

Enterprise Architecture Standard

Standard for Integrating Applications into the NASA Access Management, Authentication, and Authorization Infrastructure

EA-STD-0001

Version Date: July 30, 2008
Effective Date: August 1, 2008
Expiration Date: August 1, 2011
Responsible Office: OCIO, Chief Information Officer

Revision Record

ITEM NO.	REVISION	DESCRIPTION	DATE
1	V.1.0	Initial Version	7/30/2008

Table of Contents

Revision Record	ii
Table of Contents	iii
Table of Figures	iv
Table of Tables	iv
1. Introduction	1
1.1. Purpose	1
1.2. Scope	1
1.2.1. Definition of an Application	1
1.3. Supplemental Information	2
2. Requirements	3
2.1. NASA Account Management System (NAMS) Integration	3
2.2. Authentication and Authorization Integration	3
2.3. Authentication Credentials	3
2.4. Directory Lookup Integration	3
2.5. Commercial Off-the-Shelf (COTS) Software	3
2.6. Application Registry	3
2.7. Requirements for New and Existing Applications	4
2.8. Deviations	4
3. Identity and Access Management Infrastructure	5
3.1. Identity Management and Account eXchange (IdMAX) System	6
3.1.1. Identity Management System (IDMS)	6
3.1.2. Identity Management Workflows	6
3.1.3. NASA Account Management System (NAMS) Workflows	6
3.2. NASA Agency Forest (NAF)	6
3.3. eAuthentication	7
3.4. NASA Public Key Infrastructure	9
3.5. NASA Enterprise Directory	10
3.6. Desktop Components	11
3.7. RSA SecurID Token Infrastructure	11
4. Application Integration Decision Tree	12
5. NAMS Integration	14
5.1. NAMS Workflows	14
5.2. NAMS Provisioning	14
5.3. Reconciliation	15
5.4. Migration of User Authorization Data into NAMS	16

5.4.1.	Ensure Identities of Existing Users are in IdMAX	16
5.4.2.	Determine User Authorization Data Migration Method	17
6.	Authentication and Authorization Integration.....	19
6.1.	Authentication Integration.....	20
6.1.1.	Authentication Sources.....	20
6.1.2.	Authentication Credentials.....	22
6.1.3.	Selection of Authentication Sources and Credentials.....	22
6.2.	Authorization Integration	25
6.2.1.	NASA Identifiers	25
7.	Agency User ID (AUID).....	25
7.2.	Basic Levels of Entitlement (BLEs)	26
8.	Directory Lookup Integration	27
8.1.	Worker Lookup Migration (x.500 to NASA Enterprise Directory).....	27
Appendix A.	Acronyms.....	29
Appendix B.	Reference Documents	31
Approval.....		32

Table of Figures

Figure 1: Identity and Access Management.....	5
Figure 2: NAF Design	7
Figure 3: eAuthentication Design.....	8
Figure 4: PKI Design.....	9
Figure 5: NASA Enterprise Directory Design	10
Figure 6: Application Decision Tree (New Applications)	12
Figure 7: Application Decision Tree (Existing Applications).....	13
Figure 8: IT Remote User Workflow	16
Figure 9: Logical Access Control Framework	19

Table of Tables

Table 1: Authentication Sources	20
Table 2: Authentication Credentials	22
Table 3: NASA Enterprise Directory/x.500 Attribute Mapping.....	27

1. Introduction

1.1. Purpose

This document defines the standard for integrating NASA applications into the NASA infrastructure for access management, authentication, and authorization. Federal requirements set forth by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST) fundamentally change the way NASA vets identities and grants access to NASA physical and logical assets. The reference documents listed in Appendix B provide a derived requirement for a central architecture for logical access management and control as part of the overall NASA Enterprise Architecture. The purpose of this document is to provide guidance to application owners and developers on how to integrate their applications into NASA's infrastructure so that they comply with Federal mandates.

1.2. Scope

This document addresses application integration with NASA's access management, authentication, and authorization infrastructure for mission-related, general-purpose, research, administrative and scientific computing and networking throughout the NASA Agency. It is applicable to all NASA administrative offices, programs, projects, NASA centers and remote sites.

1.2.1. Definition of an Application

An application is defined as any server-based software running in the NASA environment that is not included as part of the standard desktop/laptop load. For the purposes of application integration, a NASA application is defined as follows:

- It is recognized that NASA owns, funds, or maintains, jointly owns or has right of first refusal or information is critical to the mission or operation of NASA
- The application provides user-based authentication today. Usually the method of authentication is a userID and password.

