



# NASA Procedural Requirements

COMPLIANCE IS MANDATORY

**NPR 2841.1**

Effective Date: January 06,  
2011

Expiration Date: June 06,  
2016

[Printable Format \(PDF\)](#)

Request Notification of Change (NASA Only)

## Subject: Identity, Credential, and Access Management

Responsible Office: Office of the Chief Information Officer

[| TOC](#) | [Preface](#) | [Chapter1](#) | [Chapter2](#) | [Chapter3](#) | [AppendixA](#) | [AppendixB](#) | [AppendixC](#) | [ALL](#) |

## Appendix A. Definitions

- A.1 **Access.** The ability to (1) obtain and use information and related information processing services; and/or (2) enter specific physical facilities (e.g., Federal buildings, military establishments, border crossing entrances).
- A.2 **Access Control.** The process of granting or denying specific access requests.
- A.3 **Access Sponsor.** A NASA person who can vouch for another individual's need for access to an asset.
- A.4 **Application.** (1) A set of computer commands, instructions, and procedures used to cause a computer to process a specific set of information. Application software does not include operating systems, generic utilities, or similar software that are normally referred to as "system software." (2) 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 that individual's interaction with the system.
- A.5 **Asserted Identity.** The set of attributes that an individual claims uniquely identifies him or her.
- A.6 **Asset.** A system, object, person, or any combination thereof, that has importance or value: includes facilities, property, information records, data, information technology systems, and applications.
- A.7 **Asset Group.** A collection of assets that are managed together for purposes of identifying Level of Risk (LoR), granting access permissions, and/or authorizing access.
- A.8 **Authentication.** (1) The validation and confirmation of a person's claim of identity. (2) The validation and identification of a computer network node, transmission, or message. (3) The process of establishing confidence of authenticity. (4) Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to facilities and information systems.

- A.9 **Authoritative.** A source of data or information that has been sanctioned by established authority as the best source of information that can be found within a given domain.
- A.10 **Authorization.** The privilege granted to a subject (e.g., individual, program, or process) by a designated official to do something, such as access information based on the individual's need to know.
- A.11 **Basic Level of Entitlement (BLE).** Access right(s) granted to a person based on attributes, including but not limited to affiliation, geographical location, and community membership.
- A.12 **Certificate.** See digital certificate.
- A.13 **Certificate Validation.** Transactions used to verify that a digital certificate is still valid, e.g., not revoked or expired.
- A.14 **Credential.** A physical/tangible or electronic object through which data elements associated with an individual are bound to the individual's identity. Credentials are presented to access control systems in order to gain access to assets.
- A.15 **Credential Service Provider (CSP).** An element of an authentication system which issues and performs life-cycle management of identity information and associated credentials.
- A.16 **Community Manager.** The individual responsible for the creation and management of a group of NASA people, generally for the provision of access to one or more assets. Members of communities have something in common that is encapsulated in an attribute of the person, including but not limited to affiliation, discipline, or organization.
- A.17 **Digital Certificate.** A credential in the form of encoded data which serves as a guarantee that parties to a transaction are who they claim to be.
- A.18 **Encryption.** Any procedure used in cryptography to convert plain text into cipher text in order to prevent anyone other than the intended recipient from reading that data.
- A.19 **End User.** A person who relies on computer systems to conduct duties or business activities.
- A.20 **Enterprise Architecture.** The organizing logic for business processes and Information Technology (IT) infrastructure reflecting the integration and standardization requirements of the firm's operating model.
- A.21 **Federated Identity.** The set of attributes of an individual that are provided to NASA and maintained by a trusted external organization to uniquely identify the individual for the purpose of gaining logical and physical access to protected resources.
- A.22 **Identity, Credential, and Access Management (ICAM) Service Managers.** ICAM Service Managers are funded and tasked to provide one or more ICAM Services to the NASA Enterprise.
- A.23 **Identity.** The set of attributes that uniquely identify an individual for the purpose of gaining logical and physical access to protected resources and identification in electronic transactions.

- A.24 **Identity Proofing.** The process for providing sufficient information (e.g., identity history, credentials, documents) to a Registration Authority (RA) when attempting to establish an identity or issue a credential.
- A.25 **Identity Provider (IdP).** An issuing authority that binds vetted claimed identities to credentials for the purpose of assertion in electronic transaction requiring authentication.
- A.26 **Identity Sponsor.** A NASA civil servant who vouches for an individual's need for identity life-cycle management services in order to be authorized to access NASA physical or IT assets.
- A.27 **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 credential or system and associated with the identity being claimed.
- A.28 **Information Owner (IO).** A NASA official with the responsibility to categorize and classify data, and to establish security controls for the generation, collection, processing, dissemination, and disposal of information under their authority. IOs and Information System Owners (ISOs) are often the same person. See NPR 2810.1 for more details about IO roles and responsibilities.
- A.29 **Information System Owner (ISO).** The NASA official who is responsible for the successful operation and protection of the system and its information. Program, project, and functional managers are often identified as information system owners. IOs and ISOs are often the same person. See NPR 2810.1 for more details about ISO roles and responsibilities.
- A.30 **Information Technology.** (1) Hardware and software operated by a Federal agency or by a contractor of a Federal agency or other organization that processes information on behalf of the Federal Government to accomplish a Federal function, regardless of the technology involved, whether by computers, telecommunications systems, automatic data processing equipment, or other. (2) 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 by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: i) requires the use of such equipment; or ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.
- A.31 **Infrastructure.** A collection of assets. See definitions for asset and system.
- A.32 **Interoperability.** For the purposes of this standard, interoperability allows any Government facility or information system, regardless of the credential issuer, to verify a cardholder's identity.
- A.33 **Information Technology (IT) Asset.** A system, application, or information that is managed under a NASA IT System Security Plan.

