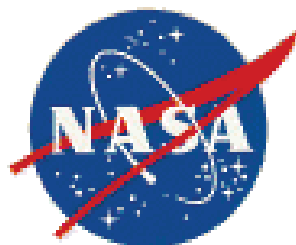




INFORMATION TECHNOLOGY SECURITY HANDBOOK

IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT (ICAM) SERVICES

EFFECTIVE DATE: JUNE 11, 2020



COMPLIANCE WITH THE POLICIES, PROCEDURES, AND PROCESSES IN THIS
HANDBOOK IS MANDATORY

Table of Contents

Table of Contents	2
Table of Figures	5
Change History	6
1 Introduction	7
1.1 Purpose	8
1.2 Scope	8
1.3 Point(s) of Contact for this Handbook	8
1.4 Applicable Documents	8
2 ICAM Key Concepts	9
2.1 NIST SP 800-63-3 Changes to Level of Assurance	10
2.1.1 Identity Assurance Level (IAL):	11
2.1.2 Authentication Assurance Levels (AAL)	12
2.1.3 Federation Assurance Level (FAL)	12
2.2 Confidence, Risk, Trust, and Assurance	12
2.3 Federated Access	14
2.4 Provisioning, Authentication, and Authorization	14
3 Systems that Support ICAM Services	15
3.1 Identity Management & Account eXchange (IdMAX)	16
3.2 Enterprise Physical Access Control System (EPACS)	16
3.3 Agency Application Rationalization Tool (AART)	16
3.4 NASA Access Management System (NAMS)	17
3.5 NASA Enterprise Directory (NED)	17
3.6 NASA Consolidated Active Directory (NCAD)	17
3.7 Access Launchpad	18
3.8 Two-Factor Token Infrastructure (TFTI)	18
3.9 NASA Operational Certificate Authority (NOCA)	18
3.10 NASA Internal Certificate Authority (NICA)	18
3.11 ICAM Tools	19
3.11.1 Identity Self Service (ID)	19
3.11.2 ICAM Support Console	19
3.12 NASA Privileged Access Management System (NPrivAMS)	19
4 Identity Management	19

4.1	Types of Identities	20
4.1.1	NASA Identities	20
4.1.2	NASA Guest Identities	20
4.1.3	NASA-Trusted Identities	20
4.1.4	Federated Identities	21
4.2	Identity Lifecycle	21
4.2.1	Creation	21
4.2.1.1	Identity Associated with a Registered Credential	22
4.2.2	Maintenance	22
4.2.3	Termination	22
5	Credential Management	22
5.1	Level of Assurance (LOA)/Authentication Assurance Level (AAL)	22
5.2	Credential Types	23
5.2.1	NASA PIV Smartcard	23
5.2.2	Agency Smart Badge	23
5.2.3	NASA Visitor Badges	23
5.2.4	NASA TFTI Tokens	23
5.2.5	NCAD Domain Username/Password	23
5.2.6	Launchpad Username/Password	24
5.2.7	Launchpad Guest Account Username/Password	24
5.2.8	NASA Derived PIV Smartcard Credential	24
5.2.9	NASA-Issued Non-Person Entity (NPE) Certificates	24
5.2.10	Registered Federal Smartcard, CAC, and PIV-I Smartcard Credentials	25
5.2.11	NASA Federated Identity Credentials (FIC)	25
5.3	NASA-Accepted Certificates	26
5.3.1	NASA-Issued Person Certificates	26
5.3.2	NASA-Issued Non-Person Entity (NPE) Certificates	26
5.3.3	Federated Certificates	26
5.3.4	Derived PIV Smartcard Credentials	26
5.3.5	NASA Trust Anchor Management	27
6	Physical Access Management	27
7	Logical Access Management	27
7.1	Description of the Logical Access Management Service	27
7.2	Logical Access Management with new Assurance Levels from 800-63-3	28
7.3	Asset Registration for AART	29

7.4	NAMS Integration	30
7.4.1	NAMS Approval-Based Workflows.....	30
7.4.1.1	NAMS Provisioning	30
7.4.1.2	NAMS Revalidation.....	30
7.4.1.3	NAMS Reconciliation.....	30
7.4.2	Basic levels of Entitlement	30
7.5	Authentication and Authorization Integration	31
7.5.1	Acceptable Authentication Protocols	31
7.5.2	NCAD	31
7.5.3	Access Launchpad	31
7.5.4	Two-Factor Token Infrastructure (TFTI)	31
7.5.5	Federated Authentication with Internal Authorization (FAIA)	31
7.5.6	Federated Authentication with Basic Levels of Entitlement (FABLE)	32
7.6	LOA 4 Memo and Two-Factor Implementation Guidance	32
7.7	Non-Person Entity (NPE) Authentication	32
7.8	Acceptable Certificate Authorities	32
7.9	Inherited NIST SP 800-53 Controls	33
8	Assessing and Mapping Risk, Confidence, and Assurance	43
8.1	Assessing Physical Access Risk	43
8.2	Assessing Logical Access Risk	43
8.3	Determining the LOC of an Identity	45
8.4	Mapping LOR to LOC	45
8.5	Mapping Credential LOA/AAL to LOC and LOR	45
9	ICAM Resources	46
9.1	Training	46
9.2	ICAM Portal	46
9.3	Other Information	46
9.4	Requesting Changes to ICAM Services	46
	Appendix A: ICAM Services Framework	48
	Appendix B: Mapping of LOR, LOC, and LOA	49
	Appendix C: Acronyms	49
	Appendix D: Glossary	54

Table of Figures

Figure 1: NASA's Implementation of Federal ICAM	16
Figure 2: Identity Lifecycle	21
Figure 3: Credential Service Provider Diagram	26
Figure 4: Logical Access Management Service.....	28

Distribution:
NODIS



Associate Chief Information Officer for
Cybersecurity & Privacy

Change History

Version	Date	Change Description
1.0	02/03/2011	Initial Version
1.1	7/15/2015	Updated outdated information and requested a one year extension for rewrite/modification.
2.0	02/06/2016	Updated Version
2.1	02/22/2016	Updated the Handbook to reflect Revision 4 of <i>NIST SP 800-53</i> .
3.0	07/10/2017	Updated Version
3.1	08/08/2018	• Revised to new Handbook format • Updated to reflect specifications in NIST SP 800-63-3
3.2	03/01/2019	ICAM Engineering Review (Draft)
3.3	04/03/2019	OPS Revisions
3.4	06/10/2019	Revised section on Guest accounts
3.5	11/7/2019	Revised Table 3: Controls Guidance
3.6	04/16/2020	Annual Review; Updated Appendix B

1 Introduction

NASA requirements for protecting the security of NASA information and information systems are derived from National Institute of Standards and Technology (NIST) guidance. Information System Owners (ISOs) and other personnel responsible for the protection of NASA information or information systems shall follow NIST guidance in the proper security categorization (*Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization for Federal Information and Information Systems*), and in the selection and implementation of information security controls (*FIPS 200, Minimum Security Requirements for Federal Information and Information Systems* and *NIST Special Publication (SP) 800-53 Revision 4, Recommended Security Controls for Federal Information Systems and Organizations*), in a manner consistent with the Risk Management Framework (*NIST SP 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems*). *NASA Policy Directive (NPD) 2810.1E, NASA Information Security Policy, NASA Procedural Requirements (NPR) 2810.1A, Security of Information Technology*, and the collection of 2810 Information Technology Handbooks (ITS-HBK) satisfy the policy and procedure controls of *NIST SP 800-53 Revision 4, Recommended Security Controls for Federal Information Systems and Organizations*.

This handbook supports implementation of requirements in *NPR 2810.1A, Security of Information Technology (IT)*, *NPD 2810.1E, NASA Information Security Policy* and *NPR 2841.1, Identity, Credential, and Access Management*. It also augments NIST guidance with NASA-specific requirements, procedures and recommendations, where applicable. NASA-specific guidance does not negate NIST guidance, unless explicitly stated. The Agency's organizationally defined values are integrated into the control requirements within the Risk Information Security Compliance System (RISCS).

1.1 Purpose

This document provides detailed guidance to support the requirements published in *NPR 2841.1, Identity, Credential, and Access Management*.

1.2 Scope

The provisions of this Handbook apply to the totality of the ICAM service and the systems and services that leverage it.

Compliance with this Handbook is mandatory. Non-compliance or any unauthorized or improper use of NASA IT may result in the suspension or revocation of access to NASA IT, disciplinary action, as well as civil and criminal penalties.

If a Handbook has or refers to an “expiration date” such date is tantamount to a “review date” for the Handbook. This Handbook and the policy/procedural guidance contained within remains in full force and effect until such time that the Handbook is formally cancelled, rescinded, or superseded by an updated document.

A documented rationale and/or justification shall accompany any non-concurrence, disapproval, denial, or request for deviation from the policy guidance or procedural requirements set forth in this Handbook to support such decision. The documented rationale/justification shall be provided to the NASA Cybersecurity and Privacy Division (CSPD) and the point of contact for this Handbook, in coordination with Center Chief Information Security Officers (CISO), to review and validate for the record.

1.3 Point(s) of Contact for this Handbook

For any questions or comments regarding the contents of this Handbook, contact:

- Rob Birchmeier, NASA ICAM Lead (rob.birchmeier@nasa.gov)
- JP Nicholas, Headquarters Office of Protective Services (OPS) ICAM Program Executive (james.p.nicholas@nasa.gov)

Any questions or concerns regarding perceived gaps in policy or implementation guidance, conflicting procedural requirements, lack of clarity pertaining to specified roles and responsibilities, or issues associated with interpretation shall be elevated to the NASA CSPD, in coordination with the CISO, and directed to the attention of the point of contact for this particular Handbook to address and resolve.

1.4 Applicable Documents

Office of Management and Budget (OMB)

- *M-07-16 Safeguarding Against and Responding to the Breach of Personally Identifiable Information*
- *OMB M-11-11 Continued Implementation of Homeland Security Presidential Directive 12 (HSPD-12) – Policy for a Common Identification Standard for Federal Employees and Contractors*
- *OMB M-16-04 Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*

Federal Information Processing Standards (FIPS)

- *FIPS 199, Standards for Security Categorization of Federal Information and Information Systems*
- *FIPS 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors*

National Institute of Standards and Technology (NIST)

- *NIST Special Publication (SP) 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations*
- *NIST SP 800-60 Revision 1, Guide for Mapping Types of Information and Information Systems to Security Categories*
- *NIST SP 800-63-3, Electronic Authentication Guideline*

- *NIST SP 800-116 Revision 1, Guidelines for the Use of PIV Credentials in Facility Access*
- *NIST SP 800-157, Guidelines for Derived Personal Identity Verification (PIV) Credentials*

Other Departments/Agencies

- *x.509 Certificate Policy For The U.S. Federal Public Key Infrastructure (PKI) Common Policy Framework*
- *x.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA)*
- *Personal Identity Verification Interoperability For Non-Federal Issuers*
- *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard (November 2016/2nd Edition)*
- *OPM Final Credentialing Standards*

National Aeronautics and Space Administration (NASA)

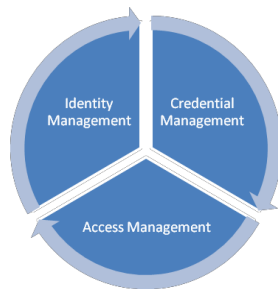
- *NASA CIO/AA, OPS signed memo: OMB M-11-11, Continued Implementation of Homeland Security Presidential Directive-12, (May 01, 2017)*
- *NPR 2841.1, Identity, Credential, and Access Management Services*
- *NPR 1600.4A, Identity and Credential Management*
- *NPR 2800.1B, Managing Information Technology*
- *NPR 2810.1A, Security of Information Technology (Revalidated with Change 1, dated May 19, 2011)*
- *NPD 2810.1E, NASA Information Security Policy*
- *IT-SOP-2841-001.1, Identity Providers and Credential Service Providers Standard Operating Procedure (SOP)*

Cancellations, Updates, Consolidations

- *IT-HBK-2841-03, Identity, Credential, and Access Management Services (ICAM)*

2 ICAM Key Concepts

ICAM addresses three key authentication/authorization questions:



- Who are you?
- How do you prove it?
- What can you access?

When identities, credentials, and access are managed in an integrated, enterprise environment, NASA can better assure that the right people have the appropriate access they need to further the mission of NASA, without putting NASA facilities and logical assets at risk.

Identity Management defines three major facets of a person:

- Distinguishing facts about the person's identity, such as name and date of birth
- Documentation of the affiliation that the person has with NASA, such as civil servant, contractor (e.g., Boeing, Lockheed) or partners (e.g., European Space Agency, Center for the Advancement of Science in Space [CASIS], Japan Aerospace Exploration Agency [JAXA])
- Knowledge of the person's fitness and suitability based on investigations and records checks

Credential Management defines the management of items that allow physical access, such as door keys and Smartcards,¹ as well as other items that allow access to IT systems, such as usernames/passwords and single-factor one-time password devices, commonly referred to as tokens.

¹ The term Smartcard refers to both NASA PIV Smartcards and Agency Smart Badges.

Credential Management seeks to ensure that credentials are:

- Issued to the proper person
- Not tampered with or used by someone other than the owner
- Properly revoked and disposed of when no longer valid

Access Management seeks to ensure that:

- People are properly authorized to access particular NASA assets, based on role
- Changes to a person's roles and/or affiliation, or the knowledge we have about that person, result in a re-assessment of appropriate access
- Access is revoked when a person is no longer affiliated with NASA

NASA's ICAM infrastructure provides the single authoritative identity source (through the Agency Identity Management and Account eXchange [IdMAX] system), single entitlement management engine with strong auditing (through the NASA Access Management System [NAMS]), and central authentication and authorization systems, such as Access Launchpad and NASA Consolidated Active Directory (NCAD). These services provide approximately 30 inheritable *NIST SP 800-53* controls for Agency systems.

The following sections cover a few key concepts that ICAM leverages. Refer to Appendix A: ICAM Services Framework.

2.1 NIST SP 800-63-3 Changes to Level of Assurance

The authoritative definitions of Level of Assurance are from NIST Special Publication 800-63, *Electronic Authentication Guideline*. Level of Assurance (LOA) 1-4 for identities, credentials, and authentication protocols are used throughout this document.

