| GSC-IAB | Government Smart Card Interagency Advisory Board |
| GSC-IAM | Government Smart Card Interagency Advisory Board |
| GSC-IS | Government Smart Card Interoperability Specification |
| GUID | Global Unique Identification Number, Globally Unique Identifier |
| HAG | High Assurance Guard |
| HDL | Hardware Description Language |
| HMAC | Hash-based Message Authentication Code, Hash-Based Message Authentication Code, Keyed-Hash Message Authentication Code |
| HR | Human Resources |
| HSM | Hardware Security Module |
| HSPD | Homeland Security Presidential Directive |
| HSPD-12 | Homeland Security Presidential Directive |
| HTTP | Hypertext Transfer Protocol, HyperText Transfer Protocol |
| HTTPS | SSL for HTTP, HyperText Transfer Protocol Secure |
| I&A | Identification and Authentication |
| IAAF | Identity Assurance Assessment Framework |
| IAB | Interagency Advisory Board |
| IAF | Identity Assurance Framework |
| IAP | Identity Assurance Profile |
| IAQ | Identity Assurance Qualifier |
| IAWG | Identity Assurance Work Group |
| IC | Integrated Circuit |
| ICAM | Identity, Credential, And Access Management, Identity, Credential, and Access Management |
| ICAMSC | Identity, Credential, And Access Management Sub Committee, Identity, Credential, and Access Management Subcommittee, Identity, Credentialing and Access Management Sub Committee, Identity, Credential, and Access Management Sub Committee |

| | |
|---|---|
| ICC | Integrated Circuit Card , Integrated Circuit Card, Integrated Circuit Chip |
| ID | Identifier, Identity Document, Identification |
| IdM | Identity Management |
| IdMS | Identity Management System |
| IDP | Identity Provider |
| IdP | Identity Provider |
| IdPO | Idp Operator, Identity Provider Operator, IdP Operator |
| IDS | Intrusion Detection System |
| IEC | International Electrotechnical Commission , International Electrotechnical Commission |
| IETF | Internet Engineering Task Force |
| IG | Implementation Guidance |
| IKE | Internet Key Exchange |
| INCITS | International Committee for Information Technology Standards, InterNational Committee for Information Technology Standards |
| INS | Instruction (second) byte of a card command |
| IP | Internet Protocol |
| IPS | Intrusion Protection System |
| IPSec | Internet Protocol Security |
| ISDN | Integrated Services Digital Network |
| ISIMC | Information Security And Identity Management Committee, Information Security and Identity Management Committee |
| ISO | International Organization for Standardization |
| ISO/IEC | International Organization for Standardization/International Electrotechnical Commission |
| ISSO | Information System Security Officer, Information Systems Security Officer |
| IT | Information Technology |
| ITL | Information Technology Laboratory |
| ITSEC | Information Technology Security Evaluation Criteria |
| IV | Initialization Vector |
| K | Key |
| KDF | Key Derivation Function |
| KMM | Key Management Message |
| LACS | Logical Access Control System |
| LDAP | Lightweight Directory Access Protocol |
| LDIF | Lightweight Directory Inter-exchange Format |
| LI | Locale Identifier |
| LOA | Level Of Assurance, Level of Assurance |
| LRA | Local Registration Authority |
| LSB | Least Significicant Bit, Least Significant Bit |
| LUID | Locally Unique Identifier |
| M | Message |
| MAC | Message Authentication Code, Media Access Control |
| MitM | Man-in-the-middle Attack |
| mm | Millimeter |
| MOA | Memorandum Of Agreement, Memorandum of Agreement |
| MRTD | Machine Readable Travel Document |
| MSB | Most Significant Bit , Most Significant Bit |
| MWR | Morale, Welfare, and Recreation |
| N | Network |
| NAC | National Agency Check |
| NACI | National Agency Check with Written Inquiries |
| NCHC | National Criminal History Check |
| NIST | National Institute Of Standards And Technology, National Institute of Standards and Technology , National Institute of Standards and Technology |
| NISTIR | National Institute of Standards and Technology Interagency Report |
| NPE | Non-person Entity |
| NPIVP | NIST Personal Identity Verification Program |
| NSA | National Security Agency |
| NSTISSI | National Security Telecommunications and Information Systems Security Instruction |

