pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

Identity Protection and Access Management (IPAM) Glossary

ITP Number APP-SEC013A	***Effective Date*** June 22, 2006
Category Recommended Policy	***Supersedes***
Contact RA-ITCentral@pa.gov	***Scheduled Review*** Annual

1. Introduction

The following sections provide a glossary of the IPAM specific terms and acronyms found throughout the IPAM Information Technology Bulletins (ITBs), as well as a hyperlink reference to all the source documents from which the Commonwealth IPAM policies were formulated.

1.1 Organization

This document provides the following information:

- Section 2 provides hyperlinked references to the IPAM policy source documents.

- Section 3 provides definitions for acronyms used throughout the IPAM ITBs.

- Section 4 provides a glossary of terms that have been adopted for the Commonwealth's IPAM initiative, including references to the sources of those terms.

1.2 Reference Items

Commonwealth Resources/Guidance

OIT Enterprise Memorandum: Commonwealth Identity Protection & Access Management Standards Compliance
http://www.oit.state.pa.us/oaoit/cwp/view.asp?A=4&Q=204991

STD-SEC014H - *IPAM Technical Architectural Standards – Federal Standards Related to FIPS 201*

Industry Resources/Guidance

SAML v2: Security Assertion Markup Language
http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

SPML v1: Service Provisioning Markup language
http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=provision

DSML v2: Directory Service Markup language
http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=dsml

SOAP v1.2: Simple Object Access Protocol
http://www.w3.org/TR/soap12-part0

WS-Security 1.0: Web Service Security
http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss

ISO 7816 – Smart Card Standard
http://www.cardwerk.com/smartcards/smartcard_standard_ISO7816.aspx

ISO 14443 – An introduction to the contactless standard for smart cards and its relevance to customers
http://www.otiglobal.com/objects/ISO%2014443%20WP%204.11.pdf

LDAP v3: Lightweight Directory Access Protocol
http://www.ietf.org/rfc/rfc3377.txt et al.

LDAP v3 Attribute Syntax Definitions
http://www.ietf.org/rfc/rfc2252.txt

LDAP Schema Standards
X.500 equivalents – http://www.ietf.org/rfc/rfc2256.txt
inetOrgPerson – http://www.ietf.org/rfc/rfc2798.txt

3. Acronym Definitions

ACL – Access Control List
AD – Microsoft Active Directory
BEA – Bureau of Enterprise Architecture
CA – Certificate Authority
CoP – Community of Practice
CoPA – Commonwealth of Pennsylvania
CoPED – Commonwealth of Pennsylvania Enterprise Directory
CoPED GUID – The Globally Unique ID used for CoPED
CP – Certificate Policy (defines the PKI)
CPS – Certification Practice Statement (defines how the SSP manages the PKI)
CWOPA – Commonwealth of Pennsylvania Active Directory forest
DC – AD Domain Controller
DIT – Directory Information Tree
DN – Distinguished Name

DSML – Directory Services Markup Language

EASC – Enterprise Architecture Standards Committee

HR – Human Resources

IANA – Internet Assigned Numbers Authority

IETF – Internet Engineering Task Force (the Internet standards body)

IPAM – Identity Protection and Access Management

LDAP – Lightweight Directory Access Protocol

OA – PA Governor’s Office of Administration

OASIS – Organization for the Advancement of Structured Information Standards

ODBC – Open DataBase Connectivity (standard database access API)

OID – Object IDentifier

OIT – Office for Information Technology

OU – Organizational Unit (the primary type of container used in the directory)

PennDOT – Pennsylvania Department of Transportation

PIN – Personal ID Number

PIV – Personal Identity Verification Card

PKI – Public Key Infrastructure

RDN – Relative Distinguished Name (name within the container)

RFC – Request For Comments (the standards published by IETF)

SOAP – Simple Object Access Protocol

SQL – Structured Query Language (standard database query)

SSN – Social Security Number

SSP – Shared Service Provider (for federal bridge PKI interoperability)

XML – Extensible Markup Language

4. Glossary

The terms defined below are used throughout the IPAM ITBs and addendums. Some terms have more than one meaning, depending on the source. For that reason, some terms may be listed multiple times.

Term	Definition	Source
Access	Ability to make use of any information system (IS) resource.	NIST PUB 800-32
Access Control	The process of granting or denying specific requests: (1) obtain and use information and related information processing services; typically a network or a location of a network or a location; and (2) enter specific physical facilities (federal buildings, military establishments, border-crossing entrances).	FIPS PUB 201 Personal Identity Verification of Federal Employees and Contractors
Access Control System	See Logical and Physical Access Control.	
Accreditation	The official management decision of the Designated Accreditation Authority to authorize operation of a PIV Card Issuer after determining that the Issuer's reliability has satisfactorily being established through appropriate assessment and certification processes.	NIST PUB 800-79
Accreditation	Formal declaration by a Designated Approving Authority that an information system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. [NS4009]	X.509 Certificate Policy; 2-15-06
Accreditation Package	The evidence provided to the Designated Accreditation Authority to be used in the accreditation decision process.	NIST PUB 800-79
Activation Data	Private data, other than keys, that are required to access cryptographic modules (unlock private keys for signing or decryption events).	NIST PUB 800-32
Agency	An executive department specified in 5 U.S.C., Sec. 101; a military department specified in 5 U.S.C., Sec. 102; an independent establishment as defined in 5 U.S.C., Sec. 104(1); and a wholly owned government corporation fully subject to the provisions of 31 U.S.C., Chapter 91.	NIST PUB 800-79
Agency	Any department, subordinate element of a department, or independent organizational entity that is statutorily or constitutionally recognized as being part of the Commonwealth of Pennsylvania.	Derived from X.509 Certificate Policy; 2-15-06
Agency Certificate	A CA that acts on behalf of an agency and is under the operational control of an agency.	NIST PUB 800-32

Term	Definition	Source
Authority (CA)		
Algorithm	A computational procedure used for performing a set of tasks such as encryption process, digital signature process, or cardholder verification.	Smart Card Handbook A-1
Anti-tamper	Refers to the technology available to prevent unauthorized alteration or modification of cards.	Smart Card Handbook A-1
Anti-tearing	The process or processes that prevent data loss when a smart card is withdrawn from the contacts during a data operation.	Smart Card Handbook A-1
Applet	A JAVA program module stored on the integrated circuit chip (ICC). It contains program code to store, retrieve, or manipulate different sets of data stored in or passed to it. Application programs running on a host computer or other applets stored on the ICC can access the data or call for services through the applet's program code. An applet is designed primarily to store data and is often referred to as a "container."	CMP Version 5
Applicant	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 PUB 201
Applicant	The subscriber is sometimes also called an “applicant” after applying to a CA for a certificate, but before the certificate issuance procedure is completed.	X.509 Certificate Policy; 2-15-06
Application	A hardware/software system implemented to satisfy a particular set of requirements. In this context, an application incorporates a system used to satisfy a subset of requirements related to the verification or identification of an end user’s identity so that the end user’s identifier can be used to facilitate the end user’s interaction with the system.	FIPS PUB 201
Application Program	A program that runs on a host computer and accesses the data and applets stored on the ICC of a smart card through a smart card reader/writer.	CMP Version 5
Application Program Interface (API)	A formal specification of a collection of procedures and functions available to a client application programmer. These specifications describe the available commands, the arguments (or parameters) that are to be provided when calling the command, and the types of return values when the command execution is completed.	Smart Card Handbook A-1

