ICAM Lexicon

24 March 2011

Prepared by:

National Security Systems

Identity, Credentialing and Access Management Focus Group

Version 0.5

Version	Description of Changes	Date
0.1	Draft Release Date	12OCT
0.2	Addition of terms from GFIPM and CNSS 1300	13OCT
0.3	Revised per first iteration of commenting within Focus Group (see attached comment matrix)	2NOV
0.4	Revised per second iteration of commenting provided by the ICAMSC COI (see attached)	18JAN
0.5	Revised per third iteration of commenting provided by the ISIMC COI (see attached)	22MAR

Purpose

Since the introduction of Identity, Credentialing and Access Management (ICAM) enterprise technologies and related standards across the U.S. Government, agencies have adopted ICAM terminology and often adjusted terms to suit their environments, frequently causing some confusion as the government migrates to an increasingly collaborative environment.

The purpose of this Lexicon is to compile a comprehensive list of Identity, Credential, and Access Management (ICAM) related definitions currently being used throughout multiple organizations within the Federal Government, identify any divergence in terminology, and select a preferred term and definition for continued usage within the Committee on National Security Systems (CNSS) as well as the rest of the Federal Government. It was compiled using the FICAM Roadmap as the baseline compared against relevant issuances within the standards, the Federal, and the general ICAM community. Multiple definitions are provided for each term; therefore, the preferred term and definition are listed first; alternate terminology has been provided to highlight where organizations have used divergent terms to describe similar concepts.

Background

The following sources were chosen based on the following rationale:

1. Internationally Accepted Standards (e.g. International Organization for Standardization)
2. National standards, approved federal documentation (e.g. National Institute for Science and Technology) and,
3. Direct relation to established ICAM programs (e.g. Defense Information Systems Agency)

One source that is more geared toward ICAM in industry is ITUwiki. This site provides a "living," list of ICAM related terms from a multitude of sources, including NIST, the World Wide Web Consortium (W3C), as well as educational sources. A link to this list can be found below:
http://www.ituwiki.com/Living_List_of_Identity_Management_Terminology

Sources

The Lexicon employs several acronyms to reference specific sources. A list of those sources is as follows:

AASC: Authorization and Attributes Services Committee, established at the direction of the Department of Defense and Office of the Director of National Intelligence Chief Information Officers.
Document: Authorization & Attributes Glossary Unclassified (08DEC2009)
Location: https://www.intelink.gov/sites/ictg/IdAM/AAS/Attributes_WG/Shared Documents/AASC-Glossary-Draft.doc

CNSS: Committee on National Security Systems Instructions
Document 1: CNSS Instruction 4009, National Information Assurance (IA) Glossary (26APR2010)
Document 2: CNSS Instruction 1300, Public Key Infrastructure, X509 Certificate Policy (OCT2009)
Location: http://www.cnss.gov/instructions.html

DHS, NIPP: Department of Homeland Security, National Infrastructure Protection Plan
Location: http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

DISA: Defense Information Systems Agency, PEO-MA, Identity Management Division (IA4)
Document 1: Policy Based Access Control Engineering Blueprint (16MAR2010)
Document 2: Draft Security Frameworks Comparison (13JAN2010)
Location: https://www.us.army.mil/suite/grouppage/112341

DoD: Department of Defense, Assistant Secretary of Defense for Networks and Information Integration
Document 1: Department of Defense Privilege Management Roadmap (DoD PvM; 6JAN2010)
Location: https://www.us.army.mil/suite/grouppage/112341
Document 2: Department of Defense Identity Management Strategic Plan (DoD IdM; APR2009)
Location: http://cio-nii.defense.gov/docs/DoDCIO_Strat_Plan.pdf
Document 3: Global Information Grid 2.0 ORA
Location: https://www.intelink.gov/wiki/GIG_2.0#.28U.29_GIG_2.0_Characteristics
Various DoD Issuances have also been cited and can be found at the following location:
http://www.dtic.mil/whs/directives/

ESM: National Security Agency (NSA) Enterprise Security Management (ESM)
Document 1: Enterprise Security Management: A Context Overview (20MAR2009)
Document 2: Enterprise Security Management: Concept of Operations (28JAN2010)
Document 3: Enterprise Security Management: Appendix A: Glossary
Location: https://www.intelink.gov/inteldocs/browse.php?fFolderId=40082

FEA: Federal Enterprise Architecture Practice Guidance (NOV2007), Office of Management and Budget
Location: http://www.whitehouse.gov/sites/default/files/omb/assets/fea_docs/FEA_Practice_Guidance_Nov_2007.pdf

FICAM: Identity, Credential and Access Management Sub-Committee, Federal CIO Council
Document: Federal Identity, Credential and Access Management Roadmap (10NOV2009)
Location: http://www.idmanagement.gov/documents/FICAM_Roadmap_Implementation_Guidance.pdf

FIPS: Federal Information Processing Standards, National Institute of Standards and Technology
Document 1: FIPS PUB 140, Security Requirements for Cryptographic Modules (03DEC2002)
Document 2: FIPS PUB 201-1, Personal Identity Verification (PIV) of Federal Employees and Contractors (MAR2006)
Location: http://csrc.nist.gov/publications/PubsFIPS.html

GFIPM: Department of Justice, Global Federated Identity and Privilege Management Documentation
Document: GFIPM Terminology Matrix
Location: http://it.ojp.gov/default.aspx?page=2316

ISO: International Organization for Standardization / International Electrotechnical Commission

Document: ISO/IEC 27000, Information Technology - Security Techniques - Information Security Management Systems - Overview and Vocabulary (01MAY2009)

Location: http://standards.iso.org/ittf/licence.html

NIST IR: National Institute of Standards and Technology Internal Reports

Document 1: NIST IR 7298, Glossary of Key Information Security Terms (25APR2006)

Document 2: NIST IR 7657, A Report on the Privilege (Access) Management Workshop (MAR2010)

Location: http://csrc.nist.gov/publications/PubsNISTIRs.html

NIST SP: National Institute of Standards and Technology Special Publications

Document 1: NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems (FEB 2010)

Document 2: NIST SP 800-39, Managing Information Security Risk (MAR 2011)

Document 3: NIST SP 800-63, Electronic Authentication Guide (APR 2006)

Document 4: NIST SP 800-116, A Recommendation of PIV Credentials in PACS (NOV2008)

Location: http://csrc.nist.gov/publications/PubsSPs.html

OMB: Office of Management and Budget

Document 1: OMB 04-04, E-Authentication Guidance for Federal Agencies (DEC2003)

Location: http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf

RFC: Request for Comment, Internet Engineering Task Force

Document 1: RFC 2560 X.509 Internet Public Key Infrastructure – OCSP (JUN1999)

Location: http://tools.ietf.org/html/rfc2560

Document 2: RFC 3280 Internet X.509 Public Key Infrastructure – CRL (APR2002)

Location: http://tools.ietf.org/html/rfc3280

Document 1: RFC 4949 Internet Security Glossary, Version 2 (AUG2007)

Location: http://tools.ietf.org/html/rfc4949

Document 2: RFC 5755 An Internet Attribute Certificate Profile for Authorization (JAN2010)

Location: http://tools.ietf.org/html/rfc5755

TFPAP: Trust Framework Provider Adoption Process (SEPT2009)

Location: http://www.idmanagement.gov/documents/TrustFrameworkProviderAdoptionProcess.pdf

U.S.C. Title 44: Title 44, Chapter 36 Management and Promotion of Electronic Government Services

Location: http://uscode.house.gov/download/pls/44C36.txt

XPSA: Cross-Enterprise Security and Privacy Authorization

Document 1: WS Trust Profile v1.4 (FEB2009)

Document 2: WS Trust Profile for Healthcare v1.0 (NOV2010)

Location: http://www.oasis-open.org/specs/

[Page Intentionally Left Blank]