Authentication is the mechanism that IT systems use to securely identify users. Authentication answers the questions: Who is the user? Is the user really who he/she claims to be?

Authorization is the mechanism by which a system determines what level of access a particular authenticated user should have to specific system resources. Authorization answers the question: Should this user be allowed to access this resource?

Authentication will occur at the lowest point of authorization:

- Each application that authorizes a subset of accounts to an external authentication source will be a discrete entry.
- A suite of applications is considered a single application if multiple applications:

- Authenticate to a single authentication source, and all users authenticated to that source have rights to the full set of applications.
- Reside on a single computer, and the OS-based access to that computer provides access to all applications resident on that computer ONLY.
- Reside behind a single physical barrier, and access through that physical barrier provides access to all applications.

1.3. Supplemental Information

This standard provides the high-level requirements and guidance for application integration. Supplemental information about how to integrate into different components of the NASA infrastructure will be provided in the IT Authentication and Authorization Infrastructure website at:

<http://insidenasa.nasa.gov/ocio/infrastructure/AA.html>

2. Requirements

Detailed requirements for application integration are provided in a series of policy documents published by NASA, the Office of Management and Budget (OMB), and the National Institute of Standards and Technology (NIST), and other Federal Agencies. References to the pertinent documents are listed in Appendix B. This section briefly describes the high-level, NASA-specific application integration requirements.

2.1. NASA Account Management System (NAMS) Integration

All applications shall use NAMS for account management, including creation, modification, and deletion of accounts. NAMS integration is discussed in Section 5.

2.2. Authentication and Authorization Integration

All applications shall utilize NASA-approved central sources for application authentication and authorization. Authentication and Authorization Sources are discussed in Section 6.

2.3. Authentication Credentials

All applications shall meet NASA Authentication Credential requirements. Authentication credential requirements are discussed in Section 6.1.2.

2.4. Directory Lookup Integration

All applications that perform directory lookups of NASA worker information shall utilize the NASA Enterprise Directory. Directory lookup integration is discussed in Section 8.

2.5. Commercial Off-the-Shelf (COTS) Software

COTS software that is purchased to meet NASA's application requirements shall be integrated with the NASA Authentication and Authorization Architecture. Therefore, all future COTS products purchased shall support integration with a directory-based authentication source, such as Active Directory.

2.6. Application Registry

All applications shall be registered in the NASA Application Tracking Tool (NATT). Applications shall be registered as soon as they begin the application development lifecycle.

NATT is available at:

<https://www7.jsc.nasa.gov/natt/>

2.7. Requirements for New and Existing Applications

All new applications must meet the requirements in Sections 2.1 through 2.6 as part of the development lifecycle.

All existing applications must meet the requirements in Sections 2.1 through 2.6 in accordance to the NASA schedule submitted to OMB:

- | | |
|---|--------------------|
| • RSA/VPN Accounts integrated into NAMS | September 30, 2008 |
| • High Impact Applications | |
| ○ Integrated into NAMS | June 30, 2009 |
| ○ HSPD-12 compliant authentication | June 30, 2009 |
| • FIPS 199 Moderate Risk Applications | |
| ○ Integrated into NAMS | September 30, 2009 |
| ○ HSPD-12 compliant authentication | September 30, 2010 |
| • FIPS 199 Low Risk Applications | |
| ○ Integrated into NAMS | September 30, 2010 |
| ○ HSPD-12 compliant authentication | September 30, 2011 |

High Impact Applications are defined as:

- FIPS 199 High Risk Applications
- Applications Containing Personally Identifiable Information (PII)
- Virtual Private Network (VPN) Infrastructure

2.8. Deviations

Requests for deviation from any of the requirements above shall be submitted in accordance with EA-STD-0004, *Procedures for Submitting an Application Integration Deviation Request and Transition Plan*. Deviations will be approved by the NASA CIO on a case-by-case basis.