Term	Definition	Source
Approved	FIPS approved or NIST recommended. An algorithm or technique that is either specified or adopted in an FIPS or an NIST recommendation.	FIPS PUB 201
Approved Certificate Authority	A CA that has been authorized to issue certificates referencing the Commonwealth of Pennsylvania's Certificate Policy.	Commonwealth of PA Certificate Policy
Architecture	A highly structured specification of an acceptable approach within a framework for solving a specific problem. The 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 such as costs, local environment, and user acceptability.	FIPS PUB 201
Archive	Long-term, physically separate storage.	NIST PUB 800-32
Assessment Method	A focused activity or action employed by an assessor for evaluating a particular attribute of a PIV Card issuer.	NIST PUB 800-79
Assessment Procedure	A set of activities or actions employed by an assessor to determine the extent to which the reliability and supporting required attributes of a PIV Card Issuer are exhibited.	NIST PUB 800-79
Asymmetric Keys	Two related keys, a public key and a private key, that are used to perform complementary operations, such as encryption and decryption or signature generation and signature verification.	FIPS PUB 201
Attribute Authority (AA)	An entity responsible for issuing and verifying the validity of an attribute certificate.	Smart Card Handbook A-1
Attribute Certificate	A message, similar to a digital certificate, which is intended to convey information about the subject. The attribute certificate is linked to a specific public key certificate. Thus, the attribute certificate conveys a set of attributes along with a public key certificate identifier or entity name.	Smart Card Handbook A-1
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.	NIST PUB 800-32
Audit Data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an	NIST PUB 800-32

Term	Definition	Source
	event.	
Authenticate	To confirm the identity of an entity when that identity is presented.	NIST PUB 800-32
Authentication	The process of establishing confidence of authenticity; in this case, in the validity of a person's identity and the PIV Card.	FIPS PUB 201
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.	X.509 Certificate Policy; 2-15-06
Authorization	Permission/ privilege granted to an identity to access various physical and logical resources.	FIPS PUB 201 pp45
Authorization to Operate	One of the three possible decisions of a Designated Accreditation Authority that is provided to a PIV Card issuer after all certification activities have been performed and the reliability of the issuer has been verified.	NIST PUB 800-79
Automated Response Unit (ARU)	A designated system for answering telephone calls and providing information to callers by recorded messages, or transferring calls to a customer service center (CSC).	Smart Card Handbook A-1
Backup	Copy of files and programs made to facilitate recovery if necessary.	NIST PUB 800-32
Bar Code	The set of vertical bars of irregular widths representing coded information placed on consumer products and other items (such as identification cards) that may require this type of identification.	Smart Card Handbook A-1
Bar Code 39	Code 39 is an alphanumeric bar code. The symbol can be as long as necessary to store the encoded data. It is designed to encode twenty-six uppercase letters, ten digits and seven special characters. It can be extended to code all 128 ASCII characters by using a two-character coding scheme. Each data character encoded in a Code 39 symbol is made up of five bars and four spaces for a total of nine elements. Each bar or space is either "wide" or "narrow" and three out of the nine elements are always wide. This is what gives the code its other name - Code 3 of 9.	http://www.barcode-1.net/pub/russadam/39code.html
Binding	An affirmation by a Certificate Authority/Attribute Authority (or its acting Registration Authority) of the relationship between a named entity and its public key or biometric template.	Smart Card Handbook A-1
Binding	Process of associating two related elements of	X.509

Term	Definition	Source
	information.	Certificate Policy; 2-15-06
Biometric	A measurable, physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity of an applicant. Facial images, fingerprints, and iris scan samples are all examples of biometrics.	FIPS PUB 201
Biometric Information	The stored electronic information pertaining to a biometric. This information can be in terms of raw or compressed pixels or in terms of some characteristic (such as patterns).	FIPS PUB 201
Biometric System	An automated system capable of the following: * Capturing a biometric sample from an end user * Extracting biometric data from that sample * Comparing the extracted biometric data with data contained in one or more references * Deciding how well they match * Indicating whether or not an identification or verification of identity has been achieved.	FIPS PUB 201
Biometric Template	Refers to a stored record of an individual's biometric features. Typically, a "live scan" of an individual's biometric attributes is translated through a specific algorithm into a digital record that can be stored in a database or on an integrated circuit chip card. The formatted digital record used to store the biometric attributes is generally referred to as the biometric template.	Smart Card Handbook A-1
Breeder Document	A document used as an original source of identity to apply for (or breed) other forms of identity credentials.	Smart Card Alliance; Feb. 2006
Bridge Certificate Authority	An entity that links two or more Certification Authorities who do not have a cross-certification agreement in place. The Bridge Certificate Authority allows CAs to validate each other's certificates.	Smart Card Handbook A-2
Capture	The method of taking a biometric sample from an end user. [INCITS/M1-040211]	FIPS PUB 201
Card Accepting Device	A device that is used to communicate with an Integrated Circuit Card (ICC) during a transaction. It may also provide power and timing to the ICC.	Smart Card Handbook A-2
Card Hot List	A list of cards that have been reported as lost, stolen, or damaged.	Smart Card Handbook A-2
Card Initialization	Refers to the process of preparing a card for use by performing the following tasks: searching for initialization files, locating definite values to use in place of variable values, and loading these values.	IDM Handbook Sept. 05

Term	Definition	Source
Card Management System (CMS)	The CMS tracks the status of a PIV card throughout its entire life cycle, including the production-request, personalization and printing, activation and issuance, suspension, revocation, and destruction phases. The CMSs typically store information in the cardholder's file that the cardholder can remember easily but that is difficult for somebody else to guess.	Federal Identity Management Handbook
Card Personalization	Refers to the modification of a card that contains data specific to the cardholder. Methods of personalization may include encoding the magnetic stripe or bar code, loading data on the ICC, or printing photo or signature data on the card.	Smart Card Handbook A-2
Card Printer	Equipment capable of printing information on the physical surface of the card.	Smart Card Handbook A-2
Card Reader	Equipment capable of reading the information contained in the magnetic stripe or chip on a card..	Smart Card Handbook A-2
Cardholder	An individual possessing an issued PIV Card.	FIPS PUB 201
Certificate	A digital representation of information which at least: (1) identifies the certification authority issuing it; (2) names or identifies its subscriber; (3) contains the subscriber's public key; (4) identifies its operational period; and (5) is digitally signed by the certification authority issuing it.	NIST PUB 800-32
Certificate Arbitrator Module (CAM)	A system that interfaces with agency applications that receives a request for the status of a certificate, passes the certificate validation request to the appropriate CA, receives the certificate validation request response returned from the CA, and reports the response to the requesting agency application.	Smart Card Handbook A-2
Certificate Authority (CA)	The Certificate Authority is a component of the PKI. The CA is responsible for issuing and verifying digital certificates. Digital certificates may contain the public key or information pertinent to the public key.	Smart Card Handbook A-2
Certificate Authority	An authority trusted by one or more users to issue and manage X.509 Public Key Certificates and CARLs or CRLs.	X.509 Certificate Policy; 2-15-06
Certificate Authority Facility	The collection of equipment, personnel, procedures, and structures that are used by a Certification Authority to perform certificate issuance and revocation.	X.509 Certificate Policy; 2-15-06
Certificate Management Authority (CMA)	A Certification Authority or a Registration Authority.	NIST PUB 800-32