| | |
|---|---|
| NTIS | National Technical Information Service |
| NTP | Network Time Protocol |
| NVLAP | National Voluntary Laboratory Accreditation Program |
| OAEP | Optimal Asymmetric Encryption Padding |
| OASIS | Organization for the Advancement of Structured Information Standards |
| OCC | On-Card Biometric Comparison |
| OCSP | Online Certificate Status Protocol |
| OFB | Output Feed Back |
| OGP | Office Of Governmentwide Policy, Office of Governmentwide Policy |
| OID | Object Identifier |
| OMB | Office Of Management And Budget, Office Of Management And Budget (US Federal Government), Office of Management and Budget, Office of Management and Budget , Office Of Management And Budget (US Federal government) |
| OP | Openid Provider |
| OPM | Office of Personnel Management |
| OTAR | Over-The-Air Rekeying |
| P1 | First parameter of a card command |
| P2 | Second parameter of a card command |
| PA | Participant Agreement |
| PACS | Physical Access Control System |
| PAS | Publicly Available Specification |
| PC/SC | Personal Computer/Smart Card |
| PCI | PIV Card Issuer |
| PDF | Portable Data File |
| PDP | Policy Decision Point |
| PDS | PKI Disclosure Statement |
| PEP | Policy Enforcement Point |
| PI | Person Identifier |
| PIA | Privacy Impact Assessment |
| PII | Personally Identifiable Information, Personal Identifying Information |
| PIN | Personal Identification Number |
| PIV | Personal Identity Verification Card, Personal Identity Verification |
| PIV-C | PIV Compatible |
| PIV-I | PIV Interoperable , Personal Identity Verification Interoperable, Personal Identity Verification – Interoperable |
| PIX | Proprietary Identifier eXtension, Proprietary Identifier extension |
| PK | Public Key |
| PKC | Public-Key Cryptography |
| PKCS | Public-Key Cryptography Standards, Public-Key Cryptographic Standards, Public Key Cryptography Standard, Public Key Certificate Standard |
| PKI | Public Key Infrastructure, Public Key Infrastructure |
| PKI-AUTH | PKI-PIV Authentication Key |
| PKI-CAK | Pki-card Authentication Key |
| PKIX | Public Key Infrastructure (X.509) (IETF Working Group), Public Key Infrastructure X.509 |
| PMA | Policy Management Authority |
| POP | Participant Operating Practices |
| PRI | Protected Resource Interface |
| PROM | Programmable Read-Only Memory |
| PSS | Probabilistic Signature Scheme |
| PUK | PIN Unblocking Key |
| PW | Password |
| RA | Registration Authority |
| RAM | Random Access Memory |
| REST | Representational State Transfer |
| RFC | Request for Comments, Request For Comment, Request for Comment, Request For Comments |
| RFU | Reserved for Future Use |
| RID | Registered application provider IDentifier, Registered application provider Identifier |
| RNG | Random Number Generator |

| | |
|---|---|
| ROM | Read-Only Memory |
| RP | Relying Party, Resource Provider |
| RPA | Relying Party Agreement |
| RSA | Rivest Shamir Adleman, Rivest, Shamir, Adleman, Rivest, Shamir and Adleman (Algorithm), Rivest-Shamir-Adleman (encryption algorithm) |
| S/MIME | Secure/Multipurpose Internet Mail Extensions, Secure Multipurpose Internet Mail Extension |
| SAC | Service Assessment Criteria |
| SAML | Security Assertion Markup Language, Security Assertion Markup Language |
| SBH | Signature Block Header |
| SC | System And Communications Protection, System and Communications Protection |
| SCAP | Security Content Automation Protocol |
| SCEPACS | Smart Card Enabled Physical Access Control System |
| SES | Senior Executive Service |
| SHA | Secure Hash Algorithm |
| SHA-1 | Secure Hash Algorithm, Version 1 |
| SIS | Student Information System |
| SK | Secret Key |
| SLO | Single Log-out |
| SOAP | Simple Object Access Protocol |
| SP | Special Publication, Service Provider |
| SPA | Simple Power Analysis |
| SPML | Service Provisioning Markup Language |
| SQL | Structured Query Language |
| SSA | Social Security Administration |
| SSH | Secure Shell |
| SSL | Secure Sockets Layer, Secure Socket Layer |
| SSO | Single Sign-on |
| SSP | Shared Service Providers, Shared Service Provider |
| STS | Security Token Service |
| SW1 | First byte of a two-byte status word |
| SW2 | Second byte of a two-byte status word |
| TA | Trusted Agent |
| TDEA | Triple Data Encryption Standard |
| TFP | Trust Framework Provider |
| TFPA | Trust Framework Adoption Process |
| TFPAP | Trust Framework Provider Adoption Process, Trust Framework Provider Application Process, Trust Framework Adoption Process |
| TIG | Technical Implementation Guidance |
| TLS | Transport Layer Security |
| TLV | Tag-Length-Value , Tag-Length-Value |
| TOE | Target Of Evaluation, Target of Evaluation |
| TR | Technical Report |
| TS | Technical Specification |
| TSA | Transportation Security Administration |
| TSDM | Trusted Software Development Methodology |
| TSF | TOE Security Functions, Target of Evaluation Security Functions |
| TSP | TOE Security Policy, Target of Evaluation Security Policy |
| U.S.C. | United States Code |
| UPN | User Principal Name |
| UPS | Uninterrupted Power Supply |
| URI | Uniform Resource Identifier |
| URL | Uniform Resource Locator |
| URN | Uniform Resource Name |
| US | United States |
| USB | Universal Serial Bus |