3. Identity and Access Management Infrastructure

NASA has established an Agency-wide infrastructure to support Identity and Access Management. (Figure 1) There are three major components that work together to provide workers access to NASA applications:

- **Identity Management** supports the lifecycle management of NASA workers' identity data, including identity creation, vetting through Security, changes in identity status and disablement. A NASA worker is defined as someone who has a working relationship with NASA.
- **Credential Management** supports the lifecycle management of NASA credentials issued to workers, including badges and PKI certificates. Credential creation, re-issuance, and revocation and examples of lifecycle management activities in Credential Management.
- **Access Management** supports the lifecycle management of access to systems and applications, including account requests and approval, authentication, and authorization.

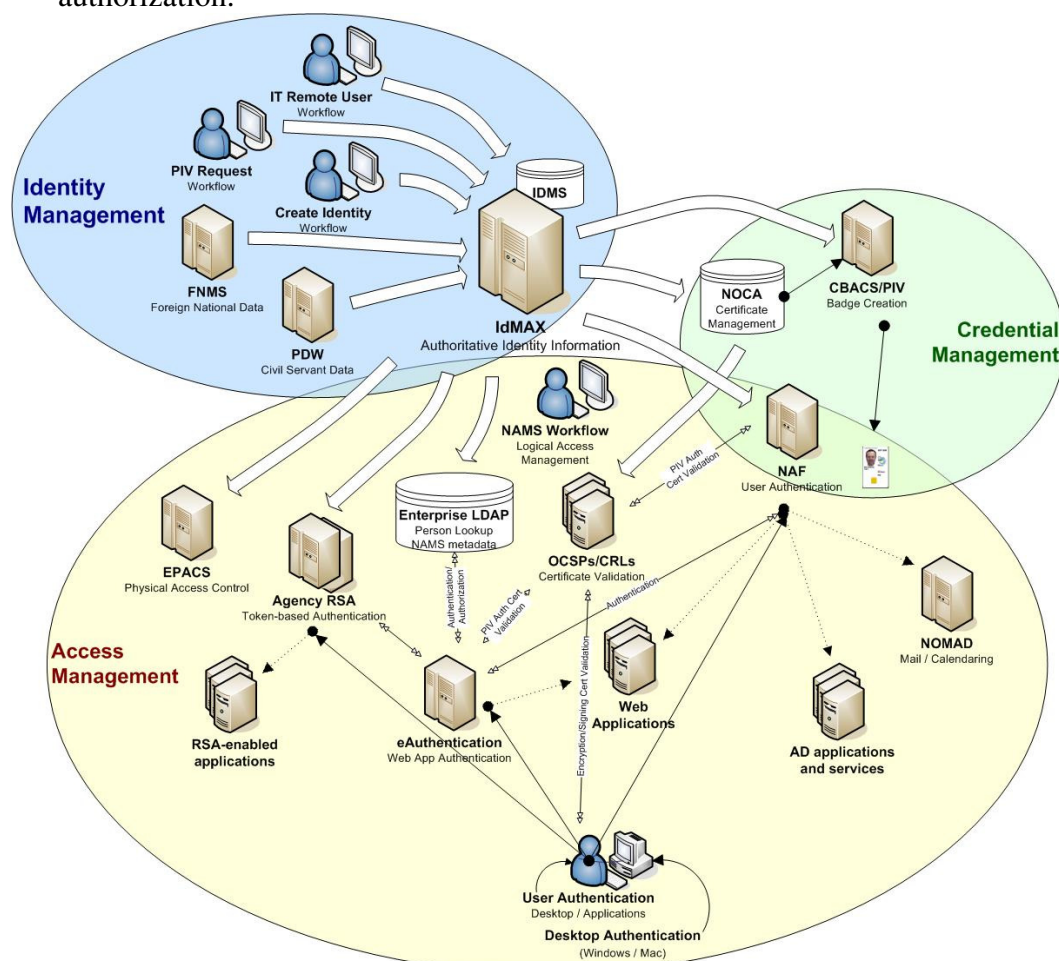


Figure 1: Identity and Access Management

The sections below briefly describe the infrastructure available to application owners and developers for application integration.

3.1. Identity Management and Account eXchange (IdMAX) System

IdMAX is a gateway for accessing multiple tools that are used for badging, IT access, and updating personal information in NASA's public information directories. IdMAX provides Identity and Access Management for NASA through a series of workflows and interfaces with authoritative data sources. The main components of IdMAX are described below.