In June 2017, NIST released version 3 of Special Publication 800-63, now called *Digital Identity Guidelines* (800-63-3). 800-63-3 fundamentally changed the meaning of assurance levels and how they are defined. This section will provide an overview to the new scheme and describe the transition.

The original source of assurance strength for identities comes from OMB M-04-04 *E-Authentication Guidance for Federal Agencies*. Four levels of assurance were specified:

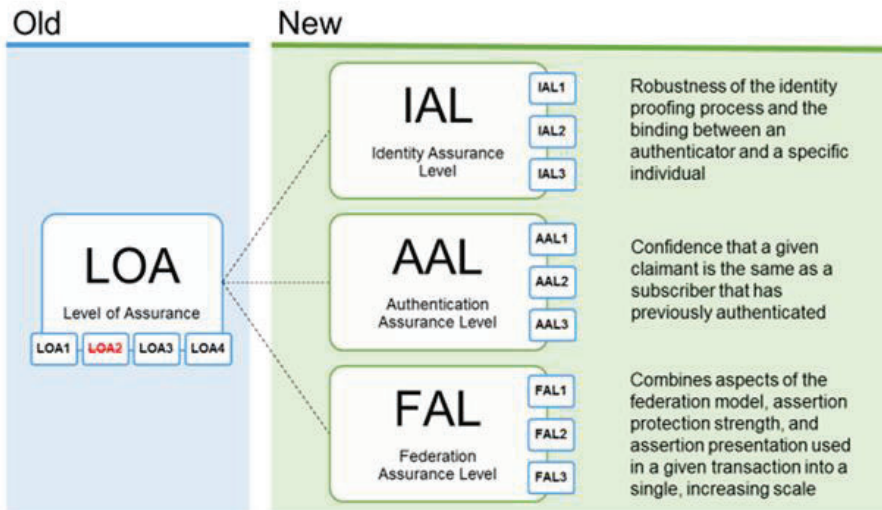
- Level 1: Little or no confidence in the asserted identity's validity.
- Level 2: Some confidence in the asserted identity's validity.
- Level 3: High confidence in the asserted identity's validity.
- Level 4: Very high confidence in the asserted identity's validity.

NIST 800-63 expanded the scope of the levels to include assurance for identity verification, credentials/authenticator issuance and usage, along with strength of authentication protocols.

A criticism of previous LOA scheme is that it combines, some say incorrectly conflates, these subjects:

- Identity: identity certainty through identity resolution, validation, verification.
- Credential: credential, an object or data structure that authoritatively binds an identity to authenticator (authenticator used to be called a token).
- Authentication protocol: security, strength, protocols and their assertion capabilities.

The new scheme decomposes the identity, credential, and protocol portion (called Federation) as per the following illustration.



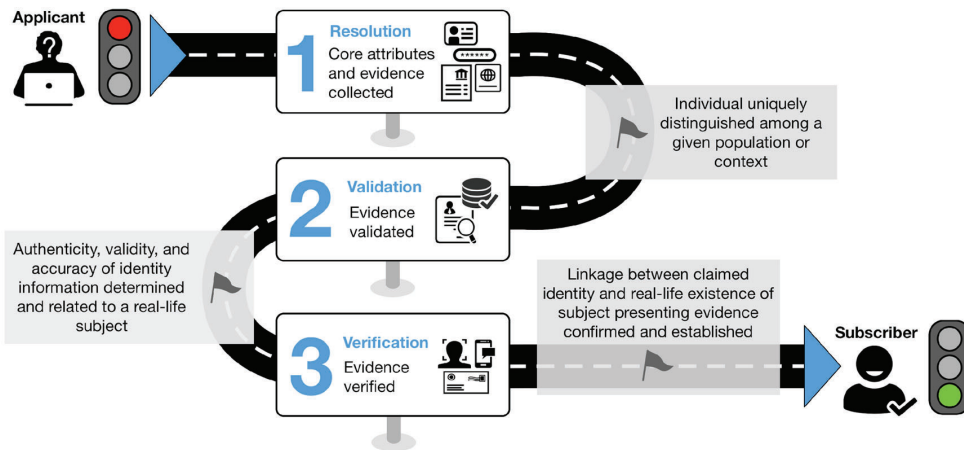
The summary effect of the change is that LOA2 has been dropped and LOA1, LOA3, and LOA4 are now represented by the respective parts for identity (IAL1, IAL2 and IAL3), authentication (credentialing) (AAL1, AAL2 and AAL3), and federation (FAL1, FAL2 and FAL3).

We will provide an overview of Identity Assurance Level (IAL, specified in Special Publication 800-63A, *Digital Identity Guidelines, Enrollment and Identity Proofing*), Authentication Assurance Level (AAL, specified in Special Publication 800-63B, *Digital Identity Guidelines, Authentication and Lifecycle Management*), and Federation Assurance Level (FAL, specified in Special Publication 800-63C, *Digital Identity Guidelines, Federation and Assertions*).

2.1.1 Identity Assurance Level (IAL):

IAL is specified in NIST SP 800-63A, *Digital Identity Guidelines, Enrollment and Identity Proofing*).

The process of identity creation is illustrated here.



Identity creation provides a measure of certainty an applicant is who they say they are. Personal attributes and characteristics are presented for validation and verification to establish proof of an applicant's identity as a subscriber. Identity assurance is not the same as confidence, which will be discussed in a subsequent section.

IA Level	Description
1	Can be self-asserted and not necessarily tied to real identity
2	Can be remotely identity proofed
3	Requires in-person identity proofing

2.1.2 Authentication Assurance Levels (AAL)

AAL is specified in Special Publication 800-63B, *Digital Identity Guidelines, Authentication and Lifecycle Management*.

AAL focuses on the strength of the authenticator, previously referred to as a token. Authenticator strength ensures a relying party a secure means to authenticate a subscriber.

There are several changes with the authentication process. Previously, a user kept a secret for authentication using a software or hardware token. In NIST SP 800-63-3, tokens are referred to as authenticators. Where biometrics are used there are new requirements for freshness (presentation attack detection—PAD). Use of text messages and email to transmit an authentication code is restricted. Where passwords are still utilized, complexity requirements are relaxed and periodic password change is no longer required. Lastly, since authenticators always contain a secret, and considering the many private information breaches, 800-63-3 states that “Knowledge-based authentication, where the claimant is prompted to answer questions that are presumably known only by the claimant, also does not constitute an acceptable secret for digital authentication.”

The primary difference in AA levels is:

AA Level	Description
1	Single-factor authentication
2	Two-factor authentication
3	Two-factor authentication with hardware token

Authenticators afford a relying party, in this case NASA, the opportunity to bind a subscriber’s identity to an authenticator (previously referred to as tokens). The authenticator, in turn, can be used by the subscriber to prove their identity to the organization. Access is subsequently granted based on the level of authentication assurance: higher authentication yields higher potential access.

2.1.3 Federation Assurance Level (FAL)

FAL is specified in Special Publication 800-63C, *Digital Identity Guidelines, Federation and Assertions*.

Federation is a process that allows for the conveyance of authentication and subscriber attribute information across networked systems.

Federation technologies primarily mean that a third party is involved with the authentication process between a user and an application (a relying party). Generally, federation as a concept, more than just the technology, refers to a process where the user and the relying party (RP) are in different organizations. *Assertions* are statements from a source identity provider (IdP) to a relying party (again, usually an application or service) that provide authentication information and optionally attributes concerning a user (a subscriber). A *bearer assertion* (a statement from an IdP representing authentication of the user) is possessed by the user and presented by the user. This is similar to presenting your smartcard at the gate in order to drive on base at a Center. A *holder-of-key assertion* requires that a user show possession of a secret (an authenticator), typically by unlocking the private keys through entry of a PIN with smartcard.

The characteristics of the Federation assurance levels are:

FA Level	Description
1	Bearer assertion, signed by IdP
2	Bearer assertion, signed by IdP and encrypted to RP
3	Holder of key assertion, signed by IdP and encrypted to RP

2.2 Confidence, Risk, Trust, and Assurance

To grant access, ICAM relies on four basic concepts – Level of Risk, Level of Confidence, Level of Trust, and Level of Assurance. It is NASA’s goal to align confidence in an individual with the risk of access, thereby establishing trust and issuing a credential to verify assurance. These terms are described below.

Assets and Asset Roles have a **Level of Risk (LOR)**, which is the degree of potential damage (financial, safety/security, or reputation) that access to an asset represents. The level of risk can help determine what type of background investigation a person requires.

The LOR for an asset is typically computed using guidance provided in *FIPS 199* as part of the security plan assessment process.

People are assigned a **Level of Confidence (LOC)**, which measures:

- the degree of certainty that a person is who they claim to be (determined through identity proofing which correlates to IAL); and
- a person's suitability/fitness for their position or access (determined through background investigations).

Confidence in an individual is related to Contractor Fitness and Civil Servant Suitability and is primarily established through OPM Tier Level requirements.

As identity proofing and background investigation actions are taken, the LOC of a person changes. The required LOC for NASA Workers² (e.g., civil servants and contractors) is determined using OPM position designation tool to identify position risk and sensitivity. NASA Workers require a minimum LOC of 40, with the exception of temporary workers (LOC 30), regardless of work location. The required LOC for non-workers³ (persons without a position or work duties) is determined by the level of risk of assets they may access. Additional information about the LOC thresholds are documented in Appendix B.

Level of Trust (LOT) is the degree of certainty that a person's access to an asset is an acceptable risk. LOT is the direct relation between LOC and LOR; if the LOR for a position or asset is 50, the individual's LOC must be 50 or higher for access to be granted. Mathematically, this is determined by subtracting LOR from LOC with the goal that LOT never be a negative number. If a LOT is negative, a person will require a higher LOC to obtain access to a particular asset. All requests for a higher LOC should go through the local Center Protective Services Office. NASA Workers will typically require a position re-designation in order to obtain a higher LOC to permit access to higher-risk assets.

Credentials have a **Level of Assurance (LOA)** which is the degree of confidence the credential presented for access represents the person accessing the asset. As referenced in 2.1, credential strength is now distinctly valued with an **Authentication Assurance Level (AAL)** in 800-63-3. NASA Workers are required to have an LOA 4 / AAL 3 credential for all access; a federally-issued PIV Smartcard badge, or an Agency Smart Badge. An LOA 3 / AAL 2 credential (e.g., an RSA Token) may be issued to NASA Workers who cannot appear at a NASA facility to be issued an LOA 4 / AAL 3 credential. Credentials with LOA 1 / AAL 1 issued for access to systems and services offered to the public. LOA 2 / AAL 1 passwords (passwords protected by encrypted transport and with other restrictions) may be used as a fallback, with exception, for NASA workers accessing internal NASA applications.

Additional information regarding LOA is found in later sections of this Handbook as well as in NIST SP 800-63. Discussion of AAL, and other updates stemming from 800-63-3, can be found in section 2.1, above.

Additional information on LOR, LOC, LOA, and their relationships is found later in this document. A complete mapping of risk, confidence, and assurance can be found in Appendix A: ICAM Services Framework.

² NASA Workers include federal employees, contractors, detailed employees, and others performing work for NASA (e.g., external partner staff, volunteers, guest researchers, seasonal employees).

³ Non-workers include members of the public utilizing NASA resources for their benefit, foreign partners performing non-NASA work, visitors, tenants, and grantees performing non-NASA work.

2.3 Federated Access

Federation is a process and technology that allows NASA to trust external partners to perform some identity management, credential management, and authentication services for external workers and non-workers. NIST defines Federation as *a process that allows for the conveyance of authentication and subscriber attribute information across networked systems*.

There is some conflict in Federal documentation concerning Federation. The key phrase above is “across networked systems”. Use of an external Federal credential, a PIV or CAC issued by another agency or DoD, for physical access to NASA facility or for logical access by directly using a smartcard reader is not considered Federation. For further information on direct use of external credentials, see section 5.2.10, Registered Federal Smartcard, CAC, and PIV-I Smartcard Credentials.

Examples of Federation include:

- A university grantee uses his/her Federated Identity Credential to access NASA research data on a NASA managed system
- An contractor working externally but collaborating on spacecraft design with data on a NASA system with security categorization low or moderate (but not high)
- A NASA worker accessing an external partner’s information system using Launchpad and single sign-on
- A non-worker customizing a public data set provided from a NASA system for download

Note, the requirements for LOC and LOR in Section 2.1 still apply. For example, a Google Account ID, having Level of Assurance 1/AAL1, is not acceptable for access to Low, Moderate or High categorized risk systems because it does not provide the necessary LOA.

The NASA ICAM architecture is being expanded to allow for flexible central federation while providing the necessary security. The following concepts are in development:

Federated Identity Credential (<u>FIC</u>)	A method for ICAM to utilize the combination of an Identity Provider, a unique user ID, and an assertion of authentication as a unique <i>credential</i>
Augmentations to create Identity workflows to support FIC registration	Basic methods to capture a FIC with Launchpad and enter FIC information into a worker record in IdMAX have been created, but are slated for production NLE Q3 2019
Trust based upon the Federal ICAM Trust Framework Provider Adoption Process (TFPAP)	TFPAP, created by FICAM and GSA, is now deprecated. Until further Federal guidance is available, trusts are based upon relationship types: Contracts via SAA, a procured Service, an IGA, other Federal agencies via reciprocity
Trust based upon Identity Providers use of Federal PKI Root certificate credentials issued with medium and medium-hardware strength	Trusts based upon the PKI model can meet all technical requirements
Federated Authentication with Internal Authorization (<u>FAIA</u>)	• Uses FIC for credential and Launchpad for authentication • Leverages NASA’s Identity Management and Authorization systems, processes and workflows • Appropriate for security plan Moderate⁴
Federated Authentication with Basic Levels of Entitlement (<u>FABLE</u>)	• NASA Identity not necessarily instantiated • Entitlements based on communities of interest • Appropriate for security plan Low rated data

An SOP in development will provide details for the requirements for federation.

2.4 Provisioning, Authentication, and Authorization

Provisioning is the process of granting access to an asset such as a facility or application. When access is requested and approved, it is then provisioned by registering that approved access in a way that can be used later. The NASA Access Management System (NAMS) is the primary means of tracking the

⁴ Due to technical limitations, this method is not generally appropriate for security categorization high.

authorization and provisioning of access to NASA applications. Actual provisioning may be manually handled by application administrators or automated through NAMS.