Term	Definition	Source
Certificate Policy (CP)	A CP is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A CP addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery, and administration of digital certificates. Indirectly, a CP 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.	NIST PUB 800-32
Certificate-Related Information	Information, such as a subscriber's postal address, that is not included in a certificate. May be used by a CA managing certificates.	NIST 800-32
Certificate Repository	A database of certificates and other PKI-relevant information available on-line.	Smart Card Handbook A-2
Certificate Revocation List (CRL)	A list of revoked public key certificates created and digitally signed by a Certification Authority. [RFC 3280]	FIPS PUB 201
Certificate Status Authority	A trusted entity that provides on-line verification to a Relying Party of a subject certificate's trustworthiness, and may also provide additional attribute information for the subject certificate.	NIST PUB 800-32
Certification	The process of verifying the correctness of a statement or claim and issuing a certificate as to its correctness.	FIPS PUB 201
Certification Agent	The individual, group, or organization responsible for conducting certification activities under the guidance and direction of a Designated Accreditation Authority.	NIST PUB 800-79
Certification Authority	A trusted entity that issues and revokes public key certificates.	IDM Handbook Sept. 05
Certification Authority Revocation List (CARL)	A signed, time-stamped list of serial numbers of CA public key certificates, including cross-certificates that have been revoked.	IDM Handbook Sept. 05
Certification Authority Software	Key Management and cryptographic software used to manage certificates issued to subscribers.	NIST PUB 800-32
Certification Practice Statement (CPS)	A document that states the practices that a CA employs in issuing certificates.	Smart Card Handbook A-2

Term	Definition	Source
Certification Practice Statement (CPS)	A statement of the practices that a CA employs in issuing, suspending, revoking, and renewing certificates and providing access to them, in accordance with specific requirements (specified in this CP or requirements specified in a contract for services).	X.509 Certificate Policy; 2-15-06
Chain of Trust	An attribute of a secure ID system that encompasses all of the system's components and processes and assures that the system as a whole is worthy of trust. A chain of trust is to guarantee the authenticity of the people, issuing organizations, devices, equipment, networks, and other components of a secure ID system. The chain of trust is also to ensure that information within the system is verified, authenticated, protected, and used appropriately.	Smart Card Alliance; Feb. 2006
Chip (Card) Operating System (COS)	The operating system within a card's integrated circuit that interprets commands sent by the workstation and performs the functions requested.	Smart Card Handbook A-2
Claimant	A party whose identity is to be verified using an authentication protocol.	FIPS PUB 201
Client (application)	A system entity, usually a computer process acting on behalf of a human user, which makes use of a service provided by a server.	NIST PUB 800-32
Common Criteria	A set of internationally accepted semantic tools and constructs for describing the security needs of customers and the security attributes of products.	NIST PUB 800-32
Comparison	The process of comparing a biometric with a previously stored reference. See also "Identification" and "Identity Verification." [INCITS/M1-040211]	FIPS PUB 201
Component	An element of a large system, such as an identity card, PIV Issuer, PIV Registrar, card reader, or identity verification support, within the PIV system.	FIPS PUB 201
Component Private Key	Private key associated with a function of the certificate-issuing equipment, as opposed to being associated with an operator or administrator.	X.509 Certificate Policy; 2-15-06
Compromise	A violation (or suspected violation) of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information may have occurred.	Smart Card Handbook A-2
Computer Security Objects Registry (CSOR)	CSOR operated by the National Institute of Standards and Technology.	NIST PUB 800-32
Confidentiality	Assurance that information is not disclosed to	NIST PUB 800-

Term	Definition	Source
	unauthorized entities or processes.	32
Configuration Audit	A process performed by either an internal or an independent system engineering group to ensure the process of configuration management can adequately answer questions regarding the management of change.	CMP Version 5
Configuration Item	Any hardware, software, or combination of both that satisfies an end use function and is designated for separate configuration management.	CMP Version 6
Configuration Management	A management process for establishing and maintaining consistency of a product's performance, functional, and physical attributes with its requirements, design, and operational information throughout its life.	CMP Version 6
Conformance Testing	A process established by NIST within its responsibilities of developing, promulgating, and supporting FIPS for testing specific characteristics of components, products, and services, as well as people and organizations for compliance with a FIPS.	FIPS PUB 201
Contact Interface	A chip card that allows interface through a contact. A contact is an electrical connecting surface on an ICC and/or interfacing device that permits a flow of energy current, thereby transmission of data.	Smart Card Handbook A-3
Contactless Interface	An ICC that enables energy to flow between the card and the interfacing device without the use of contact. Instead, induction of high-frequency transmission techniques is used through a radio frequency (RF) interface.	Smart Card Handbook A-3
Contactless Smart Card	A smart card that communicates with a reader through a radio frequency interface.	Smart Card Alliance; Feb. 2006
Container	An applet designed primarily to store data for retrieval by an application program running on a host computer or other applets co-located on the ICC.	CMP Version 6
Controlled Spaces	This relates to bases, buildings, and/or offices currently using some form of access control. This does not include higher-level security facilities dealing with classified information and processes above the unclassified level.	CMP Version 6
Corrective Action Plan	The document that identifies corrective action tasks that need to be performed in order to obtain subsequent accreditation.	NIST PUB 800-79
Credential	Evidence attesting to one's right to credit or authority; in this standard, it is the PIV Card and data elements associated with an individual that authoritatively binds an identity	FIPS PUB 201

