

USAccess Program Glossary of Terms

Access control – the process of granting or denying requests to access physical facilities or areas, or to logical systems (e.g., computer networks or software applications). See also “logical access control system” and “physical access control system.”

Applicant – An individual applying for a PIV Credential. The Applicant may be a current or prospective Federal hire, a Federal employee, or a contractor.

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.

Authentication – the process of establishing an individual’s identity and determining whether individual Federal employees or contractors are who they say they are.

Authorization – process of giving individuals access to specific areas or systems based on their rights for access and contingent on successful authentication.

Background Investigation – any one of various Federal investigations conducted by OPM, the FBI, or by Federal departments and agencies with delegated authority to conduct personnel security background investigations.

Biometric – a measurable physical characteristic used to recognize the identity of an individual. Examples include fingerprints and facial images. A biometric system uses biometric data for authentication purposes.

Biometric Information – The stored electronic information pertaining to a biometric. This information can be in terms of raw or compressed pixels or in terms of some characteristic (e.g., patterns).

Card – see "PIV Credential"

Credential – Evidence attesting to one’s right to credit or authority. In the USAccess system, it is the PIV Credential and data elements associated with an individual that authoritatively binds an identity (and, optionally, additional attributes) to that individual.

Contractor – see “Employee”.

Credential Holder – An individual possessing an issued PIV Credential.

Cryptographic Key (Key) – A parameter used in conjunction with a cryptographic algorithm that determines the specific operation of that algorithm.

Employee – as defined in Executive Order (EO) 12968, “Employee” means a person, other than the President and Vice President, employed by, detailed or assigned to, an agency, including members of the Armed Forces; an expert or consultant to an agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of an agency, including all subcontractors; a personal services contractor; or any other category of person who acts on behalf of an agency as determined by the agency head. See also “Employee” as defined in title 5 U.S.C §2105.

FBI FP Check – National Criminal History Fingerprint check of the FBI fingerprint files. This check is an integral part of the NACI.

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.

USAccess Program Definitions

Identity – The set of physical and behavioral characteristics by which an individual is uniquely recognizable.

Identity Binding – Binding of the vetted claimed identity to the individual (through biometrics) according to the issuing authority. Represented by an identity assertion from the issuer that is carried by a PIV credential.

Identity Management System (IDMS) – one or more systems or applications that manage the identity verification, validation, and card issuance process. The IDMS software is used by PIV Registrars to enroll Applicants.

Identity-proofing – the process of providing identity source documents (e.g., driver's license, passport, birth certificate, etc.) to a registration authority, or the process of verifying an individual's information that he or she is that individual and no other. FIPS 201-1 requires that one of these documents be an original State or Federal Government-issued photo ID, and the other be from the approved set of identity documents listed on Form I-9.

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.

Logical Access Control System (LACS) – protection mechanisms that limit users' access to information technology (IT) systems by restricting their form of access to those systems necessary to perform their job function. These LACS may be built into an operating system, application, or an added system.

National Agency Check (NAC) – The NAC is part of every NACI. Standard NACs are Security/Suitability Investigations Index, Defense Clearance and Investigation Index, FBI Name Check, and FBI National Criminal History Check.

National Agency Check with Inquiries (NACI) – the basic and minimum investigation required of all Federal employees and contractors consisting of searches of the OPM Security/ Suitability Investigations Index (SII), the Defense Clearance and Investigations Index (DCII), the Federal Bureau of Investigation (FBI) Identification Division's name and fingerprint files, and other files or indices when necessary. A NACI also includes written inquiries and searches of records covering specific areas of an individual's background during the past five years (inquiries sent to current and past employers, schools attended, references, and local law enforcement authorities).

Physical Access Control System (PACS) – protection mechanisms that limit users' access to physical facilities or areas within a facility necessary to perform their job function. These systems typically involve a combination of hardware and software (e.g., a card reader), and may involve human control (e.g., a security guard).

PIV Credential – a government-issued physical artifact, also referred to as a smart card or 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). The Credential Holder's facial image will be printed on the card along with other identifying information.

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

USAccess Program Definitions

identity proofing, and ensures a proper background check has been completed, before the credential is issued.

PIV Sponsor – An individual who can act on behalf of a department or agency to request a PIV Card for an Applicant.

Public Key – The public part of an asymmetric key pair that is typically used to verify signatures or encrypt data.

Public Key Infrastructure (PKI) – A service that provides cryptographic keys needed to perform digital signature-based identity verification, and to protect communications and storage of sensitive data.

Secret Key – A cryptographic key that must 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.

SF-87 – Fingerprint Chart for Federal employee(s) or applicant for Federal employment.

Submitting Office Identifier (SOI) – Number assigned by OPM to identify office that submitted the NACI request