- A.34 **Legacy.** A service, system, or application that was operational prior to the initial publication of this NPR.
- A.35 **Level of Assurance (LoA).** The amount of certainty that individuals accessing a physical or logical asset are who they claim to be. NIST SP 800-63 provides guidance for determining LoA.
- A.36 **Level of Confidence (LoC).** The amount of certainty, based on identity proofing and investigation, that an individual can be trusted with access to NASA physical and IT assets.
- A.37 **Level of Risk (LoR).** The amount of vulnerability to NASA, based on the likelihood and consequences of an adverse action through improper access or use of a physical or IT asset.
- A.38 **Logical Access.** Access to information records, data, information technology systems, and applications.
- A.39 **NASA-Accepted Identity.** An identity of a person that is affiliated with NASA or a NASA-accepted Identity Provider (IdP) that meets Federal requirements for the asserted LoC. NIST SP 800-63 provides guidance for LoC, which ranges from little or no confidence to very high confidence.
- A.40 **NASA-Accepted Credential.** A credential that has been issued by NASA or by a NASA-accepted Credential Service Provider (CSP), and meets Federal requirements for the asserted LoA.
- A.41 **Non-Person Entity (NPE).** A computer, device, system or application. In this document, an NPE may be issued credentials and or certificates in order to allow for secure transfer of data to another NPE.
- A.42 **Person.** A NASA worker or partner with whom NASA collaborates and conducts business.
- A.43 **Personal Identity Verification (PIV) Smartcard.** A physical artifact that meets the requirements of Federal Information Processing Standard (FIPS) 201-1 and supporting documents, issued to an individual 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).
- A.44 **Physical Access.** Access to NASA facilities and property.
- A.45 **PIV Sponsor.** A NASA Civil Servant who can approve the request for a NASA PIV smartcard for a person.
- A.46 **Public Key Infrastructure (PKI).** A service that provides the cryptographic keys needed to perform identity verification, encryption, and electronic signature.
- A.47 **Registration Authority.** Registration Authorities ensure that credentials are issued to, and shared secrets are created by, the person to whom the credential is assigned.
- A.48 **Remote [End] User.** Non-NASA personnel gaining logical access to NASA information system and application resources.
- A.49 **Revocation.** The removal of an individual's eligibility to access physical or logical assets based upon an adjudication that continued access poses a risk to the Agency.

- A.50 **Signing Certificate.** Digital certificate issued by a certificate authority to ensure integrity and authenticity in electronic transactions between individuals.
- A.51 **Smartcard.** Credential issued with an individual's unique vetted identity information encoded and physically printed on the exterior.
- A.52 **Special Purpose.** Special Purpose refers to IT assets that are unique in design or implementation in order to meet NASA's mission.
- A.53 **Suspension.** The temporary cessation of affiliation, community membership, use of credentials, or access. In this document, suspensions result in a temporary loss of access to physical or logical assets.
- A.54 **System.** In this document, this term is used to mean an interconnected set of information resources under the same management control which shares common functionality and requires the same level of security controls. Normally includes hardware, software, information, data, applications, telecommunication systems, network communications systems, and people.
- A.55 **System Owner.** See IT System Owner.
- A.56 **User.** Individual or (system) process authorized to access an IT asset.
- A.57 **User Authentication.** A process by which a system receives validation of a user's identity.
- A.58 **User Identification (User ID).** A unique character string used in a computer to identify a user which is not normally protected as private/privileged information but is unique within the system.
- A.59 **Vetted.** See Vetting.
- A.60 **Vetting.** A review of information about a person for possible approval or acceptance. In this document, a vetted person has been reviewed to determine eligibility for access to NASA physical and/or logical assets.

| [TOC](#) | [Preface](#) | [Chapter1](#) | [Chapter2](#) | [Chapter3](#) | [AppendixA](#) | [AppendixB](#) |  
[AppendixC](#) | [ALL](#) |

| [NODIS Library](#) | [Legal Policies\(2000s\)](#) | [Search](#) |

**DISTRIBUTION:**  
**NODIS**

---

**This Document Is Uncontrolled When Printed.**  
Check the NASA Online Directives Information System (NODIS) Library  
to Verify that this is the correct version before use: <http://nodis3.gsfc.nasa.gov>

---