Term	Definition	Source
	(and optionally, additional attributes) to that individual.	
Cross-certificate	A certificate used to establish a trust relationship between two CAs.	X.509 Certificate Policy; 2-15-06
Cross-Credentialing/ Certificate	System whereby identification credentials issued by one agency (entity) will be interoperable for logical and physical access systems and are accepted and trusted by another participating agency (entity).	SOW
Cryptographic Co-Processor	An integrated circuit chip processor that performs cryptographic functions.	Smart Card Handbook A-3
Cryptographic Key (Key)	A parameter used in conjunction with a cryptographic algorithm that determines the specific operation of that algorithm.	FIPS PUB 201
Cryptographic Module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module.	NIST PUB 800-32
Cryptography	The mathematical science used to secure the confidentiality and authentication of data by replacing it with a transformed version that can be reconverted to reveal the original data only by someone holding the proper cryptographic algorithm and key.	Smart Card Handbook A-3
Crypto Period	Time span during which each key setting remains in effect.	NIST PUB 800-32
Data Integrity	A condition in which data has not been altered or destroyed in an unauthorized manner.	Smart Card Handbook A-3
Designated Accreditation Authority	A senior agency official that has been given the authorization to accredit the reliability of a PIV Card Issuer.	NIST PUB 800-79
Digital Certificate	A portable block of data, in a standardized format, which at least identifies the certificate authority issuing it, names or identifies its subscriber, contains the subscriber's public key, identifies its operational period, and is digitally signed by the certificate authority issuing it.	Smart Card Handbook A-3
Digital Signature	A unique electronic signature that accompanies documents and messages. The digital signature serves two primary functions: verifies the authenticity of the party sending the message, and verifies that the content of the message has not been altered.	Smart Card Handbook A-3

Term	Definition	Source
Digital Signature	The result of a transformation of a message by means of a cryptographic system using keys such that a relying party can determine (1) whether the transformation was created using the private key that corresponds to the public key in the signer's digital certificate; and (2) whether the message has been altered since the transformation was made.	X.509 Certificate Policy; 2-15-06
Digitized Signature	A written signature that has been read by a computer scanner and converted into digital data.	Smart Card Handbook A-3
Discretionary Access Control	Means of restricting access to objects based on user identity.	X.509 Certificate Policy; 2-15-06
Distinguished Name	A set of data that identifies a real-world entity, such as a person in a computer-based context.	Smart Card Handbook A-3
Dual Use Certificate	A certificate that is intended for use with both digital signature and data encryption services.	NIST PUB 800-32
Duration	A field within a certificate that is composed of two subfields; "date of issue" and "date of next issue."	NIST PUB 800-32
E-Commerce	The use of network technology (especially the Internet) to buy or sell goods and services.	NIST PUB 800-32
Electronic Purse	A mechanism that allows end users to pay electronically for goods and services. The function of the electronic purse is to maintain a pool of value that is decremented as transactions are performed.	Smart Card Handbook A-3
Employee	Any person employed by an agency as previously defined.	IDM Handbook Sept. 05
Encrypted Network	Messages on this network are encrypted (e.g., using Digital Encryption Standard (DES), Advanced Encryption Standard (AES), or other appropriate algorithms) to prevent reading by unauthorized parties.	NIST PUB 800-32
Encryption	Refers to the process of translating data into a cipher, a more secure form of data. Encrypted data is less likely to be intercepted and accessed by unauthorized persons. This mechanism is particularly important in executing sensitive transactions.	Smart Card Handbook A-3
Encryption Certificate	A certificate containing a public key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes.	NIST PUB 800-32
End Entity	Relying Parties and Subscribers	NIST PUB 800-32

Term	Definition	Source
Enrollment	The process of entering the appropriate identity data for an individual into a system and associating the identity with the privileges being granted by the system.	Smart Card Alliance; Feb. 2006
Enrollment Station	A designated workstation that collects data to enroll individuals for the Smart Access Common ID Card.	Smart Card Handbook A-3
ePassport	A travel document that contains an integrated circuit chip that can securely store and communicate the ePassport holder's personal information to authorized reading devices.	Smart Card Alliance; Feb. 2006
Extensions	Extension fields in X.509 Version 3 certificates.	Smart Card Handbook A-3
False Acceptance Rate (FAR)	Refers to the rate at which an unauthorized individual is accepted by the system as a valid user.	Smart Card Handbook A-3
False Rejection Rate (FRR)	Refers to the rate at which an individual authorized to use the system is rejected as an invalid user.	Smart Card Handbook A-3
Federal Agency Smart Credential Number (FASC-N)	An element of the Card Holder Unique Identifier (CHUID) which uniquely identifies each card.	Smart Card Handbook A-3
Federal Bridge Certification Authority (FBCA)	The FBCA supports interoperability among Federal Agency PKI domains in a peer to peer fashion. The FBCA will issue a certificate only to those agency CAs specified by the owning agency (principle CAs). The FBCA, or a CA that interoperates with the FBCA, may also issue certificates to individuals who operate the FBCA. The FBCA certificates issued to agency principle CAs act as a conduit of trust. The FBCA does not add to and is not to subtract from trust relationships existing between the transacting parties. The Federal PKI Policy Authority (FPKIPA) is the governing body over the FBCA that operates under the By-Laws and Operational Procedures/Practices for the FPKIPA (draft).	NIST
Federal Bridge Certification Authority Membrane	Consists of a collection of PKI components including a variety of CA PKI products, databases, CA specific directories, border directory, firewalls, routers, and randomizers.	NIST PUB 800-32
Federal Bridge Certification Authority Operational Authority	The organization selected by the Federal PKI Policy Authority to be responsible for operating the Federal Bridge Certification Authority.	NIST PUB 800-32

Term	Definition	Source
Federal Public Key Infrastructure Policy Authority (FPKI PA)	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 PUB 800-32
Federal Information Processing Standards (FIPS)	A standard for adoption and use by federal departments and agencies that has been developed within the Information Technology Laboratory and published by NIST, a part of the U.S. Department of Commerce. A FIPS covers some topic in information technology to achieve a common level of quality or some level of interoperability.	FIPS PUB 201
FIPS	Federal Information Processing Standard	NIST PUB 800-79
Firewall	Gateway that limits access between networks in accordance with local security policy.	NIST PUB 800-32
First Responder	The First Responder may function in the context of a broader role (law enforcement, fire rescue, or industrial response). With a limited amount of equipment, the First Responder answers emergency calls to provide efficient and immediate care to ill and injured patients. After receiving notification of an emergency, the First Responder safely responds to the address or location given.	
FISMA	Federal Information Security Management Act	NIST PUB 800-79
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 is to be addressed while developing acceptable solutions to the problem(s). A description and analysis of the constraints that are to be satisfied by an acceptable solution and detailed specifications of acceptable approaches to solving the problems(s).	FIPS PUB 201
Graduated Security	A security system that provides several levels (low, moderate, high) of protection based on threats, risks, available technology, support services, time, human concerns, and economics.	FIPS PUB 201
Graphical User Interface (GUI)	A user interface to a computer that is graphics-based, rather than textual or command-based.	Smart Card Handbook A-4
Hacking	The act of gaining illegal or unauthorized access to a computer system or network.	Smart Card Alliance; Feb. 2006