3.1.1. Identity Management System (IDMS)

IDMS is the authoritative source for all workers. A worker is defined as a person who has a business relationship with NASA. Interfaces with IDMS provide identity information from other authoritative sources. Civil Servant data is fed from the Personnel Data Warehouse (PDW), the authoritative distribution source for NASA civil servant data. Foreign National data is fed from the NASA Foreign National Management System (NFMMS), the authoritative source for Foreign National data. All other worker data is entered into IDMS using the Identity Management workflows contained within IdMAX. All workers who access NASA physical or logical assets must be registered in IDMS.

3.1.2. Identity Management Workflows

Identity Management workflows allow for the creation, modification, and disablement of identities for all NASA workers who are not NASA civil servants or Foreign Nationals. Identity Management workflows also support the badging process and the identity vetting process for IT remote users. The IT Remote User workflow is discussed in more detail in Section 5.4.1.

3.1.3. NASA Account Management System (NAMS) Workflows

NAMS workflows support the creation, modification, and deletion of accounts for all NASA systems and applications. NPR 2810.1A mandates the use of NAMS for all accounts assigned to workers in order to access NASA systems and applications. Integration into NAMS for new and existing applications is discussed in Section 5 of this document.

3.2. NASA Agency Forest (NAF)

The NASA Agency Forest (NAF) will provide Active Directory authentication and authorization services across NASA. NAF accounts will be maintained using NAMS.

NASA Centers will migrate Center Active Directory domains to the NAF according to the NASA Consolidation of Active Directory (NCAD) migration schedule. Migration will begin in FY 2008 and complete in FY 2009. The NAF will provide userid/password and smartcard

authentication to all NASA Windows and Macintosh (Mac) desktops, as well as to applications and other resources that can integrate into Active Directory. The NAF will also provide Kerberos-based authentication service to eAuthentication and the NASA Enterprise Directory in future releases.

Figure 2 provides a high-level diagram of the centralized and distributed components of the NAF.