| | |
|---|---|
| UUID | Universally Unique IDentifier , Universally Unique IDentifier, Universally Unique Identifier, Universally Unique Identifier (defined by RFC 4122) |
| VM | Virtual Machine |
| VPN | Virtual Private Network |
| W3C | World Wide Web Consortium |
| WAYF | Where Are You From |
| WFN | Well-Formed Name |
| WWW | World Wide Web |
| xAL | extensible Address Language |
| XML | Extensible Markup Language |
| xNL | extensible Naming Language |
| XSD | XML Schema |
| XSS | Cross Site Scripting |

# REFERENCES


| | |
|---|---|
| **[BAE Overview]** | Backend Attribute Exchange (BAE) v2.0 Overview |
| **[FBCA CP 2.25]** | X.509 Certificate Policy For The Federal Bridge Certification Authority |
| **[FBCA Cross-certification Methodology 3.0]** | Criteria and Methodology for Cross-certification with the U.S. Federal Bridge Certification Authority |
| **[FICAM TFPAP 1.0.1]** | FICAM Trust Framework Provider Adoption Process (TFPAP) For Levels of Assurance 1, 2, and Non-PKI 3 |
| **[ICAM SAML 2.0 WB SSO Profile 1.0.2]** | Security Assertion Markup Language (SAML) 2.0 Web Browser Single Sign-on (SSO) Profile |
| **[IETF ID OAuth 2.0]** | The OAuth 2.0 Authorization Framework |
| **[IETF ID SCIM 1.0]** | Simple Cloud Identity Management: Protocol 1.0 |
| **[IETF RFC 3647]** | Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework |
| **[IETF RFC 5849]** | The OAuth 1.0 Protocol |
| **[ISO-IEC Directives Part 2]** | ISO/IEC Directives, Part 2: Rules for the structure and drafting of International Standards |
| **[InCommon Glossary]** | InCommon Glossary |
| **[InCommon IAAF 1.1]** | InCommon Identity Assurance Assessment Framework |
| **[InCommon IAP 1.1]** | Identity Assurance Profiles Bronze and Silver |
| **[Kantara IAF 1100]** | Identity Assurance Framework: Glossary |
| **[Kantara UMA]** | User-Managed Access (UMA) Core Protocol |
| **[NIST FIPS 140-2]** | SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES |
| **[NIST FIPS 201-2]** | Personal Identity Verification (PIV) of Federal Employees and Contractors |
| **[NIST IR 7693]** | Specification for Asset Identification 1.1 |
| **[NIST SP 800-130]** | A Framework for Designing Cryptographic Key Management Systems |
| **[NIST SP 800-63-1]** | Electronic Authentication Guideline |
| **[NIST SP 800-73-3 Part 1]** | Interfaces for Personal Identity Verification - Part 1: End-Point PIV Card Application Namespace, Data Model and Representation |
| **[NIST SP 800-73-3 Part 2]** | Interfaces for Personal Identity Verification - Part 2: End-Point PIV Card Application Card Command Interface |
| **[NIST SP 800-73-3 Part 3]** | Interfaces for Personal Identity Verification - Part 3: End-Point PIV Client Application Programming Interface |
| **[NIST SP 800-73-3 Part 4]** | Interfaces for Personal Identity Verification - Part 4: The PIV Transitional Interfaces and Data Model Specification |
| **[NIST SP 800-85B]** | PIV Data Model Test Guidelines |
| **[NSTIC Strategy]** | NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE, Enhancing Online Choice, Efficiency, Security, and Privacy |
| **[OASIS IMI 1.0]** | Identity Metasystem Interoperability Version 1.0 |
| **[OASIS SAML Glossary 2.0]** | Glossary for the OASIS Security Assertion Markup Language (SAML) V2.0 |
| **[OpenID Authentication 2.0]** | OpenID Authentication 2.0 |
| **[SAFE-BioPharma CP 2.5]** | SAFE-BioPharma Certificate Policy |
| **[Yadis 1.0]** | Yadis Specification 1.0 |