Term	Definition	Source
Hash Function	A function that maps a bit string of arbitrary length to a fixed length bit string. Approved hash functions satisfy the following properties: 1. One-Way. It is computationally infeasible to find any input that maps it to any pre-specified output. 2. Collision Resistant. It is computationally infeasible to find any two distinct inputs that map to the same output.	FIPS PUB 201
Hash-Based Message Authentication Code (HMAC)	A message authentication code that uses a cryptographic key in conjunction with a hash function.	FIPS PUB 201
Hashing	A software process which computes a value (hash word) from a particular data unit in a manner that enables detection of intentional/unauthorized or unintentional/accidental data modification by the recipient of the data.	Smart Card Handbook A-4
High Assurance Guard (HAG)	An enclave boundary protection device that controls access between a local area network that an enterprise system has a requirement to protect, and an external network that is outside the control of the enterprise system with a high degree of assurance.	NIST PUB 800-32
Identification	The process of discovering the true identity (such as origin and initial history) of a person or item from the entire collection of similar persons or items.	FIPS PUB 201
Identification Authentication	The process of determining the identity of a user that is attempting to access a physical location or computer resource. Authentication can occur through a variety of mechanisms including challenge/response, time-based code sequences, biometric comparison, or other techniques.	Smart Card Handbook A-4
Identification and Credentialing Issuing Station and System (ICISS)	A Graphical User Interface (GUI) to the Card Management System already in place that utilizes the functions and capabilities of AIMS to allow easier creation of smart card tokens.	Interface Control Document First Responders DHS 5/11/05
Identifier	Unique data used to represent a person's identity and associated attributes (e.g., name or a card number).	FIPS PUB 201
Identity	The set of physical and behavioral characteristics by which an individual is uniquely recognizable.	FIPS PUB 201
Identity Binding	Binding of the vetted claimed identity to the individual (through biometrics) according to the issuing authority. Represented by an identity	FIPS PUB 201

Term	Definition	Source
	assertion from the issuer that is carried by a PIV credential.	
Identity Data	The data associated with an individual's identity within a specific system and used by that system to verify the individual's identity.	Smart Card Alliance; Feb. 2006
Identity Management System (IDMS)	A system comprised of one or more systems or applications that manages the identity verification, validation, and issuance process.	FIPS PUB 201
Identity Packaging	System where the source documents and application forms used for identity proofing and vetting are electronically stored for audit purposes.	SOW
Identity Proofing	The process of providing sufficient information (such as identity history, credentials, and "breeder" documents [OMB-19]) to a PIV Registrar when attempting to establish an identity.	FIPS PUB 201
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 PUB 201
Identity Theft	The appropriation of an individual’s personal information to commit fraud, to steal his/her assets, or to pretend to be that person.	Smart Card Alliance; Feb. 2006
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 PUB 201
iNetOrgPerson RFC	This is an “informational RFC” only, but is widely supported by all of the major Lightweight Directory Access Protocol (LDAP) vendors.	
Information in Identifiable Form (IIF)	Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. [E-Gov]	FIPS PUB 201
Information System Security Officer (ISSO)	Person responsible to the designated approving authority for ensuring the security of an information system throughout its life cycle; form design through disposal.	NIST PUB 800-32
Inside Threat	An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.	NIST PUB 800-32

Term	Definition	Source
Integrated Circuit Chip Card (ICC)	The PIV Card has a credit card-size form factor, with one or more embedded. The embedded integrated circuit chips (ICC) located on the PIV card (one or more) provide memory capacity and computational capability.	FIPS PUB 201
Integrity	Protection against unauthorized modification or destruction of information. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.	NIST PUB 800-32
Intellectual Property	Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.	NIST PUB 800-32
Interface Management	The management of the performance, functional, and physical characteristics required to exist at a common boundary. In terms of the smart card, this involves the exchange of information between cards, card readers, and other computerized equipment.	CMP Version 6
Intermediate CA	A CA that is subordinate to another CA, and has a CA subordinate to itself.	NIST PUB 800-32
International Standards Organization (ISO)	A worldwide organization dedicated to fostering the development of systems standards. National standards organizations from 100 different countries are members of the ISO, including the United States (American National Standards Institute – ANSI). Member organizations participate in the development of ISO standards.	Smart Card Handbook A-4
Interoperability	For the purposes of this handbook, 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.	IDM Handbook Sept. 05
Initialization (Card)	At card initialization, the manufacturer performs functions such as programming the ICC that resides on the smart card, loading the operating system with the card serial number and security keys, and reserving areas of memory for photos, digital signatures, and biometrics.	
Issuer	The organization that is issuing the PIV Card to an applicant. Typically this is an organization for which the applicant is working.	FIPS PUB 201
JPEG	A standardized image compression function originally established by the Joint Photographic Experts Group.	FIPS PUB 201
Key	A value that particularizes the use of a	Smart Card

Term	Definition	Source
	cryptographic system.	Handbook A-4
Key Escrow	A deposit of the private key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the subscriber, the terms of which require one or more agents to hold the subscriber's private key for the benefit of the subscriber, an employer, or other party, upon provisions set forth in the agreement.	NIST PUB 800-32
Key Exchange	The process of exchanging public keys in order to establish secure.	NIST PUB 800-32
Key Generation Material	Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.	NIST PUB 800-32
Key Management	The process and means by which keys are generated, stored, protected, transferred, loaded, used, revoked, published, and destroyed.	Smart Card Handbook A-4
Key Pair	The key pair consists of a private key and its matching public key.	Smart Card Handbook A-4
Key Pair	Two mathematically related keys having the properties that (1) one key can be used to encrypt a message that can only be decrypted using the other key; and (2) even knowing one key, it is computationally infeasible to discover the other key.	X.509 Certificate Policy; 2-15-06
Legacy System	This term relates to information systems that have been in use for a significant period of time and therefore have some history. In most cases the application software was originally "stovepipe" or single purpose in nature. In many cases, it has been necessary to work out interface agreements between stovepipe applications when certain data is required, either within the application or external to it.	CMP Version 6
Life Cycle Manager	The specific roles and responsibilities for the Life Cycle Managers (LCM) are defined by the other agencies that are responsible for the smart card at their organization.	CMP Version 6
Lightweight Directory Access Protocol (LDAP)	LDAP is an emerging software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the Internet or on a corporate Intranet. LDAP is a “lightweight” (smaller amount of code) version of DAP (Directory Access Protocol), which is part of X.500, a standard for directory services in a network.	Smart Card Handbook A-4
Local Access Panel/Controller	Refers to a device used to monitor and control access to a site by utilizing an intelligent local	Smart Card Handbook A-4