Primary Term	Alternate Terms	Definition	Source
Access		Ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions	CNSSI 4009 RFC 4949
		Opportunity to make use of an information system (IS) resource.	AASC
		*** Note *** Neither definition provided for Access alludes to the application to physical access; refer to the definitions for Access Control and Access Management for greater applicability to PACS.	
Access Control		The process of granting or denying specific requests: 1) for obtaining and using information and related information processing services and 2) to enter specific physical facilities (e.g., Federal buildings, military establishments, border crossing entrances).	CNSSI 4009 FIPS 201
		A function or a system that restricts access to authorized persons only.	NIST SP 800-116
		Protection of system resources against unauthorized access.	RFC 4949
		1. Access control limits the use of a resource. Only those people, programs or devices specifically permitted to use the resource will have access. Access control mechanisms are the process by which the decision is made whether to permit or deny the discovery and access of resources and enforce that decision. 2. Controlling access in accordance with a policy.	DISA
		Means to ensure that access to assets is authorized and restricted based on business and security requirements.	ISO
Access Control List (ACL)		1. A list of permissions associated with an object. The list specifies who or what is allowed to access the object and what operations are allowed to be performed on the object. 2. A mechanism that implements access control for a system resource by enumerating the system entities that are permitted to access the resource and stating, either implicitly or explicitly, the access modes granted to each entity.	CNSSI 4009 RFC 4949
		A mechanism that implements access control for a system resource by enumerating the system entities that are permitted to access the resource and stating, either implicitly or explicitly, the access modes granted to each entity.	AASC
		A list of (identifier, permissions) pairs associated with a resource or an asset. As an expression of security policy, a person may perform an operation on a resource or asset if and only if the person's identifier is present in the access control list (explicitly or implicitly), and the permissions in the (identifier, permissions) pair include the permission to perform the requested operation.	NIST SP 800-116
Access Management		The management and control of the ways in which entities are granted or denied access to the resources of an organization and are authorized to perform a specific action(s) within a given resource.	FICAM
	Privilege Management	The collection of processes involved in enforcing the permission for an entity to perform some action against some resource.	ESM
	Privilege Management	Management of authorization to perform an action on a physical or logical resource.	DoD PvM
		Ensures that proper identity verification exists when individuals access sensitive information in computer systems and physical access to buildings. It also manages the ways in which access to resources is granted to users.	DISA
Accreditation		Formal declaration by a Designated Accrediting Authority (DAA) or Principal Accrediting Authority (PAA) that an information system is approved to operate at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards.	CNSSI 4009
		An administrative action by which a designated authority declares that an information system is approved to operate in a particular security configuration with a prescribed set of safeguards.	RFC 4949
Adjudication		Evaluation of pertinent data in a background investigation, as well as any other available information that is relevant and reliable, to determine whether a covered individual is: suitable for Government employment; eligible for logical and physical access; eligible for access to classified information; eligible to hold a sensitive position; or fit to perform work for or on behalf of the Government as a contractor or employee.	FICAM
Applicant		Individuals that request issuance of a credential or access to an application. An applicant becomes a credential holder after issuance, and a user after being granted access to an application.	FICAM
		An individual applying for a PIV Card/credential. The Applicant may be a current or prospective Federal hire, a Federal employee, or a contractor.	FIPS 201

Primary Term	Alternate Terms	Definition	Source
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).	FIPS 201
	System Architecture	The structure of system components, their relationships, and the principles and guidelines governing their design and evolution over time.	RFC 4949
Assertion		A statement from a verifier to a relying party that contains identity information about a subscriber. Assertions may also contain verified attributes. Assertions may be digitally signed objects or they may be obtained from a trusted source by a secure protocol.	NIST SP 800-63
Assessment and Authorization		*** Note *** The most recent revision of NIST SP 800-37 (Revision 1, February 2010) transformed the traditional Certification & Accreditation model into a 6 step Risk Management Framework (RMF). Two of the 6 steps include Assessment and Authorization, these definitions can be mapped back to certification and accreditation; however, only highlighting these two terms would detract from all of the tasks and nuances specified in the other four steps. The traditional definitions have been provided here for reference, but refer to the term "Risk Management Framework (RMF)" for the most up-to-date process.	NIST SP 800-37
		The process of gathering evidence regarding a PCI's satisfaction of the requirements of FIPS 201-1, followed by the decision to authorize the operation of a PCI once it has been established that the requirements of FIPS 201-1 have been met and the risks regarding security and privacy are acceptable.	NIST SP 800-79
	Certification	Comprehensive evaluation of the technical and non-technical security safeguards of an information system to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements.	CNSSI 4009 RFC 4949
	Certification	Trust Framework Provider certification of an identity provider is the determination that the identity provider's policies and practices are comparable to ICAM trust requirements.	TFPAP
	Certification	An assertion by some party (the certifier) that some condition holds, e.g., that certain attribute values are accurate when originated, or as stored someplace, or when received at a point in system workflows (e.g., when passed to a Policy Decision Point).	AASC
	Accreditation	Formal declaration by a Designated Accrediting Authority (DAA) or Principal Accrediting Authority (PAA) that an information system is approved to operate at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards.	CNSSI 4009
	Accreditation	An administrative action by which a designated authority declares that an information system is approved to operate in a particular security configuration with a prescribed set of safeguards.	RFC 4949
Assurance		Measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy.	CNSSI 4009
		The grounds for confidence that the set of intended security controls in an information system are effective in their application.	NIST SP 800-37
		An attribute of an information system that provides grounds for having confidence that the system operates such that the system's security policy is enforced.	RFC 4949
Assurance Level		A measure of trust or confidence in an authentication mechanism in terms of four levels: Level 1: LITTLE OR NO confidence, Level 2: SOME confidence, Level 3: HIGH confidence, Level 4: VERY HIGH confidence.	OMB M-04-04
		The level of assurance associated with a certificate is an assertion by a Certificate Authority of the degree of confidence that others may reasonably place in the binding of a public key to the identity and privileges asserted in the certificate. Personnel, physical, procedural, and technical security controls contribute to the assurance level of the certificates issued by a certificate management system.	DoDI 8520.2

Primary Term	Alternate Terms	Definition	Source
Attribute		A claim of a named quality or characteristic inherent in or ascribed to someone or something.	ESM DISA
		Information of a particular type concerning an identifiable system entity or object. An "attribute type" is the component of an attribute that indicates the class of information given by the attribute; and an "attribute value" is a particular instance of the class of information indicated by an attribute type.	RFC 4949
		Characteristic ascribed to an identity	DoD IdM
		A distinct characteristic of an object.	AASC
		Professional characteristics of a user that have been verified by an Identity Provider (IdP) which will allow that individual to access particular sets of services provided by an Service Provider (SP).	GFIPM
Attribute Authority		An entity recognized as having the authority to verify the association of attributes to an identity.	FICAM
		A Certificate Authority that issues attribute certificates.	RFC 4949
		A system entity that produces attribute assertions.	AASC
	Authoritative Attribute Source	The official source that originates and maintains the attributes of entities.	AASC
Attribute Based Access Control (ABAC)		Access control based on attributes associated with and about subjects, objects, targets, initiators, resources, or the environment. An access control rule set defines the combination of attributes under which an access may take place.	CNSSI 4009
		A policy model that allows for access control policy applicability; and the associated rules that govern access, to be formulated based on an extensible notion of subject, resource, and other attributes.	ESM DISA
		A policy-based access control solution that uses attributes assigned to subjects, resources or the environment to enable access to resources and controlled information sharing. ABAC could be used for access to either local or enterprise services.	AASC
Attribute Certificate		A structure similar to a Public Key Certificate; the main difference being that the Attribute Certificate contains no public key. An Attribute Certificate may contain attributes that specify group membership, role, security clearance, or other authorization information associated with the Attribute Certificate holder.	RFC 5755
Attribute Management		The act of dynamically creating, maintaining, disseminating, and revoking attributes (e.g., clearances, citizenship, location, biometrics, group memberships, and work roles), which are assigned and bound to subjects.	ESM AASC
Attribute Practice Statement		A document stating the operational guidelines and practices to which an owning organization agrees and adheres to, assuring the quality and level of service for each authoritative attribute source (AAS) and attribute service provided.	AASC
Audit		Independent review and examination of records and activities to assess the adequacy of system controls and ensure compliance with established policies and operational procedures.	CNSSI 4009
	Security Audit	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.	RFC 4949
Audit Trail		A chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security relevant transaction from inception to final result.	CNSSI 4009 FICAM
	Security Audit Trail	A chronological record of system activities that is sufficient to enable the reconstruction and examination of the sequence of environments and activities surrounding or leading to an operation, procedure, or event in a security-relevant transaction from inception to final results.	RFC 4949