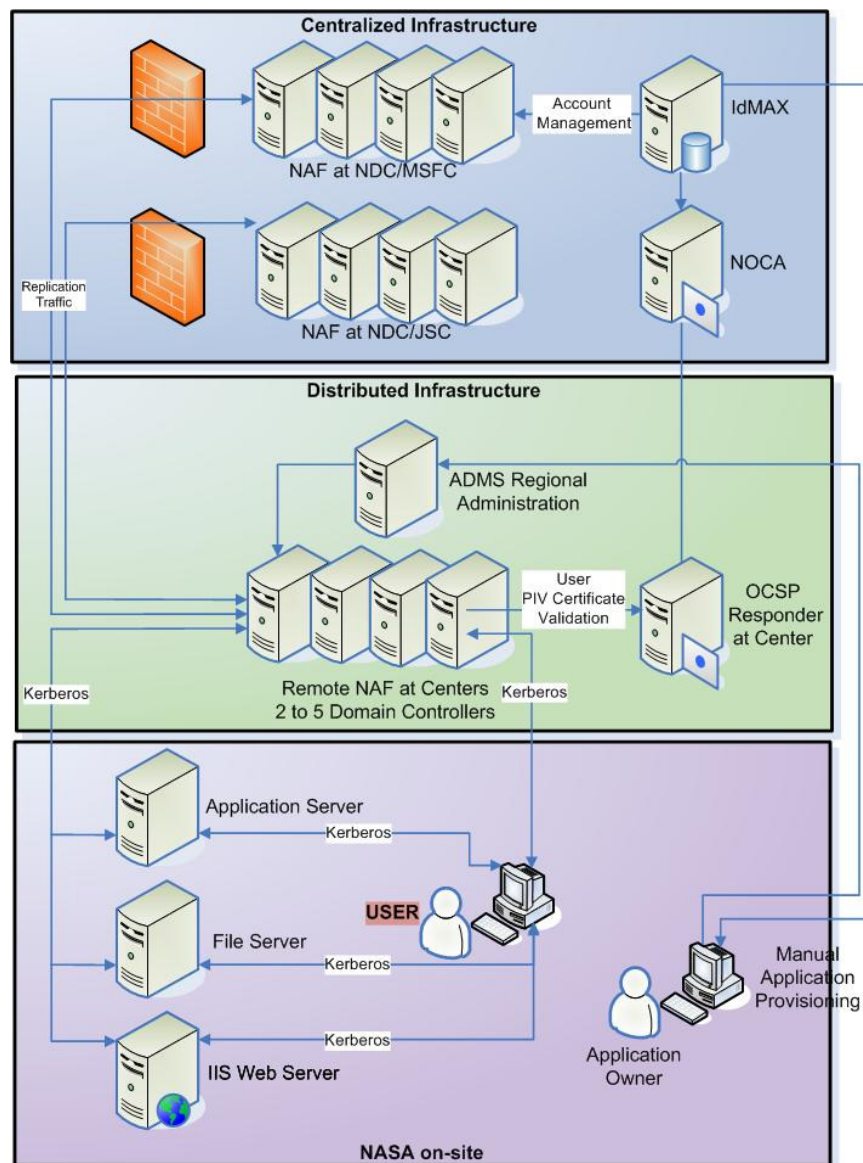


Figure 2: NAF Design

3.3. eAuthentication

The eAuthentication infrastructure provides a centralized authentication interface for NASA's web-based applications. The eAuthentication infrastructure is built using the Sun Java System

Access Manager product. The primary role of Sun Access Manager is web access management. This includes but is not limited to authentication, authorization, identity federation, single sign-on, and web services security.

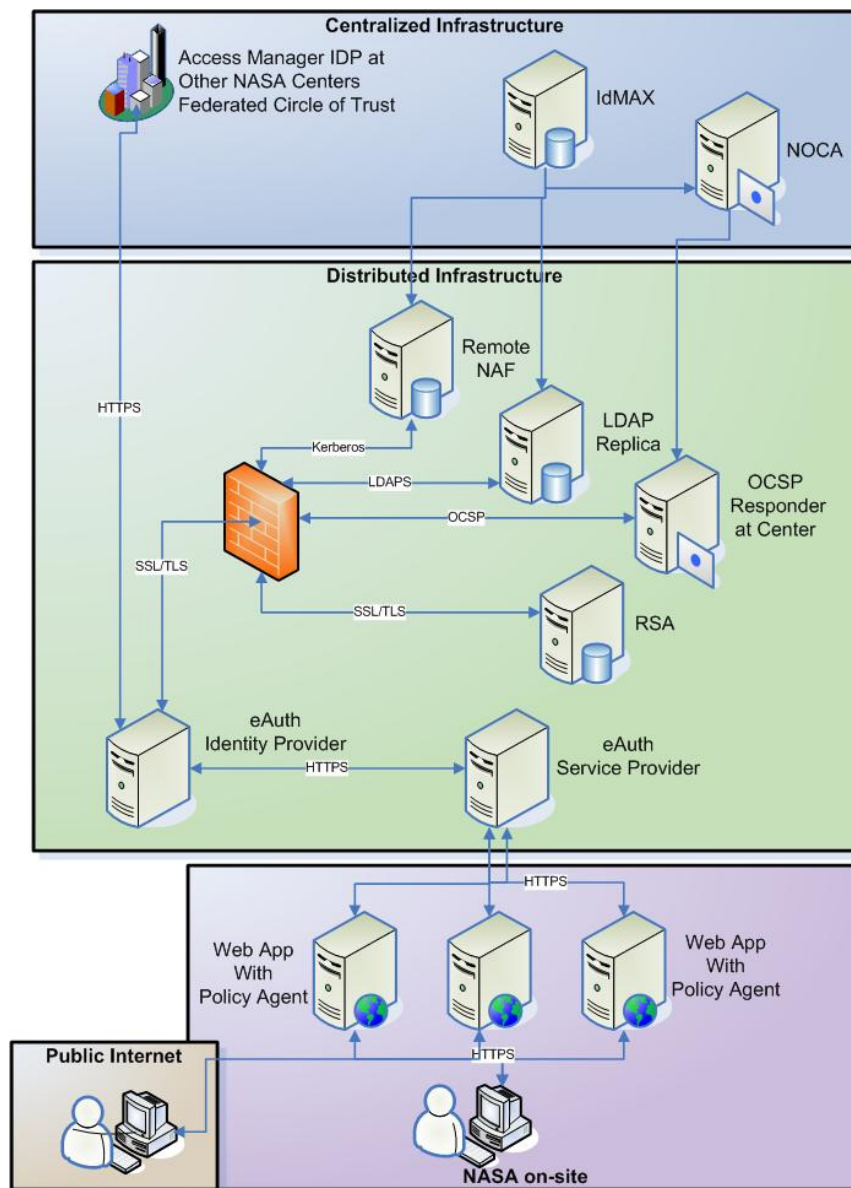


Figure 3: eAuthentication Design

The eAuthentication architecture framework is comprised of three major components:

- **The Access Manager** – This Java-based application serves as a Policy Decision Point (PDP). The Access Manager is responsible for making decisions for such tasks as user authentication and user authorization.
- **Identity Directories** – These repositories are responsible for storing all identity data which allows the Access Manager application to make decisions. The data may exist in

the same physical location as the Access Manager or it may be distributed across one or many different user identity stores. The ability to perform checks across many identity repositories is a key piece of functionality included with Sun Access Manager.