Term	Definition	Source
(LAP/C)	processing capability in combination with downloaded database processing.	
Local Registration Authority (LRA)	A Registration Authority with responsibility for a local community.	NIST PUB 800-32
Logical Access Control	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 (ACS) 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.	Smart Card Handbook A-4
Logical Resource	The logical resource is typically a network or a location on the network (such as computer workstation, folder, file, database record, software program) to which the cardholder wants to gain access.	FIPS PUB 201
Match/Matching	The process of comparing biometric information against a previously stored biometric data and scoring the level of similarity.	FIPS PUB 201
Mean Time Between Failures (MTBF)	The estimated length of time that a system is available and operational between failures.	Smart Card Handbook A-4
Mean Time to Repair (MTTR)	The estimated length of time needed to bring a system back up and make it fully operational following a system failure.	Smart Card Handbook A-5
Memorandum of Agreement (MOA)	An agreement entered into the Commonwealth of Pennsylvania and another government entity describing the terms of use for PKI services and certificates referencing the Commonwealth of Pennsylvania's Certificate Policy.	Commonwealth of Pennsylvania's Certificate Policy
Memorandum of Agreement (MOA)	Agreement between the Federal PKI Policy Authority and an agency allowing interoperability between the agency principle CA and the FBCA.	NIST PUB 800-32
Message Authentication Code (MAC)	A cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of the data.	FIPS PUB 201
Mission Support Information	Information that is important to the support of deployed and contingency forces.	NIST PUB 800-32
Model	A very detailed description or scaled representation of one component of a larger system that can be created, operated, and analyzed to predict actual operational characteristics of the final produced	FIPS PUB 201

Term	Definition	Source
	component.	
Multi-factor Authentication	The use of multiple techniques to authenticate an individual's identity. This usually involves combining two or more of the following: something the individual has (a card or token); something the individual knows (a password or personal identification number); or something the individual is (a fingerprint or other biometric measurement).	Smart Card Alliance; Feb. 2006
Mutual Authentication	Occurs when parties at both ends of a communication activity authenticate each other.	NIST PUB 800-32
Naming Authority	An organizational entity responsible for assigning distinguished names (DN) and for assuring that each DN is meaningful and unique within its domain.	NIST PUB 800-32
National Incident Management System (NIMS)	NIMS establishes standardized incident management processes, protocols, and procedures that all responders -- federal, state, tribal, and local -- will use to coordinate and conduct response actions. With responders using the same standardized procedures, they will all share a common focus, and will be able to place full emphasis on incident management when a homeland security incident occurs -- whether terrorism or natural disaster. In addition, national preparedness and readiness in responding to and recovering from an incident is enhanced since all of the nation's emergency teams and authorities are using a common language and set of procedures.	DHS: http://www.dhs.gov/dhspublic/interapp/press_release/press_release_0363.xml
National Security System	Any information system used or operated by an agency or its contractor: (1) the function, operation, or use of which involves intelligence activities; involves crypto logic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications (such as payroll, finance, logistics, and personnel management applications); or (2) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of	NIST PUB 800-79

Term	Definition	Source
	Congress to be kept classified in the interest of national defense or foreign policy.	
NIST	National Institute of Standards and Technology	NIST PUB 800-79
Non-repudiation	Refers to the determination that data was sent by one party and received by another party, and can be verified by the inclusion of information about the origin or delivery of the data. Non-repudiation protects both the sender and the recipient of data from false claims that the data was either not sent, or not received.	Smart Card Handbook A-5
Object Identifier (OID)	A specialized formatted number that is registered with an internationally recognized standards organization. The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the federal government PKI, OID is used to uniquely identify each of the four policies and cryptographic algorithms supported.	NIST PUB 800-32
Off-Card	Refers to data that is not stored within the PIV Card or to a computation that is not performed by the Integrated Circuit Chip (ICC) of the PIV Card.	FIPS PUB 201
OMB	Office of Management and Budget	NIST PUB 800-79
On-Card	Refers to data that is stored within the PIV Card or to a computation that is performed by the Integrated Circuit Chip (ICC) of the PIV Card.	FIPS PUB 201
One-to-Many	Synonym for “Identification.” [INCITS/M1-040211]	FIPS PUB 201
Online Certificate Status Protocol (OCSP)	An online protocol used to determine the status of a public key certificate. [RFC 2560]	FIPS PUB 201
Open Database Connectivity	Refers to an open or standard application programming interface (API) used to access a database. A database that is ODBC-compliant facilitates the importing, exporting, and converting of files from external databases.	Smart Card Handbook A-5

Term	Definition	Source
Open Systems Environment	A comprehensive set of interfaces, services, and supporting formats, plus user aspects for interoperability or for portability of applications, data, or people, as specified by information technology standards and profiles. An open platform is composed of hardware and software components that adhere to common standards and are non-proprietary such that multiple vendors can supply these components interchangeably. In an open platform, components from multiple vendors using different technological approaches may be assembled and interoperability across products can be ensured. The objective of an open platform is to achieve vendor independence and allow easy transition to emerging technologies.	Smart Card Handbook A-5
Out-of-Band	Communication between parties utilizing a means or method that differs from the current methods of communication (one party uses U.S. Postal Service mail to communicate with another party where current communication is occurring online).	NIST PUB 800-32
Outside Threat	An unauthorized entity from outside the domain perimeter that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.	NIST PUB 800-32
Personal Identification Number (PIN)	A secret that a claimant memorizes and uses to authenticate his or her identity. PINs are generally only decimal digits.	FIPS PUB 201
Personal Identity Verification (PIV) Card	A physical artifact (identity card, “smart” card) issued to an individual that contains stored identity credentials (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 PUB 201
Personnel Security Activities Management System (First Responders)	Data that stores a record for every employee and contractor in headquarters at the Department of Homeland Security (DHS).	Interface Control Document First Responders DHS 5/11/05
Pharming	A cyber attack that directs people to a fraudulent Web site by poisoning the domain name system server.	Smart Card Alliance; Feb. 2006

Term	Definition	Source
Phishing	A cyber attack that directs people to a fraudulent Web site to collect personal information for identity theft.	Smart Card Alliance; Feb. 2006
Physical Access Control	Refers to an automated system that controls an individual's ability to access to a physical location such as a building, parking lot, office, or other designated physical space. A physical access control system (ACS) requires validation of an individual's identity through some mechanism such as a PIN, card, biometric, or other token prior to providing access. It has the capability to assign different access privileges to different persons depending on their roles and responsibilities in an organization.	Smart Card Handbook A-5
Physical Resource	A physical resource is the secured facility (building entrance, room, turnstile, and parking gate) that the cardholder wishes to access.	
Physically Isolated Network	A network that is not connected to entities or systems outside a physically controlled space.	NIST PUB 800-32
PIV Issuer	An authorized identity card creator that procures FIPS-approved blank identity cards, initializes them with appropriate software and data elements for the requested identity verification and access control application, personalizes the cards with the identity credentials of the authorized subjects, and delivers the personalized cards to the authorized subjects along with appropriate instructions for protection and use.	FIPS PUB 201
PIV Registrar	An entity that establishes and vouches for the identity of an applicant to a PIV Issuer. The PIV Registrar authenticates the applicant's identity by checking identity source documents and identity proofing, and ensures a proper background check has been completed, before the credential is issued.	FIPS PUB 201
PIV Sponsor	An individual who can act on behalf of a department or agency to request a PIV Card for an applicant.	FIPS PUB 201
Point of Sale (POS)	Generally refers to a site where purchases are made. For the purposes of this document, POS refers to a site where purchases may be made electronically through an electronic cash register or card acceptance device.	Smart Card Handbook A-5