Authentication is the process of ensuring that a person is who s/he says s/he is, at the time when s/he requests access to an asset. A person presents one or more “authentication factors” to prove s/he is who s/he claims to be. Authentication factors are categorized as:

- Something you know
- Something you have
- Something you are



Some examples of one-factor authentication are using a Username and password to access an application (something you know), using a key to enter a room (something you have), or using a fingerprint (something you are).

Multi-factor authentication uses at least two factors. A Smartcard is considered a one-factor authenticator when it is used alone to access a room (e.g., as a proximity/swipe- only card), and a two-factor authenticator when the Smartcard and Personal Identification Number (PIN) are used to access a room or an application. NIST SP 800-63-3B identifies the permissible forms of multi-factor authenticators.

Use of two or more factors provides greater assurance that the person is who s/he claims to be.

Authorization is the process of ensuring that the person attempting to access an asset or asset role has been provisioned to do so. Authentication and Authorization are often thought of as a single process, but it is useful to understand the difference between the two. A person may be properly authenticated to a system (you’ve proven you are who you say you are), but may not be authorized to access that system. On the other hand, a person may be authorized to access a system but may not be able to authenticate because they have forgotten their password or misplaced their Smartcard.

From the definition above, authorization is the overall process and system used to ensure that a user is authorized to access an asset. It is useful to decompose the authorization process to include entitlements and provisioning. Entitlement comprises the process, workflows, and approvals used to grant access to an asset—the business rules for granting access. NAMS serves this function for NASA. Provisioning is the process of encoding the entitlement decisions into machine-readable attributes. NED (NASA Enterprise Directory, see 3.5) and NCAD (NASA Consolidated Active Directory, see 3.6) are the primary repositories for these attributes.

3 Systems that Support ICAM Services

The systems listed in this section support the ICAM services listed in *NPR 2841.1*. In the following sections, the service section number that is being referenced from *NPR 2841.1* is noted in parentheses.

Information about systems that support ICAM services are available on the ICAM Portal at <https://icam.nasa.gov>. The ICAM Portal is solely dedicated to the work of ICAM and current information to the user base. The ICAM Portal provides desk guides, one-pager instructional overviews, educational videos, frequently asked questions, lower level handbooks and other useful guides. The ICAM Portal provides points of contacts for all areas related to ICAM from an Agency as well as a Center perspective. There are also detail tabs within the portal for each specific discipline of ICAM (e.g., Identity, Physical, Logical, Badging). Also, the ICAM Portal is a direct link to all ICAM Reporting as well as community based forums that users may want to join.

NASA's Implementation of Federal ICAM

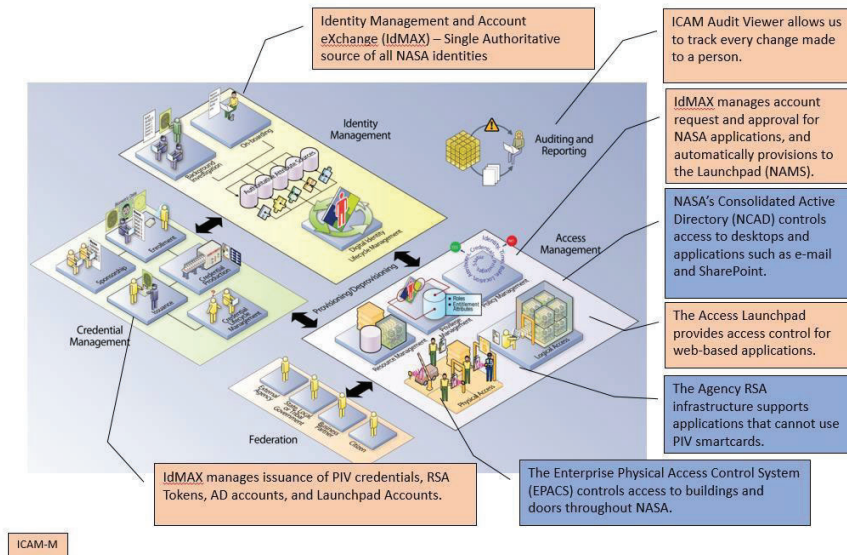


Figure 1: NASA's Implementation of Federal ICAM

3.1 Identity Management & Account eXchange (IdMAX)

The IdMAX system provides authoritative data and business process workflows to manage identities, credentials and access. The following Services described in *NPR 2841.1* are provided through IdMAX in whole or in part:

- Identity Lifecycle Management Services (1.1.1)
- Identity Maintenance Services (1.1.2)
- Credential Lifecycle Management Services (1.2.1)
 - Certificate Management Services (1.2.2)
 - Asset Management (1.3.1)
 - Community (Role Based) Access Management (1.3.2)
 - Permission Management (1.3.3)

Some level of access to IdMAX is provided to NASA Persons⁵ as a Basic Level of Entitlement (BLE). The Uniform Resource Locator (URL) for IdMAX is: <https://idmax.nasa.gov>.

3.2 Enterprise Physical Access Control System (EPACS)

EPACS provides electronic physical access control through door readers to buildings and rooms throughout NASA. Door readers accept either Smartcards or proximity cards for access. EPACS also provides video surveillance, alarm monitoring, and intrusion detection for security personnel within the OPS. The following services described in *NPR 2841.1* are provided through EPACS (for physical assets only):

- Asset management services (1.3.1)
- Permission management services (1.3.3)
- Authentication services (1.3.4)
- Authorization services (1.3.5)

3.3 Agency Application Rationalization Tool (AART)

The Agency Application Rationalization Tool (AART) is NASA's authoritative source for applications. The following service described in *NPR 2841.1* is provided through AART:

⁵ NASA Persons are NASA Workers and Non-Workers.

- Asset Management Services (1.3.1)

Access to AART can be requested through NAMS. The URL for AART is: <https://aart.nasa.gov>.

3.4 NASA Access Management System (NAMS)

NAMS is a component of IdMAX and serves as the primary means of requesting and approving access to NASA applications and physical resources. NAMS manages information at the asset level and includes workflow engines to manage the processing of individual access and authorization requests to assets as well as final provisioning and de-provisioning.

NAMS processes are initiated through IdMAX at <https://idmax.nasa.gov>. The following services described in *NPR 2841.1* are provided in whole or in part through NAMS:

- Asset Management (1.3.1)
- Community (Role Based) Access Permission Management (1.3.3)

Access to NAMS is granted as a BLE to all NASA Workers.

Development, end user, and support documentation can be found at: <https://icam.nasa.gov>.

3.5 NASA Enterprise Directory (NED)

NED provides consolidated information about people such as name, phone number, and email address. The following services described in *NPR 2841.1* are provided by the NED in whole or in part:

- Directory Services (1.1.3)
- Authorization Services (1.3.5)

A web interface to the NED is available at: <https://id.nasa.gov>.

A publicly accessible web interface to a subset of NED information is available at: <https://people.nasa.gov>.

Applications can directly use the information in NED. The NED may also be accessed directly by applications using the Secure Lightweight Directory Access Protocol (LDAP) at the URL <ldaps://dir.nasa.gov>. Note that information available may be restricted by access context. Resources for application developers can be found in the ICAM Portal <https://icam.nasa.gov>.

3.6 NASA Consolidated Active Directory (NCAD)

NCAD is an Agency-wide enterprise level distributed instance of the Microsoft Active Directory (AD) service. NCAD Engineering is currently working on a modernization project that will enhance the security and availability of the environment. NCAD is present at all NASA Centers and sites and is the Agency standard mechanism to provide AD based authentication and authorization services to NASA computer systems. NCAD supports the requirement for PIV Mandatory authentication supporting federally issued PIV smartcards and the Agency Smart Badge for logical access. The following services described in *NPR 2841.1* are provided by NCAD in part:

- Authentication Services (1.3.4)
- Authorization Services (1.3.5)
- Directory Services (1.1.3)

NASA Civil Servants are granted NCAD accounts as a BLE. All other NASA Persons are granted NCAD accounts through the NAMS tool at IdMAX on an as-needed basis. NCAD accounts are required for access to AD-integrated applications such as the NASA Operational Messaging and Directory Service (NOMAD) email and messaging services as well as other central domain managed services such as Agency SharePoint instances.

Additional information about NCAD is available at: <https://ncad.nasa.gov>.

3.7 Access Launchpad

The Access Launchpad (aka Launchpad) provides authentication and authorization services for applications that are not integrated with NCAD (typically web or Security Assertion Markup Language [SAML] 2.0-based applications). Launchpad currently is implemented with Computer Associates SiteMinder product. Launchpad supports the use of NASA and other federally-issued Smartcards, NASA TFTI tokens, and usernames/passwords for authentication. Launchpad also enforces session lifetime security controls. The following services described in *NPR 2841.1* are provided by the Launchpad in part:

- Authentication Services (1.3.4)
- Authorization Services (1.3.5)

Every enabled NASA Identity can register for a Launchpad login capability by providing security questions and answers. The URL for the Launchpad is: <https://launchpad.nasa.gov>. First time users with logical access are directed to visit this URL to create their profile by clicking on the “First Time User” button at the top of the screen. Launchpad accounts are required for Launchpad applications such as the System for Administration, Training, and Educational Resources for NASA (SATERN), <https://id.nasa.gov>, NOMAD and Web Time and Attendance Distribution System (WebTADS). Information for developers can be found at: <https://icam.nasa.gov/group/icam/launch-wiki>. If you are not already signed in, you will arrive at <https://icam.nasa.gov> where you will sign in and click the Launchpad tab.

3.8 Two-Factor Token Infrastructure (TFTI)

The TFTI service provides token-based two-factor authentication and authorization services for users who are not Smartcard eligible or systems that do not support NCAD, Launchpad, or other Smartcard-enabled authentication services. The TFTI authentication mechanism consists of a hardware token (key fob) or software token (for a smartphone), assigned to a computer user that generates an authentication code at fixed intervals (usually 30 or 60 seconds) using a built-in clock and the factory-encoded random key.

The following services described in *NPR 2841.1* are provided by TFTI in part:

- Authentication Services (1.3.4)
- Authorization Services (1.3.5)

NASA Persons can request TFTI tokens through the NAMS tool in IdMAX.

NASA system integration requires that a Plan of Action and Milestones (POA&M) or Risk-Based Decision (RBD) be filed in the Agency RISCs system.

3.9 NASA Operational Certificate Authority (NOCA)

The NOCA service provides PKI certificates for user authentication, encryption, and signing. The service also provides Transport Layer Security (TLS) certificates for machine validation. The following services described in *NPR 2841.1* are provided by the NOCA PKI service:

- Certificate Management Services (1.2.3)
- Certificate Validation Service (1.3.6)

NASA Workers who are PIV-qualified will receive a NASA-issued FIPS 201-2 compliant PIV Smartcard with PKI certificates from the NOCA. See Section 5.4 for a description of the NOCA PKI user certificates. System Administrators may request NOCA PKI certificates for Non-Person Entities (NPEs), such as computers and applications using the PKI Support Tool in IdMAX, available at <https://idmax.nasa.gov/tools/pki>.

Additional information can be found at: <http://pki.nasa.gov>.

3.10 NASA Internal Certificate Authority (NICA)

The NICA, formerly known as the Microsoft Certificate Authority (CA), manages PKI NPEs and user-derived certificates for NASA internal use. The following services described in *NPR 2841.1* are provided by the NICA:

- Certificate Management Services (1.2.3)
- Certificate Validation Service (1.3.6)

NCAD-bound computers are issued certificates through the NICA as needed to allow for device authentication. The NICA also provides a Simple Certificate Enrollment Protocol (SCEP) service for network device enrollment and derived certificates for mobile devices.

System Administrators may request NPE certificates issued from the NICA for service accounts or applications through the PKI Support Tool tool in IdMAX, available at <https://idmax.nasa.gov/tools/pki>.

3.11 ICAM Tools

The ICAM project provides a number of support tools, including Identity Self Service (iD) and the ICAM Support Console. The most commonly used tools are listed below; others may be found on the ICAM Portal at <https://icam.nasa.gov>.

3.11.1 Identity Self Service (ID)

The ID Web application allows a user to view their corporate information and to look up information for other users. The application also allows users to manage their personal information used in emergency notifications, request changes to email addresses and display names, and to perform annual access revalidation to a NASA facility or system. Updates to some information requires LOA 3/AAL2 or better access.

The URL for iD is: <https://id.nasa.gov>

3.11.2 ICAM Support Console

The ICAM Support Console is a web application designed for the customer support analysts (e.g., the Help Desk, Enterprise Service Desk [ESD]). This tool provides the ability to reset Launchpad passwords, troubleshoot, and temporarily turn off mandatory PIV Smartcard login desktops and laptops to allow use of NCAD credentials instead (in cases where the PIV Smartcard has not yet been issued, has been lost, or is otherwise unavailable).

The URL for the ICAM Support Console is: <https://icamsupport.nasa.gov>

3.12 NASA Privileged Access Management System (NPrivAMS)

The standard method to perform administrative functions at NASA is through the use of NCAD Administrative accounts, commonly referred to as AA accounts. It is a requirement that all administrative functions be performed at LOA 4/AAL3 – using the Smartcard for authentication to these accounts. Therefore, all AA accounts are set to Smartcard use only.

In cases where a password is required for an administrative task, a password can be checked-out from the NASA Privileged Access Management System (NPrivAMS), which functions as a credential vault. The credential vault is implemented using the Computer Associates (CA) Privileged Access Manager (formerly CA Xceedium) product. Resource administrators may request the use of a password for their AA account by using the “AGCY0025 Active Directory Resource Management Account” NAMS workflow in IdMAX and selecting the “Xceedium Solution” option. The administrator may then, after being authenticated via their Smartcard, check out a randomly generated password for a period of 18 hours. Each day, AA Account passwords, and the associated NTHash (cryptographically generated key), are regenerated for all AA accounts.

Active Directory generic accounts which are enabled and are not restricted to Smartcard only have passwords managed by NPrivAMS in the same manner as AA accounts. Passwords expire every 60 days, and support a “many to one” view policy to accommodate multiple owners for a single generic account.

4 Identity Management

Identity Management refers to the creation, maintenance, and termination of digital records of people who have a relationship with NASA.