Primary Term	Alternate Terms	Definition	Source
Authentication		The process of verifying that a claimed identity is genuine and based on valid credentials.	FICAM
		The process of establishing confidence of authenticity; in this case, in the validity of a person's identity and the PIV Card.	FIPS 201
		Utalizing digital credential to assure the identity of users and validate their access.	U.S.C. Title 44
		The process of establishing confidence in user identities.	NIST SP 800-63
		A process that establishes the origin of information, or determines an entity's identity. In this publication, authentication often means the performance of a PIV authentication mechanism.	NIST SP 800-116
		The process of verifying the identity or other attributes claimed by or assumed of an entity (user, process, or device), or to verify the source and integrity of data.	CNSSI 4009
		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.	CNSSI 1300
	Entity Authentication	The act of confirming the claimed identity of an entity.	ESM
	Electronic Authentication (E-Auth)	The process of establishing confidence in user identities electronically presented to an information system.	NIST SP 800-63
		Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system.	DoD IdM
		Security measure that verifies a claimed identity.	AASC
		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.	DoDD 8500.01E
		Provision of assurance that a claimed characteristic of an entity is correct.	ISO
Authoritative Attribute Exchange Service		Service that performs discovery and mapping of attributes from authoritative source repositories.	FICAM
	Identity Information Distribution (IdM)	Providing an authoritative repository of identity attribute values and exposing those attributes to the enterprise (through an attribute service provider) for use by properly authorized users, managers, or applications allowing business or mission systems to operate with a consistent and validated set of identities.	ESM
	Attribute Service	The AS retrieves user information on person and non-person entities from an attribute store. The AS retrieves user information by sharing, federating, exchanging and accessing various attributes associated with an entity's information from variety of authoritative identity stores such as directories and databases. Using the SAML standard, various profiles exist that allow attributes to be returned securely in the format understood by the requesting component.	DISA
Authority Revocation List (ARL)		A list of cross-certificates previously issued by the subject Certification Authority (CA) that have been subsequently compromised or otherwise invalidated.	FMS (Treasury)
		A list of revoked CA certificates. An Authority Revocation List (ARL) is a Credential Revocation List (CRL) for Certification Authority (CA) cross certificates.	X.509
Authorization		The processes of granting or denying specific requests for obtaining and using information processing services or data and to enter specific physical facilities.	FICAM
		Access privileges granted to a user, program, or process or the act of granting those privileges.	CNSSI 4009
		A process for granting approval to a system entity to access a system resource.	RFC 4949
		The granting or denying of access rights to a user, program, or process.	DoD IdM
		The process of determining, by locating and evaluating applicable authorization policy, whether a subject is permitted to act upon a resource possibly with a set of constraints and obligations.	ESM
		Permission, granted by an entity authorized to do so, to perform functions and access data.	AASC
Availability		The property of being accessable and usable upon demand by an authorized entity.	CNSSI 4009
		Ensuring timely and reliable access to and use of information.	U.S.C. Title 44 NIST IR 7298

Primary Term	Alternate Terms	Definition	Source
Backend Attribute Exchange (BAE)	Backend Attribute Retrieval	Service that acquires additional information not found in the authenticated credential that is required by a relying party to make an access based decision.	FICAM
Biometrics		A measureable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition. Facial images, fingerprints, and iris scan samples are all examples of biometrics.	FICAM NTSC
		A measurable, biological physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an Applicant. Facial images, fingerprints, and iris scan are all examples of biometrics.	FIPS 201 CNSSI 4009
		Measurement of biological (anatomical and physiological) and behavioral characteristics that can be used for automated recognition (e.g., fingerprints, facial, iris).	DoD IdM
	Biometric	An image or template of a physiological attribute (e.g., a fingerprint) that may be used to identify an individual. In this document, biometrics may be used to unlock authentication tokens and prevent repudiation of registration.	NIST SP 800-63
	Biometric	An authenticator produced from measurable qualities of a living person.	NIST SP 800-116
Biometric Validation		Services to support capturing, extracting, comparing and matching a measurable, physical characteristic or personal behavioral trait used to recognize the identity or verify the claimed identity of an entity. Biometrics modalities include face, fingerprint, and iris recognition and can be matched on card, on reader, or on server.	FICAM
Bind / Unbind		Building or removing a relationship between an entity's identity and further attribute information on the entity (e.g., properties, status, or credentials).	FICAM
	IA Metadata Binding	Providing a trusted relationship between the IA metadata and the data asset.	ESM
Cardholder Unique Identifier (CHUID)		A FIPS 201 authentication mechanism that is implemented by transmission of the CHUID data object from the PIV Card to PACS, or the PIV Card data object of the same name.	NIST SP 800-116
Certificate		A data object containing a subject identifier, a public key, and other information, that is digitally signed by a Certification Authority. Certificates convey trust in the relationship of the subject identifier to the public key.	NIST SP 800-116
	Digital Certificate	A certificate document in the form of a digital data object (a data object used by a computer) to which is appended a computed digital signature value that depends on the data object.	RFC 4949
		A digitally signed representation of information that 1) identifies the authority issuing it, 2) identifies the subscriber, 3) identifies its valid operational period (date issued / expiration date). In the IA community certificate usually implies public key certificate and can have the following types: cross certificate – A certificate issued from a CA that signs the public key of another CA not within its trust hierarchy tha establishes a trust relationship between the two CAs. encryption certificate – A certificate containing a public key that can encrypt or decrypt electronic messages, files, documents, or data transmissions, or establish or exchange a session key for these same purposes. Key management sometimes refers to the process of storing protecting and escrowing the private component of the key pair associated with the encryption certificate. identity certificate – A certificate that provides authentication of the identity claimed. Within the NSS PKI, identity certificates may be used only for authentication or may be used for both authentication and digital signatures.	CNSSI 4009
		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.	CNSSI 1300
		A digital representation of information that, at a minimum, identifies the certification authority issuing it, names or identifies its subscriber, contains the subscriber's public key, identifies its operational period, and is digitally signed by the certification authority issuing it.	DoDI 8520.2
Certificate Management		Process whereby certificates are generated, stored, protected, transferred, loaded, used, and destroyed.	CNSSI 4009
		The functions that a CA may perform during the lifecycle of a digital certificate, including the following: Acquire and verify data items to bind into the certificate, Encode and sign the certificate, Store the certificate in a directory or repository, Renew, rekey, and update the certificate, Revoke the certificate and issue a CRL.	RFC 4949

Primary Term	Alternate Terms	Definition	Source
Certificate Policy		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.	CNSSI 4009
		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 4949 X.509
		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.	CNSSI 1300 RFC 3647
		A named set of rules that indicates the applicability of a certificate to a particular community and/or class of information system with common security requirements. A certificate policy may be used by a certificate user to help in deciding whether a certificate and the binding therein, is sufficiently trustworthy for a particular information system.	DoDI 8520.2
Certificate Revocation List (CRL)		A signed artifact composed of all revoked or otherwise suspended certificates issued from a CA that can be used to verify the current status of a PKI certificate.	FICAM
		A list of revoked public key certificates created and digitally signed by a Certification Authority.	NIST SP 800-63 FIPS 201 CNSSI 4009
		These are digitally signed “blacklists” of revoked certificates. CAs periodically issue CRLs, and users can retrieve them on demand via repositories.	CNSSI 1300
		1. A data structure that enumerates digital certificates that have been invalidated by their issuer prior to when they were scheduled to expire. (See: certificate expiration, delta CRL, X.509 certificate revocation list). 2. (O) "A signed list indicating a set of certificates that are no longer considered valid by the certificate issuer. In addition to the generic term CRL, some specific CRL types are defined for CRLs that cover particular scopes." [X509]	RFC 4949
		A time stamped list identifying revoked certificates which is signed by a CA or CRL issuer and made freely available in a public repository. Each revoked certificate is identified in a CRL by its serial number.	DISA
Certification Authority (CA)		An authority trusted by one or more users to issue and manage X.509 public key certificates and CRLs.	FICAM
		A trusted entity that issues and revokes public key certificates.	NIST SP 800-63 FIPS 201
		An entity authorized to create, sign, and issue public key certificates.	CNSSI 1300
		An entity that issues digital certificates (especially X.509 certificates) and vouches for the binding between the data items in a certificate.	RFC 4949
Certification Practice Statement		A Statement of the practices that a certification authority employs in issuing, managing, revoking, and renewing or re-keying [PKI] certificates.	RFC 3647
Confidentiality		The property that information is not disclosed to system entities (users, processes, devices) unless they have been authorized to access the information.	CNSSI 4009
		The property that sensitive information is not disclosed to unauthorized individuals, entities or processes.	FIPS 140
		Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	U.S.C. Title 44 NIST IR 7298