Term	Definition	Source
Policy Management Authority (PMA)	Body established to oversee the creation and update of Certificate Policies, review Certification Practice Statements, review the results of CA audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate policies. For the FBCA, the PMA is the federal PKI policy authority.	NIST PUB 800-32
Population	The set of users for the application. [INCITS/M1-040211]	FIPS PUB 201
Primary Account Number (PAN)	A unique identifying number used to reference a financial account.	Smart Card Handbook A-5
Principle CA	The principle CA is a CA designated by an agency to interoperate with the FBCA. An agency may designate multiple principal CAs to interoperate with the FBCA.	NIST PUB 800-32
Privacy	Restricting access to subscriber or relying party information in accordance with federal law and agency policy.	NIST PUB 800-32
Private Key	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.	Smart Card Handbook A-5
Private Key	The key of a signature key pair used to create a digital signature. The key of an encryption key pair used to decrypt confidential information. In both cases, this key is to be kept secret.	X.509 Certificate Policy; 2-15-06
Provisioning System	Provisioning systems serve to automate the task of changing users' rights and privileges across multiple enterprise applications. They enable fast creation of new employee accounts and they augment existing security practices by allowing administrators to quickly cut off terminated accounts.	Enterprise Identity And Access Management Technical White Paper
Proximity	Refers to a technology used to provide physical access control. This technology uses a contactless interface with a card reader. An antenna is embedded in the card, which emits a unique radio frequency when in close proximity to the electronic field of the card reader.	Smart Card Handbook A-5
Public Key	A mathematical key that can be made publicly available and which is used to verify signatures created with its corresponding private key. Depending on the algorithm, public keys are also used to encrypt messages or files that can then be decrypted with the corresponding	Smart Card Handbook A-6

Term	Definition	Source
	private key.	
Public Key	The key of a signature key pair used to validate a digital signature. The key of an encryption key pair used to encrypt confidential information. In both cases, this key is made publicly available, normally in the form of a digital certificate.	X.509 Certificate Policy; 2-15-06
Public (Asymmetric) Key Cryptography	A type of cryptography that uses a key pair of mathematically related cryptographic keys. The public key can be made available to anyone who is to use it and can encrypt information or verify a digital signature; the private key is kept secret by its holder and can decrypt information or generate a digital signature.	Smart Card Handbook A-6
Public Key Infrastructure (PKI)	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 PUB 201
Public Key Infrastructure	A set of policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.	X.509 Certificate Policy; 2-15-06
Public Key Infrastructure Sponsor	Fills the role of a subscriber for non-human system components that are named as public key certificate subjects, and is responsible for meeting the obligations of subscribers.	NIST PUB 800-32
Radio Frequency Identification (RFID)	Refers to an access control system that features a tag embedded with both a circuit and an antenna. As the antenna enters the electronic field of the reader, it generates energy for the circuit, and transmits the identification number in the tag to the reader.	Smart Card Handbook A-6
Reader	An electromechanical device attached to a host computer that can read one of the machine-readable media imbedded or applied to a smart card, or other ID card. Media include smart card ICC (contact and contactless), magnetic stripe, and bar codes. Smart card and magnetic stripe readers often can also write to, or encode, the media.	CMP Version 6
Recommendation	A special publication of the Information Technology Library (ITL) stipulating specific characteristics of technology to use or	FIPS PUB 201

Term	Definition	Source
	procedures to follow to achieve a common level of quality or level of interoperability.	
Reference Implementation	An implementation of a FIPS or a recommendation available from NIST/ITL for demonstrating proof of concept, implementation methods, technology utilization, and operational feasibility.	FIPS PUB 201
Registration Authority (RA)	The Registration Authority is a component of the PKI. The RA acts as a gatekeeper by providing verification to the CA before granting a request for a digital certificate.	Smart Card Handbook A-6
Registration Authority	An entity that is responsible for identification and authentication of certificate subjects but does not sign or issue certificates (an RA is delegated certain tasks on behalf of an authorized CA).	X.509 Certificate Policy; 2-15-06
Re-key (a certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate on the new public key.	NIST PUB 800-32
Relying Party	A recipient who acts in reliance on a certificate and digital signature.	Smart Card Handbook A-6
Renew (a certificate)	The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.	IDM Handbook Sept. 05
Renewal	The process of obtaining a new certificate of the same class and type for the same subject once an existing certificate has expired.	Smart Card Handbook A-6
Repository	A database containing information and data relating to certificates as specified in this certificate policy; may also be referred to as a directory.	NIST PUB 800-32
Request for Comment (RFC)	The RFCs form a series of notes, started in 1969, about the Internet. RFC standards define the official specifications of the Internet protocol suite defined by the Internet Engineering Task Force (IETF) and its steering group, the Internet Engineering Steering Group (IESG).	Web search DBPO
Responsible Individual	A trustworthy person designated by a sponsoring organization to authenticate individual applicants seeking certificates on the basis of their affiliation with the sponsor.	NIST PUB 800-32
Revocation	The process of permanently ending the operational period of a certificate from a specified time forward. Generally, revocation is performed when a private key has been compromised.	Smart Card Handbook A-6

Term	Definition	Source
Revoke a Certificate	To prematurely end the operational period of a certificate effective at a specific date and time.	X.509 Certificate Policy; 2-15-06
Risk	The level of potential impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals of a threat or a given likelihood of that threat occurring.	NIST PUB 800-79
Risk Tolerance	The level of risk an entity is willing to assume in order to achieve a potential desired result.	NIST PUB 800-32
Root CA	The CA that issues the first certificate in a certification chain. The root's public key is to be known in advance by a certificate user in order to validate a certificate chain.	Smart Card Handbook A-6
RSA	RSA is an Internet encryption and authentication system that uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman.	
Secret Key	A cryptographic key that is to be protected from unauthorized disclosure to protect data encrypted with the key. The use of the term "secret" in this context does not imply a classification level; rather, the term implies the need to protect the key from disclosure or substitution.	FIPS PUB 201
Secret Key	A "shared secret" used in symmetric cryptography, wherein users are authenticated based on a password, PIN, or other information shared between the user and the remote host or server. A single key is shared between two parties: the sender, to encrypt a transmission, and the recipient, to decrypt the transmission, with the shared key being generated with an algorithm agreed to beforehand by the transacting parties.	X.509 Certificate Policy; 2-15-06
Secret (Symmetric) Key Cryptography	A cryptographic system that uses the same key, known as a "secret key algorithm" to encipher and decipher messages. This is contrasted with asymmetric key cryptography, which uses a secure public/private key pair.	Smart Card Handbook A-6
Secure Access Module (SAM)	A software module contained in a card access device that allows the card and terminal to mutually authenticate each other.	Smart Card Handbook A-6
Secure E-mail	Refers to the encryption of e-mail messages and attachments, so that they are protected at rest, in transit, and even after they have been accessed by recipients.	http://www.authentica.com/files/data_sheets/pb_Secure_Mail.pdf
Secure Identity	The verifiable and exclusive right to use the identity information being presented by an	Smart Card Alliance; Feb.