ICAM ensures that NASA can associate a person's identity to an appropriate IAL and LOC, helping NASA asset owners make risk-based determinations about granting access to NASA physical and/or logical assets.

A complete list of IALs and LOCs and associated requirements is found in Appendix A: ICAM Services Framework.

4.1 Types of Identities

NASA recognizes two distinct groups of identities: workers and non-workers. NASA Workers directly support the mission and goals of NASA or are compensated by NASA (e.g., civil servants and contractors). Non-workers use NASA resources and/or information to conduct independent work not directly for the benefit or consumption of NASA (e.g., researcher using computational hours on a NASA supercomputer). Refer to Appendix D: Glossary.

All identities are digital records of the individual, stored in IdMAX. The differences between the types of identities are the volume of identity information, depth of identity vetting, and the potential LOC.

The Office of Human Capital Management (OHCM), the Office of Protective Services (OPS), Office of Procurement (OP), and Office of the Chief Information Officer (OCIO) have joint responsibility for managing NASA Identities.

4.1.1 NASA Identities

NASA Identities are full identity records with complete identity data of individuals who have undergone the full NASA identity vetting process. The individual is required to have their identity requested, sponsored, enrolled, vetted, and authorized prior to receiving a credential. The strength of the identity registration process will determine the IAL. The LOC for most NASA Identities is between 20 and 70 depending on the depth of identity vetting performed.

NASA Identities may be workers or non-workers, depending on their relationship with NASA, who may be granted a credential as well as access to assets through NAMS requests and approval workflows in IdMAX. NASA Identities will be registered in IdMAX and relevant attributes are provisioned to NED, NCAD, EPACS and trusted cloud services.

4.1.2 NASA Guest Identities

NASA Guest Identities are non-workers who will receive no credential (except Username/Password) and will be granted no access (except guest services). NASA guest identities will be provisioned to NED only. There are three tiers of NASA Guest Identities.

Public Guest Identities are used for access to security data categorization Public information, typically to tailor a public NASA website profile for content viewing preferences. The LOC for a NASA Public Guest is set to 10 after confirmation of email address. Public Guest identities are IAL 1.

NASA Managed Guest identities are basic identity records with minimal identity data of individuals who have had their identity requested by an individual with a NASA identity. The LOC for a NASA Managed guest is set to 15 only after confirmation of email address, by virtue of NASA work sponsorship and managed by a worker with a full NASA Identity. NASA Managed Guest identities are typically IAL 1.

NASA Trusted Guest Identities are managed guest identities that have additionally registered a non-NASA smartcard credential and have completed remote proofing via Trulioo. The LOC for a Trusted Guest is set to 20.

4.1.3 NASA-Trusted Identities

NASA-trusted identities are partial identity records with most identity data of individuals who have been vetted by a trusted partner organization, based on a trust agreement. The IAL/LOC for a NASA-trusted identity is determined by the allowances of the trust agreement.

NASA-trusted identities are non-workers who will receive credentials and access based on the provisions of the trust agreement. NASA-trusted identities will be registered in IdMAX and provisioned to NED, NCAD, EPACS and cloud services as required by the trust agreement.

The trust agreement is an official agreement between NASA and another organization (e.g., commercial entity, foreign government). The trust agreement identifies the vetting procedures performed by the trusted organization that is then used by NASA to determine the IAL for identities associated with the trusted agreement and any additional vetting requirements that NASA may require to affect the LOC. The trust agreement also identifies the identity interactions between NASA and the organization for NASA to use the identities of individuals affiliated with the trusted organization.

4.1.4 Federated Identities

Federated identities are complete identity records with most identity data of individuals affiliated with a partner entity who have been vetted by a trusted external organization or identity provider (IdP). The identity attributes of the individual are provided to NASA and the entire identity lifecycle is maintained by the external IdP. Identity information is provided to NASA for gaining logical and physical access to protected assets utilizing credentials owned and managed by the partner entity.

4.2 Identity Lifecycle

The diagram below depicts the Identity Lifecycle. For additional information on use of identities, refer to the IdMAX User Handbook.

Identity Lifecycle (Provision Access)

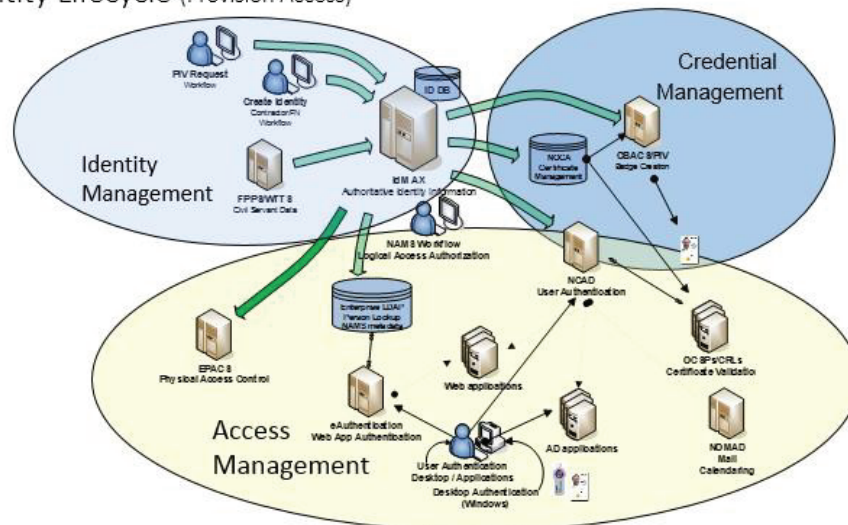


Figure 2: Identity Lifecycle

4.2.1 Creation

The IdMAX system is used for the creation of all identity records. When the NASA Visitor Management System (NVMS) is released, NVMS will be used to create identities for individuals who require access 29 days or less (cumulative) in a 365 day period and do not require logical access. IdMAX will continue to be used to create identities for those individuals who require access for 30 days or more in a 365 day period, those who require logical access for any duration, and all foreign nationals.

Identities are created through the efforts of identity requesters and through identity invitations. Requesters submit identity information on the behalf of an individual in order to create an identity record. For NASA Employees, The OHCM performs the role of requester through the Workforce Transformation Tracking System (WTTTS). The identity invitation tool allows an individual to submit one's own information prior to it being reviewed by the requester.

When an identity is created, it is assigned a NASA Universal Uniform Personal Identification Code (UUPIC). The UUPIC is a unique 9-digit number used to identify individuals associated with NASA, in place of a social security number. Use of the UUPIC and other requirements related to the UUPIC can be found in NPR 1600.4.

4.2.1.1 Identity Associated with a Registered Credential

Registered credential identities are identity records based partially upon identity data of individuals who have been vetted by another federal government agency (e.g., National Oceanographic and Atmospheric Administration [NOAA], Department of Defense [DoD]) or accredited PIV-I Smartcard credential issuers. The LOC for a registered credential identity will be based on the credential being registered. PIV-I credentials do not assert any suitability assurance.

Registered credential identities may be workers or non-workers, depending on the relationship with NASA; e.g., a non-worker might be a tenant at a NASA Center such as NOAA at Stennis. Registered credential identities will retain the credential issued them by their federal government agency but also may be issued an Agency Smart Badge in situations where their existing Federal Smartcard is not compatible with NASA technologies. Access will be based on the specific needs of the relationship as well as the LOC inherited by the credential (40 for Federal Smartcards) and may be increased based on need and validation of existing investigations for reciprocity. Registered credential identities are registered in IdMAX and provisioned to NED. Provisioning to other repositories is based on specific needs.

4.2.2 Maintenance

Maintenance of an identity includes all activities that occur between identity creation and termination. This includes performing updates to an identity record (correcting or updating identity data), renewal or reissuance of a credential, and adding access to an identity record. Certain maintenance activities may be initiated and completed by the user while others require initiation and action by identity officials.

4.2.3 Termination

Identities are terminated when an individual's affiliation with NASA ends through voluntary or involuntary means. Termination is the final act of separation and results in all access being permanently removed. Basic information will be retained in order to support audit history but any subsequent reactivation will require creation of the identity.

5 Credential Management

Credential Management refers to the issuance, registration, use, and termination (lifecycle) of credentials issued to people and devices for use in NASA facilities and systems.

ICAM ensures NASA can associate a person's identity to a credential with an appropriate LOA/AAL, and to help determine the appropriate credential for access needs.

5.1 Level of Assurance (LOA)/Authentication Assurance Level (AAL)

LOA/AAL is the degree of confidence the credential presented for access represents the person accessing the asset. Credentials are assigned an LOA/AAL primarily based on two criteria:

- The process used to issue the credential
- The number of authentication factors used to authenticate with the credential and resistance to potential security attacks

The higher the LOA/AAL, the more resistant the credential and the more detailed the issuance process. NASA Workers are required to have an LOA 4/AAL3 credential, a PIV or ASB Smartcard credential, for all logical access. This requirement supports *OMB Memo M-11-11* which requires Smartcards be used for access to all federal government systems and facilities. LOA 4/AAL3 Agency Smart Badges are issued to individuals who do not meet the requirements for a PIV Smartcard but still need an LOA 4/AAL3 credential for logical access. Credentials with LOAs 1-3 / AAL1-2 are issued by NASA for access to systems and services offered to non-Workers and the public.

NIST SP 800-63 / 800-63-3 sets out the requirements for LOA / IAL / AAL / FAL for electronic authentication to logical assets and *NIST SP 800-116* sets the requirements for LOA for physical access authentication, based on the risk of the access to the asset. *FIPS 201* summarizes the requirements for both physical and logical access.

5.2 Credential Types

NASA issues and accepts credentials which allow physical only, logical only, or physical and logical access to NASA assets. All credentials are bound to an identity and grant access utilizing an approved authentication mechanism. All applications that use credentials must be credentials issued or trusted by NASA for end-user authentication.

Credentials trusted by NASA are those issued by another federal government agency, a trusted partner, or a federated partner.

5.2.1 NASA PIV Smartcard

The NASA PIV Smartcard is issued by OPS for both physical and logical access. All NASA Workers working for NASA for 180 days or more in a 365 day period are required to have a NASA PIV Smartcard per *OMB Memo M-05-24* and the *OPM Final Credentialing Standards*. All NASA Workers qualifying for a NASA PIV Smartcard are required to travel to a NASA Center to obtain their NASA PIV Smartcard.

The NASA PIV Smartcard is an LOA 4/AAL3 credential issued to persons with an LOC of 35 or higher. The NASA PIV Smartcard provides authentication to all non-classified assets and most classified physical asset areas.

The NASA PIV Smartcard is the primary credential used for on-site access to physical and logical assets, except where restricted by technology or eligibility. Remote NASA Workers needing logical access to NASA IT systems are required to travel to a NASA Center to in order obtain their NASA PIV Smartcard.

5.2.2 Agency Smart Badge

The Agency Smart Badge (ASB) is a non-PIV Smartcard issued by OPS, for both physical and logical access, to individuals who are PIV Smartcard ineligible (e.g., individuals at NASA for less than 180 days in a 365 day period, or foreign nationals in the U.S. for less than 3 years). An Agency Smart Badge is an LOA 4/AAL3 credential issued to persons with an LOC of 30 or higher. The Agency Smart Badge provides authentication to non-classified assets. Individuals qualifying for an Agency Smart Badge are required to travel to a NASA Center to obtain their Agency Smart Badge.

5.2.3 NASA Visitor Badges

NASA Visitor Badges are issued to persons requiring access to a specific NASA Center for 29 days or less in a 365 day period. A NASA Visitor Badge allows non-electronic physical access to the Center's open areas. All other access on a visitor badge must be escorted or issued a special badge for proximity access. NASA Visitor Badges will be issued using the NASA Visitor Management System once it is fully deployed at NASA.

5.2.4 NASA TFTI Tokens

NASA Two-Factor Token Infrastructure (TFTI) Tokens are issued by the OCIO for IT access only and provide two-factor authentication for users who are not eligible to receive a Smartcard or where the user needs to access a system that is unable to utilize a Smartcard for authentication purposes.

Persons must meet LOC 20 or higher to be eligible for a NASA TFTI token. This credential meets LOA 3/AAL2. Access to IT assets at an LOR of 30 or lower can utilize this credential for remote access.

5.2.5 NCAD Domain Username/Password

The NCAD (NDC – NASA Data Center) Domain accounts are issued by the OCIO for IT access only. NAMS workflows to create NCAD Domain accounts are triggered during the identity process for NASA Persons. For civil servants, the domain account is automatically provisioned as a BLE. For all other NASA Persons, the Identity Requester indicates the domain account will be needed which begins the account creation process. It can also be requested in NAMS.

NCAD Domain username/passwords provide one-factor authentication for users who cannot use Smartcards (because they are, lost, stolen, damaged, etc.). Persons vetted at LOC 20 or higher are eligible to obtain an NCAD username/password credential. Such credentials are LOA 2/AAL1. IT assets rated at LOR 20 or below may allow the use of username/password credentials; assets with a higher LOR

may not. NASA is actively working to reduce the use of NCAD username/passwords through the requiring the use of a smartcard credential for domain account authentication.

5.2.6 Launchpad Username/Password

The Launchpad accounts are issued by the OCIO for IT access only. Launchpad usernames/passwords provide one-factor authentication for users who cannot use Smartcards or TFTI Tokens for access to Launchpad integrated applications. The Launchpad provides access control for web-based applications. Launchpad accounts are provided as a BLE to all active NASA Workers.

Persons vetted at LOC 20 or higher are eligible to obtain a Launchpad username/password credential. Such credentials are LOA 2/AAL1. IT assets rated at LOR 20 or below may allow the use of username/password credentials. Assets with a higher LOR may not use Launchpad username/password for authentication.

5.2.7 Launchpad Guest Account Username/Password

The Launchpad guest account is used for IT access only. Launchpad guest accounts provide one-factor authentication for very low-risk access to IT assets. Launchpad guest accounts can be created by any NASA Worker with an active IdMAX identity. The identity information of the guest user is not verified. Launchpad guest accounts can be created directly using IdMAX, submitted to ICAM as a batch process, or created dynamically by the guest user via self-registration within an application configured to support self-registration.

Launchpad guest accounts do not have LOC requirements. The guest identity is a claimed identity using either a password or a Google login as a credential. Application owners must receive explicit approval from ICAM and the Security Integrator before allowing this type of credential to access NASA applications.