- **The Web/Application Layer Policy Agent** – The Policy Agent serves as the Policy Enforcement Point (PEP). The Policy Agent is responsible for checking with and enforcing the Sun Access Manager Policy Decisions for authentication and authorization decisions.

The eAuthentication implementation of the Access Manager integrates with Identity Directories that are integrated with IdMAX, and allow for the use of multiple credentials including userID and password, smartcard and PIN, and RSA token and PIN. The eAuthentication Access Managers will be distributed among the NASA Centers to provide centrally managed and locally distributed authentication points for web based applications.

3.4. NASA Public Key Infrastructure

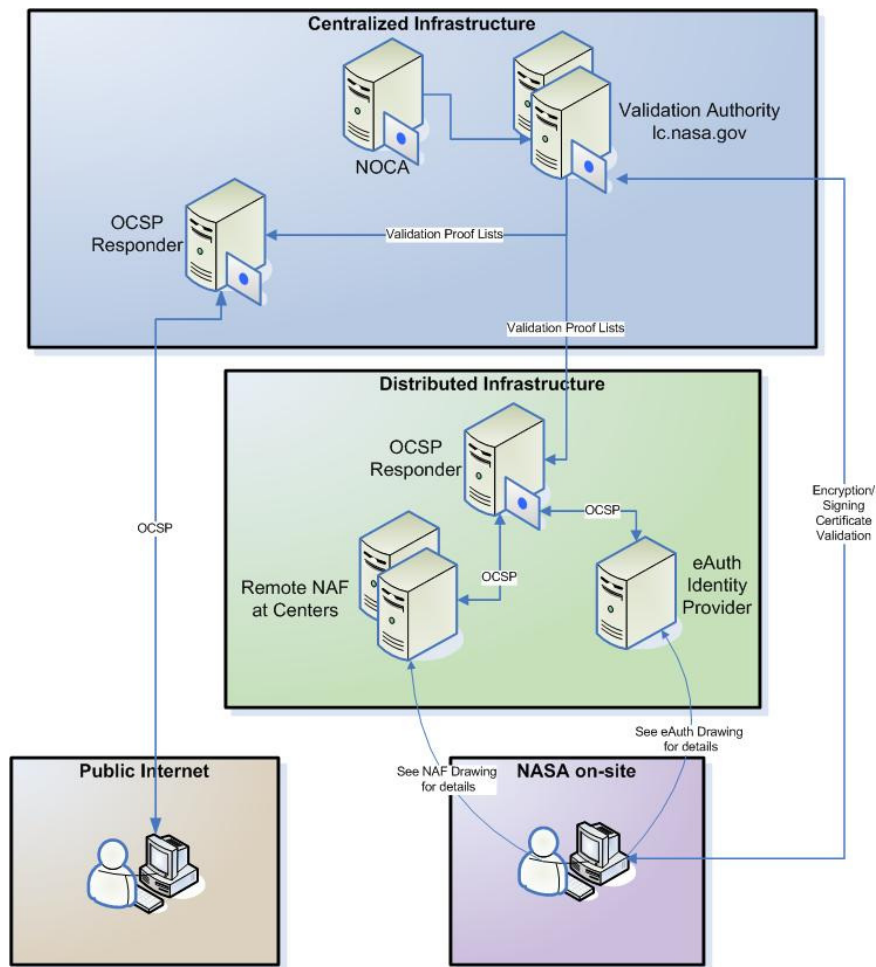


Figure 4: PKI Design

Public Key Infrastructure (PKI) provides certificate issuance and validation of certificates for authentication, signature, and encryption. The NASA Operational Certificate Authority (NOCA) provides for issuance of PKI certificates in accordance with the Federal Common Policy and HSPD-12 requirements. The NASA PKI provides a series of Certificate Revocation Lists (CRLs) and Online Certificate Status Protocol (OCSP) responders to provide continuous validation that the PKI certificates presented are valid, not expired, and not revoked.