Term	Definition	Source
	individual to access a set of privileges.	2006
Sensitive Compartmentalize Information Facility (SCIF)	A designated physical location that requires high-level security clearance for entry. An area that is generally used to maintain top secret documents and systems.	Smart Card Handbook A-6
Server	A system entity that provides a service in response to request from clients.	NIST PUB 800-32
Shared Service provider	The Office of Management and Budget has determined that federal agencies are to procure PKI services from a managed service provider. The Federal Identity Credentialing Committee (FICC) is responsible for certifying PKI service providers to operate under Federal Common Policy Framework and for managing the Shared Service Provider (SSP) program for PKI service providers.	Derived
Signature Certificate	A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.	NIST PUB 800-32
Single Sign On (SSO)	In an SSO environment, users only need to authenticate themselves once, after which they can directly access any application on the network for which they have permission. SSO eliminates the stop and go user experiences that result from multiple logins. Users no longer need to keep track of multiple passwords.	http://www.rsasecurity.com/go/google/sso/landing.html
Skimming	The proactive of stealing credit card numbers by capturing the information in a data storage device.	Smart Card Alliance; Feb. 2006
Smart Card	A device that includes an embedded integrated circuit that can be either a secure micro-controller or equivalent intelligence with internal memory or a memory chip alone. The card connects to a reader with direct physical contact or with a remote contactless radio frequency interface. With an embedded micro controller, smart cards have the unique ability to store large amounts of data, carry out their own on-card functions (such as encryption and digital signatures) and interact intelligently with a smart card reader. Smart cards are available in a variety of form factors, including plastic cards, subscriber identification modules used in GSAM mobile phones, and USB-based tokens.	Smart Card Alliance; Feb. 2006
Source Selection Evaluation Board	A group of government employees charged with evaluating responses of offerings to a task	Smart Card Handbook A-6

Term	Definition	Source
(SSEB)	order and determining which vendor is awarded the task order.	
Speaker Identity Verification (SIV)	The key feature of voice recognition software that extracts and compares unique features of a speech sample with a known sample, and accepts or rejects access based on this comparison.	Smart Card Handbook A-7
Standard	A published statement on a topic specifying the characteristics, usually measurable, that are to be satisfied or achieved to comply with the standard.	FIPS PUB 201
Storage	An electronic and/or mechanical-magnetic device that holds information for subsequent use or retrieval.	Smart Card Handbook A-7
Subordinate CA	In a hierarchical PKI, a CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA.	NIST PUB 800-32
Subscriber	A person who is the subject of, who has been issued a certificate, and who is capable of using and is authorized to use the private key that corresponds to the public key listed in the certificate.	Smart Card Handbook A-7
Subscriber	A subscriber is an entity who (1) is the subject named or identified in a certificate issued to that entity; (2) holds a private key that corresponds to the public key listed in the certificate; and (3) who does not issue certificates to another party. This includes, but is not limited to, an individual or network device.	X.509 Certificate Policy; 2-15-06
Superior CA	In a hierarchical PKI, a CA who has certified the certificate signature key of another CA, and who constrains the activities of that CA.	NIST PUB 800-32
System Configuration Management	System configuration management is the capability of identifying and defining the items in the system, controlling the change of these items throughout their life cycle, recording and reporting the status of items and change requests, and verifying the completeness and correctness of items.	CMP Version 6
System Equipment Configuration	A comprehensive accounting of all system hardware and software types and settings.	NIST PUB 800-32
System High	The highest security level supported by an information system. (NS4009)	X.509 Certificate Policy; 2-15-06
Tamper resisting	Refers to the technology available to prevent unauthorized alteration or modification of cards.	IDM Handbook Sept. 05

Term	Definition	Source
Tampering	Refers to any unauthorized alteration or modification of a card.	Smart Card Handbook A-7
Technical non-repudiation	The contribution public key mechanisms to the provision of technical evidence supporting a non-repudiation security service.	NIST PUB 800-32
Threat	Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service.	NIST PUB 800-32
Token	A physical device that carries an individual's credentials. The device is typically small (for easy transport) and usually employs a variety of physical and/or logical mechanisms to protect against modifying legitimate credentials or producing fraudulent credentials. Examples of tokens include picture ID cards (state driver's licenses), smart cards, floppy disks, and memory sticks.	Smart Card Alliance; Feb. 2006
Trust List	Collection of trusted certificates used by Relying Parties to authenticate other certificates.	NIST PUB 800-32
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 CAs.	IDM Handbook Sept. 05
Trusted Certificate	A certificate that is trusted by the relying party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. This is also known as a "trust anchor.”	NIST PUB 800-32
Trusted Timestamp	A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.	NIST PUB 800-32
Trustworthiness	Security decision with respect to extended investigations to determine and confirm qualifications, and suitability to perform specific tasks and responsibilities.	FIPS PUB 201
Trustworthy System	Computer hardware, software and procedures that: (1) are reasonably secure from intrusion and misuse; (2) provide a reasonable level of availability, reliability and correct operation; (3) are reasonably suited to performing their intended functions; and (4) adhere to generally accepted security procedures.	NIST PUB 800-32
Update	The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate.	NIST PUB 800-32

Term	Definition	Source
Validation	The process of demonstrating that the system under consideration meets in all respects the specification of that system. [INCITS/M1-040211]	FIPS PUB 201
Validation Authority	See the Online Certificate Status Protocol (OCSP) approach of "Validation Authority."	
Verification	The process by which the question "is this person who the person claims to be?" is answered. This function requires a one-to-one match between presented identity information and identity information that is known to a system.	Smart Card Alliance; Feb. 2006
Wiegand	Refers to a technology that provides physical access control capability by way of a contact interface that is "swiped" similar to a magnetic stripe card. A Wiegand card is more secure and durable than a magnetic stripe card because it is embedded with a magnetic coating during production.	Smart Card Handbook A-7
Zeroize	A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data.	X.509 Certificate Policy; 2-15-06
zzzzzzzzzzzzz	Bottom place holder	

5. Publication Version Control

It is the user's responsibility to ensure they have the latest version of this publication. Questions regarding this publication are to be directed to RA-itcentral@pa.gov.

This chart contains a history of this publication's revisions:

Version	Date	Purpose of Revision
Original	6/22/2006	Base Policy
Revision	6/22/2009	Added STD-SEC014H IPAM Technical Architecture Standards: Federal Standards Related to FIPS 201 to Section 2,-Reference Items
	4/2/2014	ITP Reformat