5.2.8 NASA Derived PIV Smartcard Credential

A derived PIV Smartcard credential is an X.509 certificate derived from an applicant's original PIV Smartcard credential. A derived PIV Smartcard credential is an additional identity credential for use with mobile devices. A derived credential can be issued based on proof of possession and control of an authenticator associated with a previously issued PIV Smartcard credential, so as not to duplicate the identity proofing process. NASA has the capability to issue derived credentials to the enterprise managed mobile devices including tablets and smartphones in which the hardware interface for an add-on Smartcard reader is challenging.

Derived credentials are intended for certificate-based user application authentication and mobile services including virtual private network authentication and corporate wireless network authentication. The provisioning process is designed to conform to the guidance from *NIST SP 800-63-3* and *NIST SP 800-157*.

NASA Derived PIV Smartcard credentials currently are issued from the NASA Internal Certificate Authority (NICA), and are not interoperable per the *NIST SP 800-157* guidance. Therefore, first generation NASA Derived PIV Smartcard credentials can only be accepted for user authentication on systems and equipment that have the NICA trust anchors or utilize Launchpad services.

The implementation is leveraging the Center for Internal Mobile Applications (CIMA) mobile authentication architecture, which is integrated with the enterprise mobile device management gateway implementation. The Mobile Device Registration Service provisions derived PIV Smartcard credentials. Once there is a viable business case, NASA derived credentials may also be issued from the NASA Operational Certification Authority to ensure that the credentials are interoperable government-wide to ensure compliance with *NIST SP 800-157*.

5.2.9 NASA-Issued Non-Person Entity (NPE) Certificates

NPE certificates are issued to computing devices, operating systems, network appliances, or applications to authenticate end-points, generally for secure data exchange. Both the NOCA or NICA certificate authorities are used to issue NPE certificates internally within NASA. To request an NPE certificate from either the NOCA or NICA, visit <http://pki.nasa.gov> and review the Server Certificates FAQ. The FAQ

contains detailed instructions for the necessary steps to follow to submit an NPE request through the NAMS tool in IdMAX, as well as technology specific certificate request guidance.

It is permitted to obtain certificates for NPEs from approved acceptable commercial certificate authorities (some restrictions may apply). To obtain commercial certificates for NASA Websites, the Agency Webmaster can provide additional guidance and provider approval.

Self-signed NPE certificates are not permitted for use at NASA except in network isolated environments.

5.2.10 Registered Federal Smartcard, CAC, and PIV-I Smartcard Credentials

OMB and NIST guidance requires NASA to accept Federal Smartcards and Common Access Card (CAC) Smartcards issued by other federal agencies and the Department of Defense for identification and authentication. In addition, NASA can accept PIV-I Smartcards from non-federal PIV Smartcard issuers as well as other credentials from partners and the general public. Therefore, NASA does accept Federal Smartcards issued by other federal agencies, as well as CAC Smartcards issued by the United States Department of Defense. NASA will support PIV-I Smartcards from accredited providers. PIV-I Providers, for which NASA will accept PIV-I credentials issued from, are listed at:

<https://www.idmanagement.gov/trust-services/#piv-i>.

The requirements for LOC and LOR in Section 2.2 still apply.

5.2.11 NASA Federated Identity Credentials (FIC)

In a process similar to the way an externally issued Smartcard may be bound to a NASA identity, a FIC may also be bound to a NASA identity. The Trust Framework Provider Adoption Process (TFPAP) provides guidance as a basis for forming trust in the remote identity and the asserted credential. NASA is planning to accept TFPAP approved credential service providers (CSPs) and expand the credential registration capabilities.

Note, as of year-end, 2018, TFPAP has been deprecated. Until there is new guidance from GSA and NIST on a trust process for Federation NASA will rely on contracts with a Space Act Agreement (SAA), a procured Service, an IGA, or other Federal agencies via reciprocity to form trust relationships. A typical case for NASA is to form Federation relationships with trusted business partners. This will normally entail completion of a SAA.

Notionally, a FIC is comprised of a pair, also known as a tuple, of the identity provider and a unique name or key representing the identity. As with all externally issued credentials, there are life cycle management considerations should attribute change with the unique identifiers making up the FIC, including a change of the name of an identity provider.

The unique name or key may take one of multiple forms. The preferred form is an immutable key similar to the UUPIC. The following figure shows the functions the Credential Service Provider (CSP) that an IdP can provide. Though this figure is from a deprecated reference, TFPAP, the services of a CSP are clearly shown. *IT SOP-2841-001, Identity and Credential Service Providers Standard Operating Procedure (SOP)* provides additional details about federal requirements for Federated Identities.

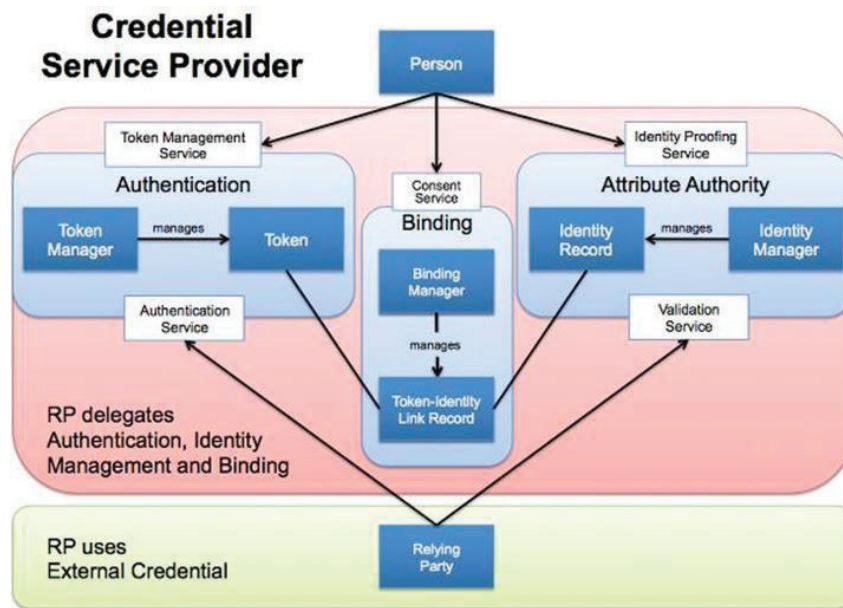


Figure 3: Credential Service Provider Diagram

5.3 NASA-Accepted Certificates

5.3.1 NASA-Issued Person Certificates

The NOCA is the sole issuer of PKI certificates for Smartcards at NASA. The NICA issues the user derived certificates.

- PIV Authentication Certificate
- Encryption Certificate
- Signing Certificate
- Card Authentication Key (used for physical access)

These certificates are issued as part of the PIV Smartcard issuance process.

5.3.2 NASA-Issued Non-Person Entity (NPE) Certificates

NPE Certificates are issued in order for computing devices and applications to securely exchange data.

The following NPE Certificates can be used by NASA systems:

- NOCA Certificates
- NICA Certificates
- Commercial Certificates

Use the NAMS tool in IdMAX to request NOCA and NICA Certificates. Visit <http://pki.nasa.gov> for information about use of Commercial Certificates.

5.3.3 Federated Certificates

NASA can accept PKI certificates for authentication, encryption, and signing from any entity that is cross-certified with the Federal Bridge Certificate Authority (FBCA). The document *X.509 Certificate Policy for The Federal Bridge Certification Authority (FBCA)* outlines policies for various PKI certificates and can be found at:

http://pki.treas.gov/docs/x509_certificate_policy_for_the_federal_bridge_certification_authority.pdf

Procedural requirements for cross-certification are established and maintained by the Federal PKI Policy Authority (FPIPA). Information can be at: <https://www.idmanagement.gov/fpki/>

5.3.4 Derived PIV Smartcard Credentials

NASA systems and networks can accept active Derived PIV Smartcard credentials from external federal-approved credential issuers for user authentication, that are interoperable and compliant to the *NIST SP*

800-157 guidance for Derived PIV Smartcard Credentials. Externally issued Derived PIV Smartcard credentials do need to be registered with the person's NASA identity.

5.3.5 NASA Trust Anchor Management

Computer operating systems, as well as some third-party applications, such as Mozilla Firefox, Mozilla Thunderbird, Adobe products, and Java, contain trusted certificate stores. The trusted certificate stores provide the root of trust for authentication, secure transactions, data protection, communication channel protection, device trust, and code integrity. The certificate stores are already preloaded and updated periodically by the product vendors with trusted certificates that are required for standard business functionality. In addition to these vendor-supplied certificates, some of these certificate stores require additional certificates for interoperability with Agency and Agency affiliate services. This collection of additional certificates is managed through the NASA Trust Anchor Management (NTAM) effort. More information on NTAM can be found on the Cybersecurity Standards and Engineering Team (CSET) website at <https://cset.nasa.gov/idi/trust-anchor-management/>.

6 Physical Access Management

EPACS provides physical access control through door readers and other devices throughout the Agency. NASA-issued PIV Smartcards, Agency Smart Badges, and Center-specific proximity cards can be used to access physical assets protected through EPACS.

Physical access requests are managed through the NAMS tool in IdMAX and can be automatically provisioned for all Centers. Similar to applications, Physical Access Management (PAM) developers can assign an LOR to physical resources to ensure users are appropriately vetted. Users requiring access to a Center other than their assigned location can initiate an access request through the NAMS tool in IdMAX.

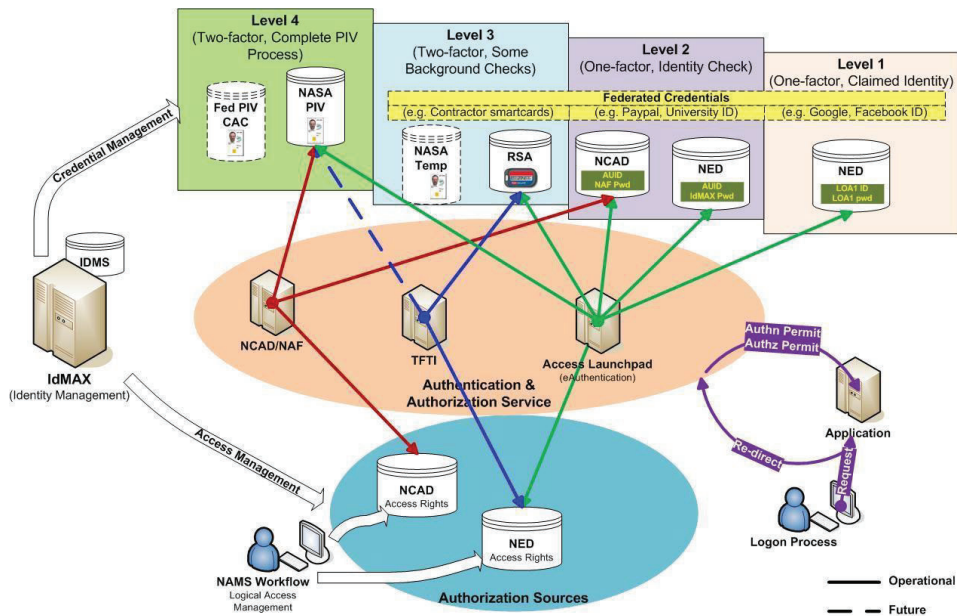
NIST SP 800-116 and *NPR 1620.3* provide guidance for deploying the appropriate authentication mechanisms for physical assets. The Interagency Security Committee Facility Security Level Determination Matrix provides mandated guidance for assigning levels of risk to facilities.

7 Logical Access Management

Logical Access Management includes processes for requesting, approving, and provisioning access to applications, systems, as well as authentication and authorization of specific access requests.

7.1 Description of the Logical Access Management Service

The diagram below depicts NASA's Logical Access Management Service.



As depicted, all credentials issued or registered, and all access provisioned, are tied to a person's records managed through IdMAX. Upon approval of an access request made through the NAMS tool in IdMAX, entries are made in one of the NASA Authorization sources. When a person attempts to access a NASA system or application, the Authentication/Authorization service validates the credential, including the Level of Assurance, being used (authentication), and the access rights provisioned (authorization). The logical access management service then allows or denies access.

NASA has integrated the NCAD and Launchpad authentication services so that NASA people who log in to NCAD with a smartcard through their desktop computer on the NASA internal network, can access any NCAD or Launchpad-enabled application without re-authenticating. This is referred to as Single Sign-On or Simplified login.

7.2 Logical Access Management with new Assurance Levels from 800-63-3

The following table shows requirements for IAL, AAL, and FAL, along with the notional NASA LOC scheme.

Table 1: *Nominal Assurance Level Usage by Security Categorization with Level of Confidence Overlay*

Security Categorization	Acceptable Assurance Level(s) ⁶	Minimum Expected Level of Confidence ⁷
Public ⁸	IAL1-3 AAL1-3 FAL1-3	LOC 0-10
Low	IAL2-3 AAL1-3 FAL2-3	LOC 20+
Moderate	IAL2-3 AAL2-3 FAL2 ⁹ , FAL3	LOC 30+
High	IAL3 AAL3 FAL2 ¹⁰ , FAL3	LOC 40+

Where compliance with the assurance level requirements cannot be met, a Risk Based Decision (RBD) shall be included in the associated System Security Plan (SSP).

7.3 Asset Registration for AART

All websites, web-applications, and custom applications that are in-scope for *NPR 2841.1* are required to be registered in AART. The URL for AART is: <https://aart.nasa.gov/>.

The AART site includes user guides and instructions for applying for access. Access to AART is granted through the NAMS tool in IdMAX.

AART includes many attributes that are used by OCIO for various reporting and compliance purposes. Most fields are required to meet the registration requirement in *NPR 2841.1*; however, other OCIO groups may need these fields. The fields listed below are needed for ICAM:

- Center
- Application Name
- URL¹¹
- Description/Purpose
- Responsible Org
- FIPS 199 system security categorization
- TFTI or Virtual Private Network (VPN) Infrastructure?
- System/Application Owner
- Security Plan Number in RISCs
- Contains Personally Identifiable Information (PII)?

⁶ These are the nominal designations. Due to exigencies, such as specific agreements, Intergovernmental Agreements (IGAs), etc., there may be variance with specific use cases.

⁷ Ibid.