Primary Term	Alternate Terms	Definition	Source
Credential		An object that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by an entity.	FICAM
		A data object that is a portable representation of the association between an identifier and a unit of authentication information, and that can be presented for use in verifying an identity claimed by an entity that attempts to access a system. Example: X.509 public-key certificate.	RFC 4949
		Evidence or testimonials that support a claim of identity or assertion of an attribute and usually are intended to be used more than once.	CNSSI 4009
		Evidence attesting to one's right to credit or authority; in this standard, it is the PIV Card and data elements associated with an individua that authoritatively binds an identity (and, optionally, additional attributes) to that individual.	FIPS 201
		In this publication, a collection of information about a person, attested to by an issuing authority. A credential may be a physical artifact (e.g., a PIV Card) or a data object (e.g., a certificate). One or more data object credentials may be stored on the same physical memory device (e.g., a smart card).	NIST SP 800-116
Credential Issuance		Process by which possession of a credential is passed to an entity. Service characteristics vary by credential type.	FICAM
		The process by which an issuing authority obtains and verifies information about a person, assigns one or more unique identifiers to the person, prepares information to be placed in or on a credential, produces a physical or data object credential, and delivers the finished credential to its subject. In the case of PIV Cards, issuance is performed only by accredited PCIs.	NIST SP 800-116
		Providing a means for an ESM CredM Manager to provide one or more credentials (typically contained in a physical token but may also be made accessible by downloading after receiving a onetime password) to a human user that has established his identity as the authorized party to receive the identity credential.	ESM
Credential Lifecycle Management		Refers to maintenance of a credential and associated support over the lifecycle; common processes include renewal, reissuance, suspension, blocking and unblocking, revocation, etc. Lifecycle support activities vary depending on the credential type, and may include a Self Service component.	FICAM
	Credential Management	Includes the sponsorship, enrollment, issuance and revocation of authentication tokens. An authentication token binds a digital identity to a user in the form of a credential such as a PKI certificate or SAML assertion so that the user can present the token as proof of identity.	DISA
	Credential Management	Provide identity credentials that bind the identifier of the entity, and possibly certain entity attributes, with information about the credential (e.g., validity dates) and the issuer's authority. The credentials may be instantiated in hardware (e.g., DoD Common Access Card) or software (e.g., PKI-based PKCS-12) mechanisms, depending upon the acceptable assurance level for the environment and the mission.	ESM
	Credential Maintenance	Providing lifecycle support for identity credentials to include credential revocation, renewal, suspension, rekey, and recovery.	ESM
Credential Validation		Establishes the validity of the identity credential presented as part of the authentication transaction; PKI certificates are validated using techniques such as revocation status checking and certificate path validation. Validation of other credentials can include PIN check, security object check, Cardholder Unique Identifier (CHUID) validation, mutual SSL/TLS, the validation of digital signatures, or other non-biometric and non-cryptographic mechanisms.	FICAM
		Providing an assured, robust, timely means to verify the validity of an identity credential.	ESM
	Credential Validation Service (CVS)	The CVS validates PKI certificates by checking the revocation status of certificates from the certificate issuer. In order to validate the PKI certificate, the CVS also has to have a trust chain to the issuing certificate authority and the certificates must not be expired. The CVS is typically used as part of user authentication, in verifying digital signatures, and in encrypting/decrypting messages. If the certificate in question is being validated as an authentication token, then the presenter must prove possession of the private key before authentication is complete.	DISA

Primary Term	Alternate Terms	Definition	Source
Cryptographic Key		A parameter used in conjunction with a cryptographic algorithm that determines: the transformation of plaintext data into cipher text data, the transformation of cipher text 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.	FIPS 140
		A value used to control cryptographic operations, such as decryption, encryption, signature generation or signature verification.	NIST SP 800-63
		A parameter used in conjunction with a cryptographic algorithm that determines the specific operation of that algorithm.	FIPS 201
	Key	An input parameter used to vary a transformation function performed by a cryptographic algorithm.	RFC 4949
	Key	A numerical value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification.	CNSSI 4009
Cryptographic Module		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.	FIPS 140
Cryptography		Art or science concerning the principles, means, and methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form.	CNSSI 4009
Decryption		A transformation that restores encrypted data to its original form.	RFC 4949
		The process of making encrypted information readable again.	FICAM
Digital Certificate		See Certificate.	
Digital Identity		The representation of identity in a digital environment.	FICAM
Digital Identity Lifecycle Management		Process of establishing and maintaining the attributes that comprise an individual's digital identity; supports general updates to an identity such as a name change or biometric update.	FICAM
Digital Policy		A policy to be enforced by a system that is encoded in such a way that it can be interpreted and enforced by an enterprise system in an automated way, without human intervention.	ESM
		Hierarchical rule sets that control digital resource management, utilization, and protection.	AASC
	Security Policy	The security policy includes the rules regarding authorizations required to access a protected resource and additional security conditions (location, time of day, cardinality, separation of duty purpose, etc.) that constrain enforcement. Matching the user attributes against the security policy provides the means to determine if access is to be permitted.	XSPA
Digital Policy Management		The act of dynamically creating, disseminating, and maintaining hierarchical rule sets to control digital resource management, utilization, and protection. This includes identifying and adjudicating conflicts that may occur among existing and new rule sets due to the hierarchical and dynamic nature of policy. Digital policy may define rules for authentication (trusted authorities, criteria for determining authenticity), authorization (access rules, authorized providers), Quality of Protection (QoP), Quality of Service (QoS), transport connectivity, bandwidth allocation and priority, audit, and computer network defense. Digital Policy Management must protect digital policies, allowing only authorized subjects to create, modify, and delegate management of rules. It assures proper implementation and enforcement of rules through interactions with policy engines and policy enforcement mechanisms and it provision individual aspects of policy decisions to appropriate IA mechanisms.	ESM AASC
		A holistic set of activities and controls required to administer and govern Digital Policy.	DPM TEM

Primary Term	Alternate Terms	Definition	Source
Digital Signature		A value computed with a cryptographic algorithm and associated with 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 4949
		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.	NIST SP 800-63
		Cryptographic process used to assure data object originator authenticity, data integrity, and time stamping for prevention of replay.	CNSSI 4009
		The result of a cryptographic transformation of data which, when properly implemented, provides the services of: 1. origin authentication 2. data integrity, and 3. signer non-repudiation.	FIPS 140
		A data object produced by a digital signature method, such as Rivest, Shamir, Aldeman (RSA) or the Elliptic Curve Digital Signature Algorithm (ECDSA), that when verified provides strong evidence of the origin and integrity of the signed data object.	NIST SP 800-116
Encryption		Cryptographic transformation of data (called "plain text") into a different form (called "cipher text") that conceals the data's original meaning and prevents the original form from being used.	RFC 4949 FICAM
		The process of changing plaintext into cipher text for the purpose of security or privacy.	CNSSI 4009
Enterprise		An organization with a defined mission/goal and a defined boundary, using information systems to execute that mission, and with responsibility for managing its own risks and performance. An enterprise may consist of all or some of the following business aspects: acquisition, program management, financial management (e.g., budgets), human resources, security, and information systems, information and mission management.	CNSS I 4009 ESM
		For the purposes of the DoD/Intelligence Community AASC, the enterprise consists of the Intelligence Community, DoD and their partners.	AASC
Enterprise Architecture		A management practice for aligning resources to improve business performance and help agencies better execute their core missions. An EA describes the current and future state of the agency, and lays out a plan for transitioning from the current state to the desired future state.	FEA
		The description of an enterprise's entire set of information systems: how they are configured, how they are integrated, how they interface to the external environment at the enterprise's boundary, how they are operated to support the enterprise mission, and how they contribute to the enterprise's overall security posture.	CNSSI 4009
	DoD Enterprise Architecture	A federation of descriptions that provide context and rules for accomplishing the mission of the Department. These descriptions are developed and maintained at the Department, Capability Area, and Component levels and collectively define the people, processes, and technology required in the "current" and "target" environments; and the roadmap for transition to the target environment.	DoDD 8000.1
	Federal Enterprise Architecture	A business-based framework for government-wide improvement developed by the Office of Management and Budget that is intended to facilitate efforts to transform the federal government to one that is citizen-centered, results-oriented, and market-based.	CNSSI 4009
Enterprise Security Management		The systems and resources required to order, create, disseminate, modify, suspend and terminate management controls to provision and operate Information Assurance services, processes and devices across the enterprise.	ESM
Enterprise Services		Common or shared IT services that support core mission areas and business services.	FEA
		A set of one or more computer applications and middleware systems hosted on computer hardware that provides standard information systems capabilities to end users and hosted mission applications and services.	CNSSI 4009
		A common set of information resource capabilities designed to provide awareness of, access to, and delivery of information.	DoDD 8000.1