⁸ Public refers to 'Public Information'. 'Public information' means any information, regardless of form or format, that an agency discloses, disseminates, or makes available to the public (44 U.S.C. Chapter 35). Rules for access here concern access where a persistent profile is provided for customization of display, selection, or related capabilities for public access to public information. See also 'Public Access', Page 34, in NIST SP 800-53 Revision 4.

⁹ As FAL3 (Holder of Key) is not widely supported, FAL2 may be used within NASA based on concepts specified in prior SP 800-63 versions, namely:

- All Verifiers are under the control of a single management authority that ensures the correct operation or Verifiers are trusted partners operating under explicit agreements with NASA.
- The Subscriber authenticates to the Verifier using an AAL2 or AAL3 authenticator as appropriate.
- FAL3 requirements unrelated to non-repudiation are satisfied.

¹⁰ Ibid.

¹¹ If applicable.

7.4 NAMS Integration

All NASA applications that require authentication and authorization must use the NAMS tool in IdMAX for access requests, approval, and provisioning. NAMS includes a Workflow Configuration Tool (WCT), which is used to set up NAMS approval-based workflows and BLEs. Contact the Center's Logical Authorization Subject Matter Expert (SME) for assistance with NAMS integration. The list of ICAM SMEs is available at <https://icam.nasa.gov> on the home page. The ICAM Organization Chart can also be found in Appendix E – ICAM Organization Charts.

7.4.1 NAMS Approval-Based Workflows

Approval-based workflows are used when each access request must be approved by the system owner or delegate. Approval-based workflows can be set up to allow approval workflows from very simple to extremely complex. Approval workflow can branch by Center, and/or by specific role in the application. Approvals can be set up to be a group, be sequential or concurrent. Escalation workflows are also supported. Center Logical Authorization SMEs can help determine the best way to set up a NAMS workflow for applications.

Many application owners have found that they can simplify the approval process that was used prior to NAMS integration. This is because NAMS already ensures that potential users are active in IdMAX, have taken IT security training, and have fully completed the NAMS request. NAMS can also automatically initiate processes to close accounts when someone leaves NASA. Furthermore, assets can be configured to automatically close access based on a number of factors including explicit expiration date, expired training, and changes in LOC for the user.

7.4.1.1 NAMS Provisioning

NAMS allows for either manual or automatic provisioning once the final approval has been received.

With manual provisioning, an email is sent from NAMS to the list of defined provisioners, who then set up the appropriate access, and confirm in NAMS that they have completed the provisioning task.

With automatic provisioning, a system call is made that provisions the access. Automatic provisioning allows NAMS to directly provision authorization in applications that support it. Provisioning occurs in two ways – by NCAD or Launchpad group membership, or by a direct Simple Object Access Protocol (SOAP) communication to an application's provisioning URL. Applications integrated with NCAD can use NCAD group membership to indicate authorization. Applications that use Launchpad can use NED groups. To support automatic provisioning applications must be prepared to use one of these methods to automatically build internal structures needed to support appropriate user access.

7.4.1.2 NAMS Revalidation

All NASA Persons with access granted through NAMS must revalidate their need for access on an annual basis. NAMS sponsors can also revalidate accounts on behalf of a user. Revalidation simply means reviewing registered accounts to verify that they are needed for an individual to perform their duties at NASA. Each time revalidation occurs, the user's revalidation "clock" is reset, meaning it will be another year before the user will be prompted to revalidate. Users should revalidate their accounts anytime their position or affiliation at NASA changes.

7.4.1.3 NAMS Reconciliation

Reconciliation is a process of ensuring that access rights recorded in NAMS for a particular application match what is actually provisioned in the application. Periodic review of access is needed to ensure that applications are not allowing access that has not been approved in NAMS, especially where manual provisioning is used. NAMS does not provide any direct mechanisms for reconciliation, however reports can be generated via the ICAM Reporting tool which can then be imported into a per-application custom reconciliation tool to generate exceptions.

7.4.2 Basic levels of Entitlement

BLE is the term used to describe access that is granted based on membership in a particular community that is captured through an attribute. For example, several applications are BLEs for civil servants. Any active NASA Person with the civil servant attribute set in the NED is automatically provisioned to access these applications.

BLEs must be registered in NAMS by the NAMS Admin. Currently, the BLE registry in NAMS is simply an informational record, and, like manual provisioning above, the application's development team must ensure that access is properly granted based on the BLE attributes defined.

7.5 Authentication and Authorization Integration

Authentication and Authorization integration can be complex, and requires involvement of an application's development team. Center Logical Authorization SMEs can help to coordinate conversations between the application development team and ICAM service providers. This section explains some basics about integrating applications with the ICAM infrastructure.

7.5.1 Acceptable Authentication Protocols

NASA has standardized on the following authentication protocols for the central authentication services. Within the NCAD environment, Kerberos is the accepted authentication protocol. Certificate-based authentication typically implemented with Transport Layer Security (TLS) client authentication can be used. Within Access Launchpad, SAML 2.0 is the preferred accepted authentication protocol (integration with SiteMinder policy agents for authentication is an acceptable alternative).

Integration with Access Launchpad via SAML 2.0 shall use the [Federal ICAM \(FICAM\) SAML 2.0 Web Browser Single Sign-On \(SSO\) Profile](#) as the baseline profile.

Applications and services that are authenticating to the NDC Domain NCAD using methods other than the Kerberos protocol must submit a POA&M (if future compliance is planned) or a RBD request (if future compliance is not planned) through RISCs system.

7.5.2 NCAD

Applications integrating with NCAD should do so utilizing the Kerberos protocol. Further guidance on how to integrate with NCAD is available at: <https://icam.nasa.gov>.

7.5.3 Access Launchpad

Web-based applications must integrate with the Access Launchpad. In some cases, a web proxy integrated with the Launchpad can be used to allow access to a non-web application. Guidance on how to integrate with the Launchpad is available at: <https://icam.nasa.gov/launchpad>.

7.5.4 Two-Factor Token Infrastructure (TFTI)

The TFTI supports applications that require two-factor authentication, yet cannot leverage either NCAD or the Access Launchpad. A POA&M or RBD request must be submitted via the RISCs system for applications that use TFTI; however, this is an acceptable alternative when neither NCAD nor the Launchpad can be used.

7.5.5 Federated Authentication with Internal Authorization (FAIA)

The primary use case of Federation for NASA will include the creation of a NASA identity in IdMAX and the use of NCAD and Launchpad/NED for authorizations. This method is called *Federated Authentication with Internal Authorization* (FAIA). Section 5.3 references the Federated identity that is instantiated in IdMAX and used by NAMS. Section 5.3 also references the use of a FIC for authentication. FAIA will be suitable for use with most classes of systems at NASA, including FIPS 199 Security Categorization (SC) Low and Moderate. FAIA may be usable for SC High systems with additional controls and methods.

Assurance levels associated with FAIA are strong; they should be FAL2 or FAL3. From section 2.1,

FA Level	Description
2	Bearer assertion, signed by IdP and encrypted to RP
3	Holder of key assertion, signed by IdP and encrypted to RP

FAL3 is not yet widely implemented. FAL2 should be augmented with additional controls where FAL3 is not practicable.

For SC High systems, credential registration (see 5.2.10) may be considered.

7.5.6 Federated Authentication with Basic Levels of Entitlement (FABLE)

Based on previous efforts through the National Strategy for Trusted Identities in Cyberspace (NSTIC) comes the ability to use acceptable IdP brokers for access to NASA. Though definitive implementations and general authority for Federal utilization is limited at this time, one public facing IdP that NASA can utilize is login.gov.

It is anticipated that there will be some class of NASA systems, typically those with SC Public or Low data, which will be able to be utilized without specific authorization to a user. These systems will authorize users based upon membership in a class. NASA ICAM architecture uses the terminology community membership for such situations. NASA ICAM considers this use case *Federated Authentication with Basic Levels of Entitlement (FABLE)*.

7.6 LOA 4 Memo and Two-Factor Implementation Guidance

Citing *OMB M-11-11*, the *NASA CIO/OPS LOA 4 Memo (March 29, 2017)* directs that a PIV Smartcard be used for routine authentication at NASA, with some exceptions. NASA Persons who are ineligible for a PIV Smartcard need to use an Agency Smart Badge. Notably, all administrative roles must use LOA 4/AAL3 authentication. In cases where a password is required for an administrative task, a password can be checked-out from the NASA Credential Vault/NPrivAMS (3.12).

Other relevant two-factor federal directives include *OMB Memo 04-04*, *OMB Memo 07-16*, and *NIST SP 800-63*. These documents require:

- Remote, moderate-risk, and high-risk access must be protected with LOA 3/AAL2 or better credentials.
- Remote access to Privacy information must be protected with LOA 3/AAL2 or better credentials, and that credential must be separate from the device being used.

Beyond mandating Smartcard use, the governance directives also require retirement of the NCAD password. NASA is transitioning NCAD user accounts to use of a Smartcard only. The state of Smartcard only authentication for NCAD users accounts is known as User-Based Enforcement (UBE).

Center VPNs implement Smartcard authentication as an option in addition to TFTI tokens for two-factor access. TFTI token use for this purpose is expected to decline over time.

Any application can enforce two-factor authentication at the application layer. For NCAD, the choice of authenticator is a password (where such use is properly exempted) or a Smartcard. Applications can enforce access to Smartcard use through Authentication Mechanism Assurance (AMA). NCAD's implementation of AMA causes use of the Smartcard by the user to be represented as a Windows Security Group. A list of approved object identifiers (OIDs) are maintained for which security groups are created. For example, NCAD has a security group based on usage of a certificate with the *id-fpki-common-authentication* OID. If a user is a member (set dynamically at logon through use of a Smartcard) of *id-fpki-common-authentication*, then the user used a PIV Smartcard for domain logon. For Launchpad integrated applications, application owners can configure for two-factor access by requiring an LOA 3/AAL2 credential (TFTI tokens) or LOA 4/AAL3 (Smartcards).

7.7 Non-Person Entity (NPE) Authentication

As referenced in Section 5.2.9, self-signed certificates are not permitted for use at NASA except in network isolated environments. NPE certificates are typically authenticated to prove device identity, to establish secure communication channels (Internet Protocol Security [IPSec], TLS), or to provide access to resources. In all cases, relying parties are responsible for validating certificate status. Relying parties should avail themselves of NASA Certificate Authority (or other issuing certificate authority) Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP) services for this purpose.

Please see <https://pki.nasa.gov> for further information.

7.8 Acceptable Certificate Authorities

NASA accepts any Certificate Authority that has been cross-certified with the Federal Bridge Certificate Authority (FBCA). The FBCA is cross-certified with all federal CAs, as well as major CAs serving private

industry. The Certipath Bridge CA, which includes major Aerospace corporations that partner with NASA, is one of the private industry CAs that is cross-certified with the FBCA.

NTAM includes all root and intermediate certificates that should be included in The Federal PKI Program audits the cross-certified CAs. A listing is available at: <https://www.idmanagement.gov/fpki-cas-audit-info/>

7.9 Inherited NIST SP 800-53 Controls

When asset authorization approval processes are integrated with NAMS and real-time authentication/authorization relies on NCAD or the Launchpad, several security controls required by *NIST SP 800-53* are inherited from the ICAM services, and applications do not have to enforce these controls.

ISOs can cite these Security Plans when they inherit controls from ICAM Services:

Table 2: ICAM Services Security Plans

Plan Number	Plan Title	Uses
OA-9999-M-MSF-2968	NASA Agency Forest	Inherited controls when NCAD is used as the Authentication/Authorization source.
OA-9999-M-MSF-2712	Identity, Credential and Access Management (ICAM)	Inherited controls for Identity Management, for provisioning through NAMS, Authentication/Authorization through the Access Launchpad

Any low-risk or moderate-risk application can inherit controls from either security plan.

Table 2 explains which *NIST SP 800-53* controls are inherited, and to what extent, when applications are integrated with NAMS and the Authentication Architecture.

Table 3: Controls Guidance

Control	ICAM Responsibility	Application/Resource Owner Responsibility	Comments
AC-1 Access Control Policy and Procedures	Responsible for the Central Authentication and Authorization (A&A) source/service	Responsible for the application	
AC-2 Account Management (1) <i>Automated System Account Management</i>	Responsible for management of accounts.	Responsible for management of access to the application.	NAMS provides the automated mechanism for both account and access management. Application owners are responsible for adhering to the NAMS process for adding and removing accounts.
AC-2 Account Management (2) <i>Removal Of Temporary/Emergency Accounts</i>	Responsible for automatic termination of accounts.	Responsible for termination of access.	Through NAMS, temporary and emergency access should have an expiration date of 15 days. Application owners should review NAMS access lists and ensure access is removed when the expiration date is reached. NAMS sends "Close Account" requests automatically whenever an individual leaves NASA.
AC-2 Account Management (3) <i>Disable Inactive Accounts</i>	Responsible for disablement of inactive accounts.	Agency apps are required to use LP or NCAD or obtain a deviation. NCAD has a process in place to enforce disabling inactive accounts at 60 days.	Application owners do not need to employ automated processes to disable access. Semi-annual reconciliation of NAMS access lists and application accounts is sufficient to meet this control. Application owners do not have to remove access based on inactivity for applications that are accessed infrequently as a matter of course.

Control	ICAM Responsibility	Application/Resource Owner Responsibility	Comments
AC-2 Account Management (4) <i>Automated Audit Actions</i>	Responsible for account audits. Responsible for access audits to the extent that access is handled by the Central A&A source.	Responsible for access audits managed within the application.	NAMS provides part of this audit capability. Typically, basic access to the application is managed by the Central A&A source, and it therefore has audit responsibility. Auditing of creation, modification, disabling, and termination actions performed in NAMS.
AC-2 Account Management (5) <i>Inactivity Logout</i>	ICAM enforces screen lock after 15 minutes of inactivity.		NCAD provides part of this capability.
AC-2 Account Management (13) <i>Disable Accounts For High-Risk Individuals</i>	Responsible for providing application owners up-to-date Level of Confidence values for persons. Responsible for coordination of the termination of access if an identity is terminated.	Responsible for evaluating changes to Level of Confidence values for persons in accordance with Section 2.1 of the ICAM Handbook and terminating accounts which exceed an acceptable level of risk.	NAMS supplies the report of LOC changes. NAMS issues account close requests for terminated identities.
AC-3 Access Enforcement	May provide the control, but not responsible for restricting privileged functions on the A&A source itself.	Responsible for restricting privileged functions on the application.	Customized NAMS workflows may be used to facilitate access applications for detailed resources, roles or privileges, but it is up to the system owners to interpret and enforce such access.
AC-4 Information Flow Enforcement	None.	Application owners retain full responsibility for this control.	