Primary Term	Alternate Terms	Definition	Source
Entitlement Attributes	Privilege Attributes	Attributes associated with an individual that are used as the basis for determining access decisions to both physical and logical resources.	FICAM
	Authorization Attributes	Attributes used by the PDP when making an access control decision.	AASC
Event		Any observable occurrence in a system and/or network. Events sometimes provide indication that an incident is occurring.	CNSSI 4009
Federal Agency Smart Credential Number (FASC-N)		As required by FIPS 201, the primary identifier on the PIV Card for physical access control. The FASC-N is a fixed length (25 byte) data object, specified in [TIG SCEPACS], and included in several data objects on a PIV Card.	NIST SP 800-116
Federal Bridge Certification Authority (FBCA)		The Federal Bridge Certification Authority consists of a collection of Public Key Infrastructure components (Certificate Authorities, Directories, Certificate Policies and Certificate Practice Statements) that are used to provide peer-to-peer interoperability among Agency Principal Certification Authorities.	NIST IR 7298
Federal Public Key Infrastructure Policy Authority (FPKIPA)		The Federal PKI Policy Authority is a federal government body responsible for setting, implementing, and administering policy decisions regarding interagency PKI interoperability that uses the FBCA.	NIST IR 7298
Federation		A trust relationship between discrete digital identity providers (IDPs) that enables a relying party to accept credentials from an external identity provider in order to make access control decisions; provides path discovery and secure access to the credentials needed for authentication; and federated services typically perform security operations at run-time using valid NPE credentials.	FICAM
		A union of organizations.	AASC
	Federated Environment	An IT or mission environment in which a number of enterprises work cooperatively to accomplish a mission, where each enterprise retains its identity and autonomy and there is not a strict hierarchical command and control structure.	ESM
		A group of entities agreeing to use a common IdM system concept which enables these entities to share selected identity information about users with others in defined trust relationships.	DoD IdM
		A group of agencies acting together in a peer relationship to share sensitive information with each other, subject to applicable access control policies.	GFIPM
Framework		A structured description of a topic of interest, including a detailed statement of the problem(s) to be solved and the goal(s) to be achieved. An annotated outline of all the issues that must be addressed while developing acceptable solutions to the problem(s). A description and analysis of the constraints that must be satisfied by an acceptable solution and detailed specifications of acceptable approaches to solving the problems(s).	FIPS 201
Identification		The process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system.	NIST IR 7298 DoD
		An act or process that presents an identifier to a system so that the system can recognize a system entity (e.g., user, process, or device) and distinguish that entity from all others.	CNSSI 4009
Identifier		A data object - often, a printable, non-blank character string - that definitively represents a specific identity of a system entity, distinguishing that identity from all others.	CNSSI 4009 RFC 4949
		Unique data used to represent a person's identity and associated attributes. A name or a card number are examples of identifiers.	FIPS 201
		In this publication, a data object, assigned by an authority, that unambiguously identifies a person within a defined community. For example, a Driver License number identifies a licensed driver within a State. The authority registers people and guarantees assignment of each identifier to a unique person.	NIST SP 800-116
		A representation mapped to a system entity that uniquely refers to it.	AASC

Primary Term	Alternate Terms	Definition	Source
Identity		The set of attribute values (i.e., characteristics) by which an entity is recognizable and that, within the scope of an identity manager's responsibility, is sufficient to distinguish that entity from any other entity.	CNSSI 4009
		The unique biological person defined by DNA; the physical being	FICAM
		The collective aspect of a set of attribute values (i.e., a set of characteristics) by which a system user or other system entity is recognizable or known.	RFC 4949
		The set of physical and behavioral characteristics by which an individual is uniquely recognizable	FIPS 201
		Set of characteristics by which an entity is recognizable (sufficient to distinguish that entity from any other)	DoD IdM
		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.	NIST SP 800-63
		A representation (e.g., a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.	AASC
Identity Attribute Discovery		Process of mapping pathways and creating indexes or directories that allows identification of authoritative data sources (ADS) of identity data.	FICAM
Identity Management		The combination of technical systems, policies and processes that create, define, govern and synchronize the ownership, utilization and safeguarding of identity information.	DoD IdM FICAM
		Consists of the standards, rules and procedures for the protection of a digital user identity. This includes the trustworthy process for vetting and adjudication associated with assigning a subject, user, or entity attributes to a digital identity.	DISA
		Defines standards, rules, and procedures for the protection of personal identity information. Unambiguously associates identities with entities such as individuals, organizations, COIs, automated processes, and devices – anyone or anything that can perform an action anywhere in the enterprise.	ESM
		The act of registering identities and issuing, maintaining, and revoking globally unambiguous, assured identifiers for human and non-human subjects (e.g. individuals, organizations, work roles, COIs, devices, and automated processes). Identity management is performed in a federated manner. Subjects will exchange and must reliably interpret federated identifiers; therefore, identifiers must be defined and communicated according to open standards. Identity Management is fundamentally integrated with Credential Management, the ESM capability where identity proofing is performed.	AASC
Identity Management System		An automated system comprised of one or more systems or applications that provides the workflow management of identity functions.	FICAM
		Comprised of one or more systems or applications that manages the identity verification, validation and issuance process.	FIPS 201
	Identity Provider	An organizational entity that manages users and user identities is called an identity provider (IdP). An identity provider conveys information about an end user to a service provider and performs basic user management tasks such as vetting, credentialing, and authentication.	GFIPM
Identity Proofing		A process that vets and verifies the information (e.g. identity history, credentials, documents) that is used to establish the identity of a system entity.	FICAM
		A process that vets and verifies the information that is used to establish the identity of a system entity.	RFC 4949
		The process by which a CSP and an RA validate sufficient information to uniquely identify a person.	NIST SP 800-63
		Process by which a credential issuer validates sufficient information to uniquely identify an individual applying for the credential.	DoD IdM
		The process of providing sufficient information (e.g., identity history, credentials, documents) to a PIV Registrar when attempting to establish an identity.	FIPS 201

Primary Term	Alternate Terms	Definition	Source
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.	TFPAP
		A Network entity providing the digital identity claims used by a relying party.	XSPA
	Credential Service Provider (CSP)	A trusted entity that issues or registers subscriber tokens and issues electronic credentials to subscribers. The CSP may encompass Registration Authorities 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
Incident		An assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system; or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.	CNSSI 4009 ESM
		A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices.	NIST SP 800-61
	Security Incident	A security event that involves a security violation.	RFC 4949
Information Assurance		Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.	CNSSI 4009 RFC 4949 DoDD 8500.01E
Information Security		The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.	CNSSI 4009 U.S.C. Title 44
		Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide: (A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity; (B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and (C) availability, which means ensuring timely and reliable access to and use of information.	FISMA
		Measures that implement and assure security services in information systems, including in computer systems and in communication systems.	RFC 4949
		Preservation of confidentiality, integrity and availability of information.	ISO
Information Technology		Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.	FICAM CNSSI 4009 DoDD 8000.1 Clinger-Cohen Act of 1996
Integrity		The property whereby an entity has not been modified in an unauthorized manner.	CNSSI 4009
		The property that sensitive data has not been modified or deleted in an unauthorized and undetected manner.	FIPS 140
		Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.	U.S.C. Title 44 NIST IR 7298
Interoperability		The ability of different operating and software systems, applications, and services to communicate and exchange data in an accurate, effective, and consistent manner.	U.S.C. Title 44
		The capability of two or more networks, systems, devices, applications, or components to exchange and readily use information—securely, effectively, and with little or no inconvenience to the user.	NSTIC (Draft)
		For the purposes of this standard, interoperability allows any government facility or information system, regardless of the PIV Issuer, to verify a cardholder's identity using the credentials on the PIV Card.	FIPS 201 NIST SP 800-116

Primary Term	Alternate Terms	Definition	Source
Joint Personnel Adjudication System (JPAS)		The Department of Defense personnel security system, which provides information regarding clearance, access, and investigative status to authorized DoD security personnel and other interfacing organizations.	FICAM
		A master repository and centralized processing tool that provides the capability to perform comprehensive personnel security management of all DoD employees, military personnel, civilians and DoD Contractors.	DoD
Key		See Cryptographic Key.	
Key Management		The activities involving the handling of cryptographic keys and other related security parameters (e.g., IDs and passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and zeroization.	FIPS 140 CNSSI 4009 FICAM
		The process of handling keying material during its life cycle in a cryptographic system; and the supervision and control of that process.	RFC 4949
	Cryptographic Key Management	Generates and maintains the key products required to support a wide range of operational missions involving both DoD and DoD partner cryptographic systems.	ESM
Linking / Association		Process of linking one identity record with another across multiple systems; activation and deactivation of user objects and attributes as they exist in one or more systems, directories, or applications in response to an automated or interactive process; used in conjunction with Authoritative Attribute Exchange.	FICAM
Logical Access		Access to an organizational information system by a user (or process acting on behalf of a user) communicating through a direct connection .	CNSSI 4009
Logical Access Control System (LACS)		An automated system that controls an individual's ability to access one or more computer system resources such as a workstation, network, application, or database. A logical access control system requires validation of an individual's identity through some mechanism such as a PIN, card, biometric, or other token. It has the capability to assign different access privileges to different persons depending on their roles and responsibilities in an organization.	FICAM
Message Authentication Code (MAC)		A cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of the data.	NIST SP 800-63 FIPS 201
		A specific ANSI standard for a checksum that is computed with a keyed hash that is based on DES.	RFC 4949
	Checksum	Value computed on data to detect error or manipulation.	CNSSI 4009
Metadata		Descriptive information about a data object; i.e., data about data, or data labels that describe other data.	RFC 4949
		Structured information that describes, explains, locates or otherwise makes it easier to retrieve, use, or manage an information resource.	FICAM
	IA metadata	Are specific data tags that clearly define how data or resources are to be accessed, stored, or transmitted.	DISA
Metadata Management	Resource Attribute / Metadata Management	Process for establishing and maintaining data (such as rules for access, credential requirements, etc.) for a resource/asset being provisioned to define the access, protection, and handling controls. Specific data tags are used that explicitly state how data or a service is accessed, stored, transmitted or even if it can be made discoverable.	FICAM
	Resource and Metadata Management	Resource management includes the compliance with and maintenance of memoranda of agreements, system interface agreements, quality of service, service level agreements, performance, configuration, and security posture. These resources include but are not limited to web services, applications, databases, document libraries and portals. Related to resource management is metadata management, which is the association, registration, collection, storage and dissemination of structural metadata for information resources and services. Metadata management focuses on IA metadata and resource context metadata. IA metadata provides the security properties, classification, and releasability of the resource, and resource context metadata provides characteristics of the resource, for instance, COI membership, owner, identifier, version, status, and keywords.	DISA
Multi-Factor Authentication		Authentication based on more than one factor. In some contexts, each factor is a different authenticator. In other contexts, each factor is one of "something you know, something you have, something you are" (i.e., memorized fact, token, or biometric) and thus the number of factors is 1, 2, or 3.	NIST SP 800-116

Primary Term	Alternate Terms	Definition	Source
Network		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.	CNSSI 4009
		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 (e.g., impersonation, man-in-the-middle, session hijacking…) and passive (e.g., eavesdropping) attack at any point between the parties (claimant, verifier, CSP or relying party).	NIST SP 800-63
		An information system comprised of a collection of interconnected nodes.	RFC 4949
Non-Person Entity (NPE)		Any type of non-human device (e.g., routers, servers, switches, firewalls, sensors) or software object.	FICAM DoD IdM
		An authorized system, device, program, or other subject in the system that is not a user.	ESM
Non-Repudiation		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.	CNSSI 4009 NIST SP 800-53
		Is the security service by which the entities involved in a communication cannot deny having participated. Specifically the sending entity cannot deny having sent a message (non-repudiation with proof of origin) and the receiving entity cannot deny having received a message (non-repudiation with proof of delivery).	NIST IR 7298
Online Certificate Status Protocol (OCSP)		Enables applications to determine the (revocation) state of an identified certificate. OCSP may be used to satisfy some of the operationa requirements of providing more timely revocation information than is possible with CRLs and may also be used to obtain additional status information. An OCSP client issues a status request to an OCSP responder and suspends acceptance of the certificate in question until the responder provides a response.	RFC 2560
Path Discovery and Validation (PDVAL)		The process of discovering a chain of cross-certificates and CA certificates running from the relying party's trust anchor to the end-entity's certificate; the process of examining each certificate that comprises the trust path and consulting the issuing CA's CRL/OCSP/SCVP responder to determine each certificate's validity status at that moment.	RFC 3280
		Trust Path Discovery: is the process of discovering a chain of cross-certificates and certification authority certificates running from the registered party's trust anchor to the end-entity's certificate. A trust path may be discovered dynamically each time as needed or it may be constructed once and stored (or "cached"). Trust Path Validation: is the process for examining each certificate that comprises the trust path and consulting the issuing certification authority's credential revocation list or OCSP responder to determine each certificates validity status at that moment.	Federal PKI PA
Persona	Persona Certificate	An X.509 certificate issued to a system entity that wishes to use a persona to conceal its true identity when using privacy enhanced mail (PEM) or other Internet services that depend on PKI support.	RFC 4949
		A super-identity or 'avatar' of an entity; a persona may be the result of federating several existing identities.	ITUwiki
		A preexisting Digital Identity that a user through an Agent has the ability to select and use to represent themselves in a given Identity Context.	ITUwiki
Personal Identity Verification (PIV)	PIV Card	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).	FIPS 201 CNSSI 4009
	PIV Card	The identity credential mandated by HSPD-12 and defined by FIPS 201 as an end-point PIV Card. A PIV Card is a smart card with contact and contactless communication capability, and eleven defined data objects for interoperability, five mandatory and six optional.	NIST SP 800-116

Primary Term	Alternate Terms	Definition	Source
Physical Access Control System (PACS)		An automated system that manages the passage of people or assets through an opening(s) in a secure perimeter(s) based on a set of authorization rules.	FICAM
		An electronic system that controls the ability of people or vehicles to enter a protected area, by means of authentication and authorization at access control points.	NIST SP 800-116
PIV Implementation Maturity Model (PIMM)		PIMM is a PIV implementation maturity model that can be used to measure the progress of a facility or an agency towards accepting PIV Card.	NIST SP 800-116
Policy		A plan or course of action that is stated for a system or organization and is intended to affect and direct the decisions and deeds of that entity's components or members.	RFC 4949
		A function to be evaluated, plus an action to take if the function is true. The Applicable Policy Function determines the policy to be applied to a given request.	AASC
		Overall intention and direction as formally expressed by management.	ISO
Policy Administration		The process of creating, disseminating, modifying, managing and maintaining hierarchical rule sets to control digital resource management, utilization, and protection in a standard policy exchange format.	FICAM
Policy Based Access Control (PBAC)		A form of access control that uses an authorization policy that is flexible in the types of evaluated parameters (e.g., identity, role, clearance, operational need, risk, heuristics).	CNSSI 4009
		An access control framework that combines information from the enterprise including policies, user attributes, resource metadata, environmental attributes, and the action performed to provide access control capabilities to dynamic operating environments.	DISA
Policy Decision Point (PDP)		A system entity that makes authorization decisions for itself or for other system entities that request such decisions.	AASC NIST IR 7657
	Policy Decision	Serves as an access control authorization authority for evaluating access control policies based on a variety of inputs.	FICAM
	Privilege Management Authorization	Providing the ability to determine if the conditions for access are met by the requesting authenticated entity and providing the decision to the enforcement sub function.	ESM
Policy Enforcement Point (PEP)		A system entity that requests and subsequently enforces authorization decisions.	AASC NIST IR 7657
		Verifies user authentication and enforces access control decisions on interactions between users and resources. For user authentication, the PEP would validate a user's credentials, for instance, by using the CVS to validate a PKI certificate and verifying the user has the private key or by verifying a single sign-on assertion. After a successful authentication, the PEP queries the PDS for an access control decision. The PEP has the ability to grant or deny user access to the resource and enforce workflow obligations or constraints on the interaction.	DISA
	Policy Enforcement	Restricts access to specific systems or content in accordance with policy decisions that are made.	FICAM
	Privilege Management Enforcement	Providing for compliance with access control policy by granting or denying access requests for GIG resources, including any constraints and obligations contained in the authorization decision.	ESM
Private Key		The secret part of an asymmetric key pair that is typically used to digitally sign or decrypt data.	NIST SP 800-63
		A cryptographic key used with a public key cryptographic algorithm, which is uniquely associated with an entity, and not made public; it is used to generate a digital signature; this key is mathematically linked with a corresponding public key.	NIST SP 800-116 FIPS 140
		A mathematical key (kept secret by the holder) used to create digital signatures and, depending upon the algorithm, to decrypt messages or files encrypted (for confidentiality) with the corresponding public key.	CNSSI 1300
		In an asymmetric cryptography scheme, the private or secret key of a key pair which must be kept confidential and is used to decrypt messages encrypted with the public key or to digitally sign messages, which can then be validated with the public key.	CNSSI 4009
Privilege		A right granted to an individual, a program, or a process.	CNSSI 4009
		A synonym for "authorization," and "entitlement."	RFC 4949