Control	ICAM Responsibility	Application/Resource Owner Responsibility	Comments
AC-5 Separation of Duties	None.	Application owners retain full responsibility for this control.	
AC-6 Least privilege	Responsible for enforcement only if the least privilege set is "All."	Application Owners are responsible for enforcing least privilege unless the least privilege set is "All."	In general, Central A&A sources provide coarse-grained access to the application itself, and applications provide finer-grained access control. Therefore, applications are responsible for enforcing least privilege except in those rare cases where the Central A&A source is providing finer-grained access control.
AC-7 Unsuccessful Login Attempts	Responsible for managing unsuccessful login attempts.	None.	
AC-8 System Use Notification	Responsible for system use notification.	None.	
AC-9 Previous Logon Notification	Central A&A sources can provide this information.	Applications can display the information provided by the Central A&A source, if desired.	The previous logon information provided would be the last logon to any application using the Central A&A source, not necessarily the last logon to the specific application.

Control	ICAM Responsibility	Application/Resource Owner Responsibility	Comments
AC-11 Session Lock	Responsible for providing Group Policy mechanism and processes for deployment of necessary settings to NCAD integrated Windows machines. For applications using standard integration to Launchpad with the Web Agent, responsible for session lock requiring re-authentication.	For NCAD integrated Windows machines, responsible for ensuring necessary Group Policy Object is applied. For Launchpad applications that are SAML based or self-configured, the application is responsible for implementing session suspension based upon a pre-determined period of inactivity thus necessitating re-authentication through Launchpad.	
AC-11 Session Lock (1) <i>Pattern-Hiding Displays</i>		For NCAD integrated Windows machines, responsible for ensuring that the session lock mechanisms obscures the screen.	
AC-12 Session Termination	Responsible for session termination within ICAM applications.	Responsible for terminating sessions within the application.	
AC-14 Permitted Actions without Identification or Authentication	Not applicable.	Responsible if non-authenticated access is granted.	By definition, Central A&A sources only deal with identified and authenticated users.

Control	ICAM Responsibility	Application/Resource Owner Responsibility	Comments
AC-16 Automated Labeling	None.	Responsible for any required labeling of information.	Application sources can use identifiers passed by the A&A source to label information.
AC-17 Remote Access (1) <i>Automated Monitoring/Control</i>	Responsible for the A&A sources.	Responsible for the application.	
AC-17 Remote Access (2) <i>Protection Of Confidentiality/Integrity Using Encryption</i>	Responsible for the A&A sources.	Responsible for the application.	
AC-17 Remote Access (3) <i>Managed Access Control Points</i>	Responsible for the A&A sources.	Responsible for restricting access points to their application.	
AC-17 Remote Access (4) <i>Privileged Commands/Access</i>	May provide the control, but not responsible for ensuring this control is met.	Responsible for ensuring that remote access for privileged functions is permitted only for compelling operational needs	

Control	ICAM Responsibility	Application/Resource Owner Responsibility	Comments
AC-18 Wireless Access Restrictions	Not applicable. Not inheritable from ICAM.	Not applicable.	
AC-19 Access Control for Portable and Mobile Devices	Not applicable. Not inheritable from ICAM.	Not applicable.	
AC-20 Use of External Information Systems	Not applicable. Not inheritable from ICAM.	Not applicable.	
AU-6 Audit Review, Analysis, and Reporting	Responsible for review, analysis, and reporting of audit records pertaining to the A&A sources.	Responsible for audit records pertaining to the application.	
IA-1 Identification and Authentication Policy and Procedures	All A&A sources follow NASA policy and procedures.	None.	

Control	ICAM Responsibility	Application/Resource Owner Responsibility	Comments
IA-2 User Identification and Authentication	Full responsibility.	None.	
IA-2 User Identification and Authentication (11) <i>Remote Access – Separate Device</i>	ICAM is responsible for providing Smartcards and TFI tokens which are separate devices, as well as the authentication infrastructure to enable the use of those devices.	Applications integrated with Launchpad should ensure LOA 3/AAL2 or LOA 4/AAL3 authentication is required. Applications integrated with NCAD should ensure LOA 4/AAL3 authentication is nominally required.	Applications that cannot integrate with the ICAM Infrastructure require a PO&AM, and the application owner is then responsible for implementing LOA 3/AAL2 or LOA 4/AAL3 authentication for remote access.
IA-2 User Identification and Authentication (12) <i>Acceptance Of PIV Smartcard Credentials</i>	ICAM is responsible for providing Smartcards and the authentication infrastructure to enable the use of these cards.	Application is responsible for integrating into ICAM authentication services as per Section 7.4 of this document to enable PIV Smartcard authentication.	ICAM provides a service to register Smartcard credentialed users from DoD and other federal agencies for use within NASA.
IA-3 Device Identification And Authentication	ICAM provides PKI certificates for certificate-based device authentication.	Application is responsible for proper device authentication and validation.	
IA-4 Identifier Management	Full responsibility within the ICAM service.	Application has responsibility to properly map ICAM identifiers to records for authorization within the application.	Identifiers under the purview of ICAM are not reused, including AUIDs.

Control	ICAM Responsibility	Application/Resource Owner Responsibility	Comments
IA-5 Authenticator Management	Full responsibility for the provisioning and management of ICAM authenticators including NCAD and Access Launchpad passwords, one-time password devices, and PIV, ASB and PIV-I smartcards. ICAM enforces proper issuance, credential strength fitness for purpose, processes for lost, damaged, and stolen credentials, credential lifetime controls, and password enforcement for complexity and against re-use.	Responsibility for non-ICAM authentication methods.	
IA-8 Identification And Authentication (1) <i>Acceptance of PIV Smartcard Credentials from Other Agencies</i>	Full Responsibility as documented in Section 5.2.10.	None.	
IA-8 Identification And Authentication (2) <i>Acceptance of Third-Party Credentials</i>	Responsibility for ICAM authentication services.	Responsibility for non-ICAM authentication services.	NASA information systems should not be using authentication mechanisms beyond those identified in Section 7.4; however, in the event that other authentication sources are used, the application is responsible for ensuring that only FICAM-approved third-party credentials are used. As practical, ICAM will work to enable use of other FICAM-approved third-party credentials.

Control	ICAM Responsibility	Application/Resource Owner Responsibility	Comments
IA-8 Identification And Authentication (3) <i>Use Of FICAM-Approved Products</i>	Responsible for ICAM components.	Responsible for application components.	
IA-8 Identification And Authentication (4) <i>Use Of FICAM-Issued Profiles</i>	Responsible for ICAM components.	Responsible for application components.	
IA-8 Identification And Authentication (5) <i>Acceptance Of PIV-I Smartcard Credentials</i>	Responsible for ICAM components.	Responsible for application components.	
SC-17 Public Key Infrastructure Certificates	ICAM is fully responsible.		Other application/resource owners should use the NASA Trust Anchor Management Service to ensure interoperability.

8 Assessing and Mapping Risk, Confidence, and Assurance

Section 2.1 at the beginning of this document provided an introduction to risk, confidence, assurance, and their basic relationships. All position risks are assessed using the calculations defined by the OPM Position Designation Tool and implemented in IdMAX.

A complete mapping of risk, confidence, and assurance can be found in Appendix B – ICAM Services Framework and Appendix B: Mapping of LOR, LOC, and LOA.

IdMAX currently tracks investigations (used to establish confidence) which lead to clearances. Clearance information is not currently tracked in IdMAX; therefore, clearances must still be verified for individuals accessing classified assets through Personnel Security.

8.1 Assessing Physical Access Risk

NIST SP 800-116, Interagency Security Committee Facility Security Level Determination Matrix, and *NPR 1620.3* provide guidance for assigning levels of risk to facilities and deploying the appropriate authentication mechanisms for physical assets.

The process for determining physical risk is as follows:

1. Determine the Facility Security Level (FSL) of the physical area using the Interagency Security Committee process from *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard (November 2016/2nd Edition)* and map to NIST security impact level.
 - a. FSL II (minimum for NASA controlled area) – Controlled
 - b. FSL III – Limited (refer to step 2.b-c)
 - c. FSL IV – Limited or Exclusion (refer to step 2.d-e)
2. Map the NIST security impact level to the level of risk.
 - a. Controlled – LOR 35-40¹²
 - b. Limited (unclassified) – LOR 50
 - c. Limited (classified SECRET) – LOR 55
 - d. Exclusion (unclassified) – LOR 60 (OPTIONAL based on Center risk determination)
 - e. Exclusion (TOP SECRET) – LOR 70
3. Add all identified assets and their associated risks in the NAMS workflow configuration tool and deploy appropriate authentication mechanisms (e.g., door readers).

8.2 Assessing Logical Access Risk

Logical risk for an IT system falls into two broad categories: the overall risk that the system presents, and the risks inherent in various roles within the system. Overall IT system risk is documented in the IT System Security Plan (SSP) and is determined by processes detailed in FIPS-199. The SSP will document the logical risk for each role within the system.

There are many instances where a role may have restricted access to application data which may present a lower risk than the overall application risk itself. For example:

- A System that contains Personally Identifiable Information (PII), Sensitive but Unclassified (SBU), or International Traffic in Arms Regulations (ITAR)/Export Administration Regulation (EAR) will have a minimum risk categorization of “Moderate” due to confidentiality requirements. A role within the application that restricts a specific user’s access to a limited amount of PII, SBU, or ITAR/EAR may, however, be considered a “Low” risk role. Roles that permit access to a large or unlimited amount of PII, SBU, or ITAR/EAR within the application would be at least “Moderate.”

¹² Temporary workers (LoC 30) may be granted access (per the OPM Credentialing Standards and OPM 05-24) to controlled facilities (LoR 35).

- A System that has a “Moderate” risk categorization due to availability requirements may be rated by the FIPS-199 process as “Low” for data integrity and confidentiality. Therefore, roles that do not affect data availability (e.g., normal user roles) could be categorized as “Low,” while those that do affect availability (e.g., system or database administrator) would be categorized as “Moderate”.
- A system that is categorized as “High” risk due to life safety management may have “Low” or “Moderate” view only roles if those roles do not impact operations.

NAMS allows for an overall asset IT LOR. The LOR for the overall asset is defined in the main IT Asset definition “Basic Asset Configuration” section. NAMS handles asset LOR in one of two ways:

- If the “Is level of risk required?” bullet is set to “Yes” then a requester cannot request an asset/role unless their LOC at least matches the IT LOR for the asset/role.
- If the “Is level of risk required?” bullet is set to “No” then a requester can request the asset/role, A warning flag is applied to the request so that approvers and provisioners know to pay special attention to the request.

Similarly, NAMS can apply LOR checks to each role defined for the asset. For role definitions NAMS provides the following flags:

- “Privilege Type” is a non-enforced reporting identifier that flags the type of privilege a role carries. This flag is used in various OMB reports and should reflect the maximum privilege level granted by the role within the asset.
- “Level of IT Risk” defines the LOR conferred by the role. This may be lower than the overall LOR of the asset as noted above.
- “Is level of risk required?” determines whether or not a particular user may request a role based on their LOC. If set to “Yes” then a user without sufficient LOC to cover the specified LOR cannot request the role. If set to “No” a user without sufficient LOC can make the request but it is flagged for approvers and provisioners for special consideration.

The process for determining IT LOR settings for NAMS assets and roles is:

1. Determine the overall risk of the IT System using the FIPS-199 process. This step is normally carried out by the cognizant Information System Security Officer (ISSO) under the auspices of the ISO.
 - a. For Low risk systems the LOR would normally be 40 it may be more appropriate to set the LOR for the asset to 35. This allows users with in-process investigations (LOC 35) to request access in NAMS while their investigations are pending. Any system that requires Smartcard access shall always be set to at least LOR 35.
 - b. The “Is level of risk required?” flag should be set to “No” to allow users access if the LOR of any roles (see below) is less than the overall LOR of the asset. Thus a Moderate (LOR 50) asset with a Low (LOR 30) role should set this flag to “No”. If all roles have an LOR at or above that of the overall asset then the flag should be “Yes”.
2. Identify system roles. These are typically defined in the SSP, however not all roles may be explicitly spelled out in the SSP; for example a “basic access” role may be implied by simply having access to the system. Typically you should see:
 - a. Normal user/worker roles.
 - b. Administrative roles including system administration, database administration, system operations.
 - c. Non-worker/external roles.
3. Work with the ISSO and ISO to assign appropriate LOR values to each system role. In general:
 - a. The LOR for a role should be commensurate with the FIPS-199 analysis performed as part of the SSP development. Roles not explicitly defined in the SSP should be analyzed against FIPS-199 criteria to assign an LOR.

- b. Identify whether or not the role is privileged within the application. The LOR for privileged roles should not be less than the overall LOR for the asset as defined in the SSP but may be higher.
- c. LOR for most non-privileged roles should be set commensurate with the FIPS-199 risk for the role as determined in the SSP.
 - i For Moderate and High systems user roles with restricted access may be set to Low as discussed above.
 - ii For Moderate and Low roles enforcement of the LOR is usually approved on a case-by-case basis so the “Is level of risk required?” flag should be set to “No.”
- d. LOR for administrative (privileged) roles will usually be the LOR of the system, so administrative role in a High system would be 60, Moderate system would be 50, and Low system would be 40. The “Is level of risk required?” flag should normally be “Yes.”

8.3 Determining the LOC of an Identity

In order to determine the overall confidence associated with an individual, positions for workers are assessed through the Position Designation Tool which determines the necessary investigation process for the position. Position designations should take into account the complete list of logical and physical assets to which the position has or could potentially access.

NASA Workers undergoing an investigation are assigned an LOC of 35 following submission of an investigation and completion of a fingerprint check. Temporary workers are assigned an LOC of 30 following the onboarding and proofing process and completion of a fingerprint check.