Primary Term	Alternate Terms	Definition	Source
Privilege Attributes	Entitlement Attributes	See Entitlement Attributes	FICAM
Privilege Management		Processes for establishing and maintaining the entitlement or privilege attributes that comprise an entity's access profile. This provides rules for the subject of an access transaction. These attributes are features of an individual that can be used as a basis for determining access decisions to both physical and logical resources.	FICAM
		Privilege management is the definition, creation, translation, validation, and distribution of user permissions in the form of digital policy and user attributes used for authorization. As such, privilege management consists of the policy management and attribute management functional areas. Policy management provides the set of standards and processes required to define, generate, structure, and store access control policies that can be use for access control decision and enforcement. Attribute management enables the linking of attributes to a digital identity and the discovery of user attributes for authorization, their permitted values, their sources, and the extent to which attributes are authoritative and reliable.	DISA
Protocol		Set of rules and formats, semantic and syntactic, permitting information systems to exchange information.	CNSSI 4009
Provisioning		Creating user access accounts and assigning privileges or entitlements within the scope of a defined process or interaction; provide user with access rights to applications and other resources that may be available in an environment; may include the creation, modification, deletion, suspension, or restoration of a defined set of privileges.	FICAM
Public Key		The public part of an asymmetric key pair that is typically used to verify signatures or encrypt data.	NIST SP 800-63 FIPS 201
		A cryptographic key used with a public key cryptographic algorithm, uniquely associated with an entity, and which may be made public; it is used to verify a digital signature; this key is mathematically linked with a corresponding private key.	NIST SP 800-116
		A cryptographic key used with a public key cryptographic algorithm that is uniquely associated with an entity and that may be made public.	FIPS 140
		The publicly disc losable component of a pair of cryptographic keys used for asymmetric cryptography.	RFC 4949
		A mathematical key that has public availability and that applications use to verify signatures created with its corresponding private key. Depending on the algorithm, public keys can encrypt messages or files that the corresponding private key can then decrypt.	CNSSI 1300
		A cryptographic key that may be widely published and is used to enable the operation of an asymmetric cryptography scheme. This key is mathematically linked with a corresponding private key. Typically, a public key can be used to encrypt, but not decrypt, or to validate a signature, but not to sign.	CNSSI 4009
Public Key Certificate		A digital document issued and digitally signed by the private key of a Certification 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.	NIST SP 800-63
		A digital certificate that binds a system entity's identifier to a public key value, and possibly to additional, secondary data items; i.e., a digitally signed data structure that attests to the ownership of a public key.	RFC 4949
Public Key Enablement	Public Key Enabling	The incorporation of the use of certificates for security services such as authentication, confidentiality, data integrity, and non-repudiation.	CNSSI 4009
	Public Key Enabling	The incorporation of the use of certificates for security services such as authentication, confidentiality, data integrity, and nonrepudiation. PK-Enabling involves replacing existing or creating new user authentication systems using certificates instead of other technologies, such as userid and password or Internet Protocol filtering; implementing public key technology to digitally sign, in a legally enforceable manner, transactions and documents; or using public key technology, generally in conjunction with standard symmetric encryption technology, to encrypt information at rest and/or in transit.	DoDI 8520.2

Primary Term	Alternate Terms	Definition	Source
Public Key Infrastructure		The framework and services that provide for the generation, production, distribution, control, accounting and destruction of public key certificates. Components include the personnel, policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, recover, and revoke public key certificates.	CNSSI 4009 DoDI 8520.2
		The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system. Framework established to issue, maintain, and revoke public key certificates.	CNSSI 1300
		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.	FIPS 201
		A service of products which provide and manage X.509 certificates for public key cryptography	DISA
		A system of CAs (and, optionally, RAs and other supporting servers and agents) 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 4949
Registration		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.	NIST SP 800-63 CNSSI 4009
	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.	FIPS 201
		An administrative act or process whereby an entity's name and other attributes are established for the first time at a CA, prior to the CA issuing a digital certificate that has the entity's name as the subject.	RFC 4949
	Registration of Human Users	Providing a globally-unique identifier (ID Reference) that serves as the foundation for the enterprise to distinguish each individual from every other operating on the enterprise.	ESM
	Registration of Non-Person Entities	A globally-unique identifier that allows the enterprise to distinguish every application, service, and device operating on the enterprise.	ESM
Registration Authority (RA)		An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of an authorized CA).	FICAM
		An optional PKI entity (separate from the CAs) that does not sign either digital certificates or CRLs but has responsibility for recording or verifying some or all of the information (particularly the identities of subjects) needed by a CA to issue certificates and CRLs and to perform other certificate management functions.	RFC 4949
		An entity authorized by the CAS to collect, verify, and submit information provided by potential Subscribers which is to be entered into public key certificates. The term RA refers to hardware, software, and individuals that collectively perform this function.	CNSSI 1300
		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).	NIST SP 800-63 CNSSI 4009

Primary Term	Alternate Terms	Definition	Source
Relying Party		An entity that requests and/or receives information about the identity of an individual or authentication assertions from another party such as an IDP, CSP, or Trusted Broker. The requestor is referred to as a relying party, since the requestor relies upon information provided from an external source to authenticate an identity. When a relying party requests information about the validity of a user's identity, they receive an assertion based on the source, the time of creation, and attributes associated with the source. The relying party trusts the information provided to them about the user and makes access decisions based upon the IDP's or Trusted Broker's assertions.	FICAM
		Used in a legal context to mean a recipient of a certificate who acts in reliance on that certificate.	RFC 4949
		An entity that relies on the validity of the binding of the Subscriber's name to a public key to verify or establish the identity and status of an individual, role, or system or device; the integrity of a digitally signed message; the identity of the creator of a message; or confidential communications with the Subscriber.	CNSSI 1300
		An entity that relies upon the subscriber's credentials, typically to process a transaction or grant access to information or a system.	NIST SP 800-63 CNSSI 4009
		In this publication, an entity, such as a PACS, that depends upon the trust model of the PIV System to correctly produce the results of authentication, i.e., the identity of the cardholder.	NIST SP 800-116
		A system entity that decides to take action based on information from another system entity.	AASC
		Any entity that uses a digital certificate to identify the creator of digitally signed information, verify the integrity of digitally signed information, or establish confidential communication with the holder of a certificate by relying on the validity of the binding the subscriber's name to the public key contained in the certificate.	DoDI 8520.2
Resource Attribute Management	Metadata Management	See Metadata Management	
Revocation		The process by which an issuing authority renders an issued credential useless. For example, a Certification Authority may revoke certificates it issues. Typically, a certificate is revoked if its corresponding private key is known to be, or suspected to be, compromised, or if the certificate's subject affiliation is changed.	NIST SP 800-116
Risk		An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.	RFC 4949
		A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occur,; and (ii) the likelihood of occurrence.	CNSSI 4009 NIST SP 800-37
		The potential for an unwanted outcome resulting from an incident, event, or occuance as determined by its likelyhood and the associated consequence.	DHS, NIPP
		The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.	NIST IR 7298
		Combination of the probability of an event and its consequence.	ISO
Risk Adaptable Access Control (RadAC)		A form of access control that uses an authorization policy that takes into account operational need, risk, and heuristics.	CNSSI 4009
Risk Assessment		The process of identifying, prioritizing, and estimating risks. This includes determining the extent to which adverse circumstances or events could impact an enterprise. Uses the results of threat and vulnerability assessments to identify risk to organizational operations and evaluates those risks in terms of likelihood of occurrence and impacts if they occur. The product of a risk assessment is a list of estimated, potential impacts and unmitigated vulnerabilities. Risk assessment is part of risk management and is conducted throughout the Risk Management Framework (RMF).	CNSSI 4009 NIST IR 7298
		The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Synonymous with risk analysis.	NIST SP 800-37
		Overall process of risk analysis and risk evaluation.	ISO

Primary Term	Alternate Terms	Definition	Source
Risk Management		The process of identifying, measuring, and controlling (i.e., mitigating) risks in information systems so as to reduce the risks to a level commensurate with the value of the assets protected.	RFC 4949
		The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system.	NIST SP 800-37
		The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation resulting from the operation or use of an information system, and includes: 1) the conduct of a risk assessment; 2) the implementation of a risk mitigation strategy; 3) employment of techniques and procedures for the continuous monitoring of the security state of the information system; and 4) documenting the overall risk management program.	CNSSI 4009 NIST IR 7298
		The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time.	NIST SP 800-39
	Enterprise Risk Management	The methods and processes used by an enterprise to manage risks to its mission and to establish the trust necessary for the enterprise to support shared missions. It involves the identification of mission dependencies on enterprise capabilities, the identification and prioritization of risks due to defined threats, the implementation of countermeasures to provide both a static risk posture and an effective dynamic response to active threats; and it assesses enterprise performance against threats and adjusts countermeasures as necessary.	CNSSI 4009
		Coordinated activities to direct and control an organization with regard to risk.	ISO
Risk Management Framework (RMF)	Security Categorization	The process of determining the security category for information or an information system. Security categorization methodologies are described in CNSS Instruction 1253 for national security systems and in FIPS 199 for other than national security systems.	NIST SP 800-37 (Revision 1)
	Security Control Selection	*** Adapted *** The processes of developing a security plan to include: identification, selection, monitoring, and review of security controls that are put in place for organizational information systems.	
	Security Control Implementation	*** Adapted *** The implementation and associated documentation of the previously developed security plan.	
	Security Control Assessment	The testing and/or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.	
	Authorization (to operate an Information System)	The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.	
	Security Control Monitoring	*** Adapted *** Includes the processes of determining the security impact, assessing the controls, remidiating the controls (as necessary), updating the security plan, reporting to the Authorizing official, and reviewing the security controls periodically.	
Role		A group attribute that ties membership to function. When an entity assumes a role, the entity is given certain rights that belong to that role. When the entity leaves the role, those rights are removed. The rights given are consistent with the functionality that the entity needs to perform the expected tasks.	CNSSI 4009
		A job function or employment position to which people or other system entities may be assigned in a system.	RFC 4949
		A job function within the context of an organization that has associated semantics regarding the authority and responsibility conferred on the user assigned to the role.	AASC

Primary Term	Alternate Terms	Definition	Source
Role Based Access Control (RBAC)		A model for controlling access to resources where permitted actions on resources are identified with roles rather than with individual subject identities.	AASC
		A form of identity-based access control wherein the system entities that are identified and controlled are functional positions in an organization or process.	RFC 4949
		Access control based on user roles (i.e., a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals.	CNSSI 4009
Secret Key		A key used by a symetric key algorithm to encrypt, decrypt, sign, or verify information. In a symetric key infastructure (SKI), the sender and reciever encrypted information must share the same key.	NIST SP 800-116
Security Category		The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals.	FIPS 199
	Mission Assurance Category	A Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) term primarily used to determine the requirements for availability and integrity.	CNSSI 4009
	Mission Assurance Category	Applicable to DoD information systems, the mission assurance category reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the war fighters' combat mission. Mission assurance categories are primarily used to determine the requirements for availability and integrity.	DoDD 8500.01E
Server-Based Certificate Validation Process (SCVP)		Allows a client to delegate certification path construction and certification path validation to a server.	RFC 5055
Service Provider		An organizational entity that manages resources is called a service provider (SP). An SP maintains complete control of its resources and performs basic resource management tasks, including definition and enforcement of resource access requirements and access control policies.	GFIPM
Threat		Any circumstance or event with the potential to adversely affect a system through unauthorized access, destruction, disclosure, or modification of data, or denial of service.	RFC 4949
		Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.	CNSSI 4009 NIST IR 7298
		potential cause of an unwanted incident, which may result in harm to a system or organization	ISO
Trust		A relationship between a certificate user and a CA in which the user acts according to the assumption that the CA creates only valid digital certificates.	RFC 4949
		The willingness to take actions expecting beneficial outcomes, based on assertions by other parties.	NIST SP 800-95
		The characteristic that one entity is willing to rely upon a second entity to execute a set of actions and/or make a set of assertions about a set of subjects and/or scopes.	XSPA

Primary Term	Alternate Terms	Definition	Source
Trust Anchor		An established point of trust (usually based on the authority of some person, office, or organization) from which a certificate user begins the validation of a certification path.	RFC 4949
		A named entity producing digital signatures, and a corresponding certificate that a relying party has decided to trust, i.e., if a digital signature is verified using the public key within the certificate, the signature is trusted to have been made by the entity named in the certificate.	NIST SP 800-116
		An established point of trust (usually based on the authority of some person, office, or organization) from which an entity begins the validation of an authorized process or authorized (signed) package. A "trust anchor" is sometimes defined as just a public key used for different purposes (e.g., validating a Certification Authority, validating a signed software package or key, validating the process (or person) loading the signed software or key).	CNSSI 4009
		A public key and the name of a certification authority that is used to validate the first certificate in a sequence of certificates. The trust anchor public key is used to verify the signature on a certificate issued by a trust anchor certification authority. The security of the validation process depends upon the authenticity and integrity of the trust anchor. Trust anchors are often distributed as self-signed certificates.	NIST IR 7298
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.	TFPAP
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.	TFPAP
Trust Mechanism		A means of establishing and maintaining a state of reliance on an entity to be "correct" from a security viewpoint.	NIST IR 7298
Trusted Agent		Entity authorized to act as a representative of an Agency in confirming subscriber identification during the registration process. Trusted agents do not have automated interfaces with Certification Authorities.	CNSSI 4009 NIST IR 7298
		An individual explicitly aligned with one or more RA Officers who has been delegated the authority to perform a portion of the RA functions. A TA does not have privileged access to CAS components to authorize certificate issuance, certificate revocation, or key recovery.	CNSSI 1300
User		Individual, or (system) process acting on behalf of an individual, authorized to access an information system.	CNSSI 4009
		An individual or a process (subject) acting on behalf of the individual that accesses a cryptographic module in order to obtain cryptographic services.	FIPS 140
		An individual that is utilizing services provided by an agency. Users may be credential holders, applicants, or employees. This definition is specific to the Use Case. General term is applied to an individual who is at one stage an Applicant and who becomes a Cardholder or other status.	FICAM
	System User	A system entity that consumes a product or service provided by the system, or that accesses and employs system resources to produce a product or service of the system.	RFC 4949
		A person authorized to interact with the system.	ESM

Primary Term	Alternate Terms	Definition	Source
Validation		Confirmation (through the provision of strong, sound, objective evidence) that requirements for a specific intended use or application have been fulfilled (e.g., a trustworthy credential has been presented, or data or information has been formatted in accordance with a defined set of rules, or a specific process has demonstrated that an entity under consideration meets, in all respects, its defined attributes or requirements).	CNSSI 4009
		The process of demonstrating that the system under consideration meets in all respects the specification of that system.	FIPS 201
		In this publication, the process of determining that an identity credential was legitimately issued and is still valid, i.e., has not expired or been terminated.	NIST SP 800-116
		In credential management, validation is the act of determining that a credential meets its specified criterion. For example, if the credential is an X.509 certificate, validation would involve ensuring that it is not past its expiration date; that it is properly signed by a recognized CA; that all options and values conform to policies; and that the certificate is syntactically and semantically correct.	ESM
	Identity Validation	Process of determining that a credential has not expired or been revoked, and is processed and formatted properly.	DoD IdM
	Validate	Use "validate" when referring to a process intended to establish the soundness or correctness of a construct (e.g., certificate validation).	RFC 4949
Verification	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.	FIPS 201
		The process of determining if an assertion is true, particularly the process of determining if a data object possesses a digital signature produced by the purported signer.	NIST SP 800-116
		Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled (e.g., an entity's requirements have been correctly defined, or an entity's attributes have been correctly presented; or a procedure or function performs as intended and leads to the expected outcome).	CNSSI 4009
		The process of confirming a claimed identity.	DoD IdM
	Verify	Use "verify" when referring to a process intended to test or prove the truth or accuracy of a fact or value (e.g., authenticate).	RFC 4949
Vetting		Process of examination and evaluation, including background check activities; results in establishing verified credentials and attributes.	FICAM
	Vet	To examine or evaluate thoroughly.	RFC 4949
Vulnerability		Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.	CNSSI 4009
		A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.	RFC 4949
		A physical feature or operational attribute that renders and entity open to exploitation or suseptible to a given hazard.	DHS, NIPP
		Weakness of an asset or control that can be exploited by a threat.	ISO