Non-workers requiring logical-only access will be proofed to an LOC 20 minimum, and non-workers requiring physical access will be proofed to an LOC 30 minimum. Therefore, non-workers are restricted to very-low risk roles (LOR 30 or less) that do not require an investigation (excepting special circumstances). Trusted identities will have their LOC established by the agreement. Guest Identities have their LOC set by the level of proofing performed, which also establishes IAL.

8.4 Mapping LOR to LOC

The LOC determines the highest asset or role LOR an individual may access without risk acceptance. A person’s LOC may be equal to or higher than, but should never be lower than, the LOR of the asset or role to which access is requested.

Access to an asset or role with an LOR higher than an individual’s LOC will require risk acceptance or a change in position. Risk Acceptance is granted by the application owner.

8.5 Mapping Credential LOA/AAL to LOC and LOR

The levels of assurance, in terms of strength, maybe a simple concept but a can be complex in implementation. The following section describes the complexity of credential LOA/AAL and introduces new terms beyond basic credential LOA/AAL discussed earlier in this document.

LOA, with regard to a credential used for access, has three distinct factors:

- Potential LOA/AAL – the LOA/AAL granted a credential based on its capabilities (e.g., fingerprints, factors, etc.), discussed in earlier sections.
- Required LOA/AAL – the mapping of LOA/AAL and LOR to ensure the credential being used cannot grant access to assets with a higher risk than the credential allows.
- Actual LOA/AAL – the mapping of LOA/AAL and LOC to determine the degree of certainty the person accessing the asset is the person who was granted access.

Each of these LOA/AAL factors works together to enable and allow access while ensuring access is limited to what is permitted. There is a very important relationship between the values of LOA/AAL, LOC, and LOR that must be taken into account. These are outlined, in numeric order of precedence, below:

1. LOC must be greater than or equal to LOR (i.e., confidence in the individual must be higher than the asset risk).
2. LOA/AAL must be greater than or equal to LOR (i.e., higher risk assets may not be accessed by lower assurance credentials).
3. LOA/AAL may be higher than LOC (i.e., a higher assurance credential can be given to a person with low confidence).

While LOA is measured on a scale of 1 to 4, it can be easily translated into multiples of 10 (i.e., LOA 1=10, 2=20, 3=30, and 4=40). The new AAL can also be mapped to a numeric range (see Table 1 in section 7.2, *Nominal Assurance Level Usage by Security Categorization with Level of Confidence Overlay*). The relationship between potential, actual, and allowed LOA/AAL is easier to conceptualize using this scale. Beyond LOA 4/AAL3 (40), credential capabilities (e.g., protocol strength, PIN, biometric, certificates) enable LOA 4 /AAL 3 credentials to access assets and roles with risks up to 70 and enforce confidence up to 70. A complete mapping of risk, confidence, and assurance can be found in Appendix A: ICAM Key Concepts Chart and Appendix B: Mapping of LOR, LOC, and LOA. Administrative roles will always require an LOA 4 credential.

9 ICAM Resources

This section discusses ICAM resources that are available (e.g., ICAM Portal, SATERN training, forums, distribution lists).

9.1 Training

SATERN provides training for specific roles within ICAM, such as Identity Requesters and Sponsors. To find training visit: <https://satern.nasa.gov>

Following is a list of the available courses:

- Personal Identity Verification (PIV) Security Workbench
- NASA Access Management (NAMS) Developer and Support Course
- Personal Identity Verification (PIV) Affiliation Sponsor
- Personal Identity Verification (PIV) ICAM Overview
- Personal Identity Verification (PIV) Issuance Official
- Personal Identity Verification (PIV) Foreign National Approver
- Personal Identity Verification (PIV) Requester Module
- NASA Foreign National Escort Training Module
- Access Manager 3.0 Application Center Administration
- Foreign National Access Management (FNAM) International Visit Coordinator (IVC) Training Module
 - NOTE: This is available through the FNAM Website (<https://www.hq.nasa.gov/office/ops/nasaonly/internal/FNAM/index.html>).

9.2 ICAM Portal

The ICAM Portal is located at <https://icam.nasa.gov>. See Section 3 for more details.

9.3 Other Information

The ICAM InsideNASA page provides high level information about ICAM: <https://inside.nasa.gov/ocio/infrastructure/icam.html>.

9.4 Requesting Changes to ICAM Services

Anyone at NASA may submit Service Requests (SRs) for ICAM services.

ICAM services use the NASA Integrated Service Management System (NISM) to register and manage SRs. Anyone can submit an SR in NISM via the ICAM Portal or one can follow the direct link that is listed below:

<https://nism.ndc.nasa.gov/arsys/forms/mcsitsm.ndc.nasa.gov/SRS%3AServiceRequestConsole/Default+Administrator+View/?cacheid=edac3f29>

There are three basic types of SRs:

- Break/Fix
- Master Data
- Change Request

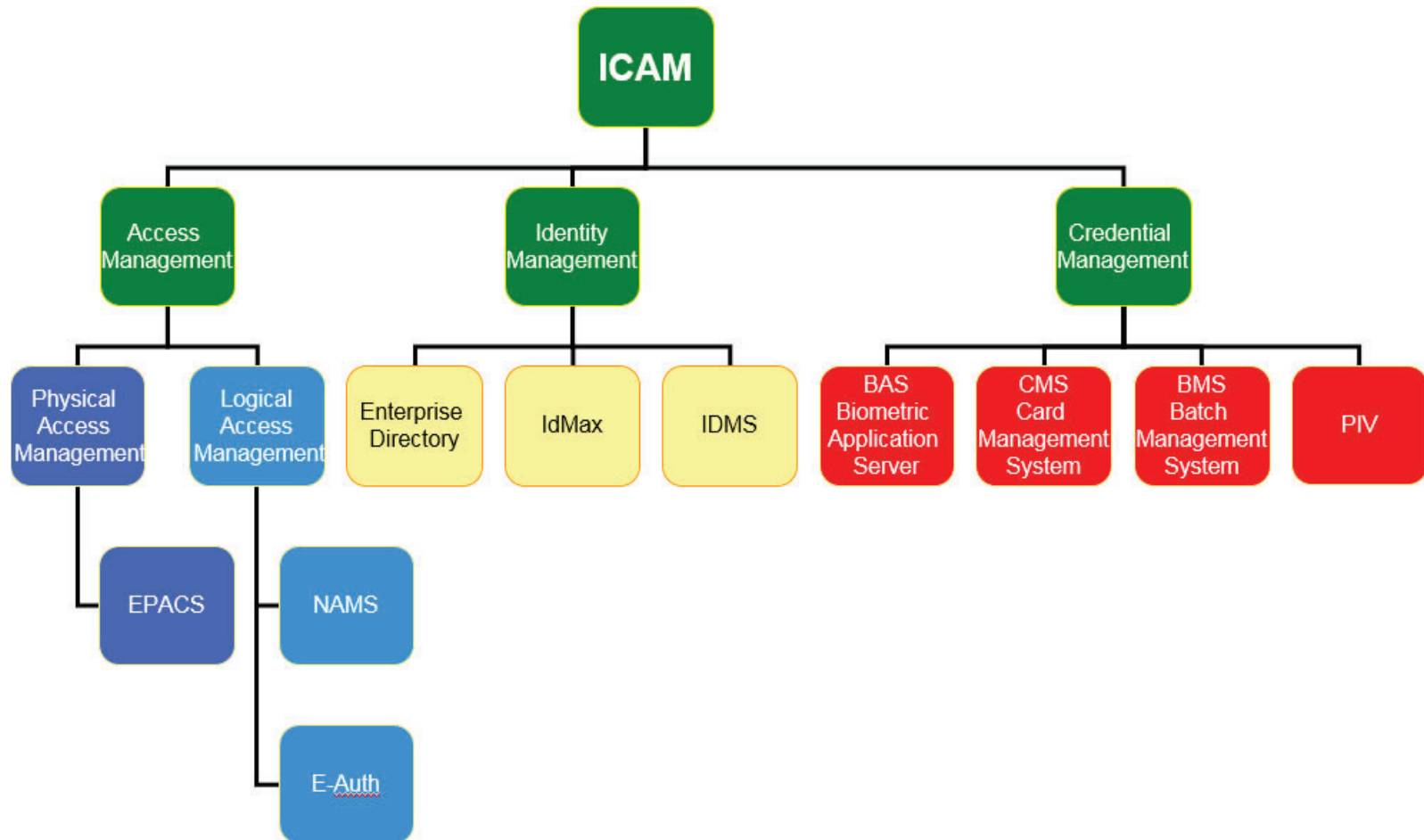
A Break/Fix request is submitted when an ICAM service is not working properly and requires immediate repair. Break/Fix SRs are addressed by the ICAM Service Providers directly and typically follow stringent service level agreements (SLAs).

A Master Data request is submitted when someone requires a change to data in the ICAM systems that cannot be self-serviced. Master Data SRs are also addressed by the ICAM Service Providers directly.

A Change Request is submitted when someone requires a change or enhancement to an ICAM Service. Change Requests are reviewed and approved by the appropriate governing body, depending on size, complexity, and impact to other ICAM and non-ICAM services. Once approved by the appropriate governing body, they are prioritized and then scheduled for implementation.

Small enhancements that are in scope of ICAM and fall within ICAM's cost allocation are prioritized by the assigned ICAM SME(s), and approved by the Program Executive in OCIO and/or OPS. Change requests that impact systems outside of ICAM, that are out of the current scope of ICAM, or have significant cost impacts, may need to be approved by other governing bodies. The specific governing bodies will change based on the type and impact of the change requested.

Appendix A: ICAM Services Framework



Appendix B: Mapping of LOR, LOC, and LOA

https://icam.nasa.gov/documents/-/document_library/AeRnBATjmPZn/view_file/6521494

Appendix C: Acronyms

A&A	Authentication and Authorization
AA	Administrative Account
AAL	Authentication Assurance Level
AART	Agency Application Rationalization Tool
AD	Active Directory
AMA	Authentication Mechanism Assurance
AO	Authorizing Official
ASB	Agency Smart Badge
BLE	Basic Level of Entitlement
CA	Certificate Authority
CAC	Common Access Card
CASIS	Center for the Advancement of Science in Space
CIMA	Center for Internal Mobile Applications
CIO	Chief Information Officer
CISO	[Center] Chief Information Security Officer
CRL	Certificate Revocation List
CSET	Cybersecurity Standards and Engineering Team
CSP	Credential Service Provider
CSPD	Cybersecurity and Privacy Division
DoD	Department of Defense
EAR	Export Administration Regulation
EO	Executive Order
EPACS	Enterprise Physical Access Control System
ESD	Enterprise Service Desk

FABLE	Federated Authentication with Basic Levels of Entitlement
FAIA	Federated Authentication with Internal Authorization
FAL	Federation Assurance Level
FBCA	Federal Bridge Certification Authority
FIC	Federated Identity Credential
FICAM	Federal Identity, Credential, and Access Management
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FNAM	Foreign National Access Management
FPKIPA	Federal PKI Policy Authority
FSL	Facility Security Level
GSA	General Services Administration
HBK	Handbook
HSPD	Homeland Security Presidential Directive
IAL	Identity Assurance Level
ICAM	Identity, Credential, and Access Management
ICSP	Identity and Credential Service Providers
iD	Identity Self Service
IdMAX	Identity Management and Account eXchange
IdP	Identity Provider
IPSec	Internet Protocol Security
ISO	Information System Owner
ISSO	Information System Security Officer
IT	Information Technology
ITAR	International Traffic in Arms Regulations
ITS	Information Technology Security
IVC	International Visit Coordinator
LDAPS	Secure Lightweight Directory Access Protocol

LOA	Level of Assurance
LOC	Level of Confidence
LOR	Level of Risk
LOT	Level of Trust
NAMS	NASA Account Management System
NASA	National Aeronautics and Space Administration
NCAD	NASA Consolidated Active Directory
NDC	NASA Data Center
NED	NASA Enterprise Directory
NICA	NASA Internal Certificate Authority
NISM	NASA Integrated Service Management System
NIST	National Institute of Standards and Technology
NOAA	National Oceanographic and Atmospheric Administration
NOCA	NASA Operational Certificate Authority
NOMAD	NASA Operational Messaging and Directory Service
NPD	NASA Policy Directive
NPE	Non-Person Entity
NPR	NASA Procedural Requirement
NPrivAMS	NASA Privileged Access Management System
NSTIC	National Strategy for Trusted Identities in Cyberspace
NTAM	NASA Trust Anchor Management
NVMS	NASA Visitor Management System
OCIO	Office of the Chief Information Officer
OCSP	Online Certificate Status Protocol
OHCM	Office of Human Capital Management
OID	Operational Identifier
OMB	Office of Management and Budget
OP	Office of Procurement

OPM	Office of Personnel Management
OPS	Office of Protective Services
PACS	Physical Access Control Systems
PACS	Physical Access Control Systems
PAM	Physical Access Management
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIV	Personal Identity Verification
PIV-I	PIV Interoperable
PKI	Public Key Infrastructure
POA&M	Plan of Action and Milestones
RBD	Risk-Based Decision
RISCS	Risk Information Security Compliance System
SAML	Security Assertion Markup Language
SATERN	System for Administration, Training, and Educational Resources for NASA
SBU	Sensitive But Unclassified
SC	Security Categorization
SCEP	Simple Certificate Enrollment Protocol
SLA	Service Level Agreement
SME	Subject Matter Expert
SOAP	Simple Object Access Protocol
SOC	Security Operations Center
SOP	Standard Operating Procedure
SP	Special Publication
SR	Service Request
SSP	System Security Plan
TADS	Time and Attendance Distribution System
TFPAP	Trust Framework Provider Adoption Process

TFS	Trust Framework Solutions
TFTI	Two-Factor Token Infrastructure
TLS	Transport Layer Security
UBE	User-Based Enforcement
URL	Uniform Resource Locator
UUPIC	Universal Uniform Personal Identification Code
VPN	Virtual Private Network
WCT	Workflow Configuration Tool
WTTS	Workforce Transformation Tracking System

Appendix D: Glossary

NASA Workers	• Federal employees / civil servants • Contractors • Detailed employees • Others performing work for NASA (volunteers, guest researchers, seasonal employees)
Non-workers	• Members of the public utilizing NASA resources for their benefit (e.g., USAJOBS, IRS, PTO) • Foreign partners performing non-NASA work • Visitors • Tenants • Grantees performing non-NASA work
NASA Persons	NASA Workers and non-workers