PKI certificate validation will occur through the NAF and eAuthentication when these authentication sources are smartcard-enabled. Therefore, intimate knowledge of PKI is not required of application owners in order to enable smartcard authentication for applications. Smartcard enablement of an application directly, rather than through a central authentication source, is not allowed except by deviation.

3.5. NASA Enterprise Directory

The NASA Enterprise Directory is the online phone and information directory for all workers. Identity data is provided by IdMAX. The NASA Enterprise Directory replaces legacy x.500 systems that were managed by each NASA center.

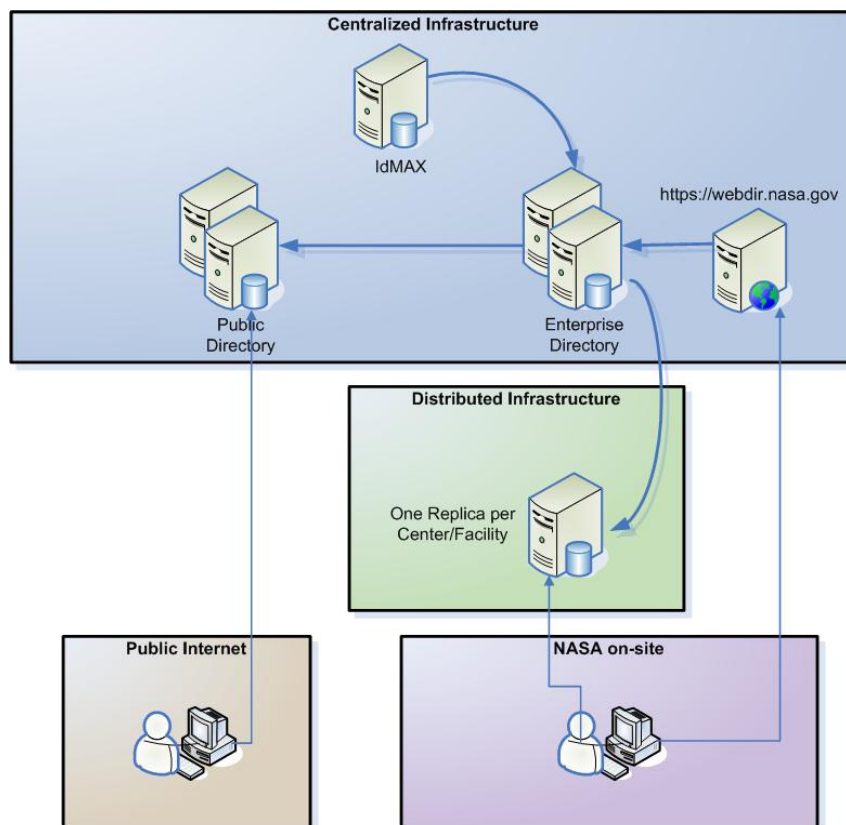


Figure 5: NASA Enterprise Directory Design

The NASA Enterprise Directory also contains application authorization data from NAMS workflows. This data is accessed by eAuthentication for authorization to integrated applications.

Two directory servers co-residing in the NASA Data Center (NDC) at Marshall Space Flight Center (MSFC) serve as masters (suppliers). Two master directory servers with replication agreements to the NDC masters are deployed at Johnson Space Center (JSC) to support disaster recovery.

Replica directory servers deployed throughout the agency support authentication and authorization services provided through eAuthentication.

3.6. Desktop Components

NASA desktops require additional components in order to utilize smartcards. Those components are:

- Smartcard reader
- Middleware

The NASA standard middleware is ActivIdentity ActiveClient. The Agency has a site license for the ActivClient software suite. ActivClient distribution is scheduled to coincide with NCAD migration.

NASA-STD-2804 and NASA-STD-2805 have been updated to incorporate new Desktop Standards to meet requirements for smartcard enablement.

3.7. RSA SecurID Token Infrastructure

NASA is establishing an Agency-wide RSA infrastructure to meet the needs of applications and systems for which the use of smartcards is not feasible. Until the Agency infrastructure is implemented, use of Center RSA token infrastructures that have been integrated into NAMS and use the Agency User ID (See Section 7) can be considered. Use of SecurID tokens in lieu of smartcards is a deviation that must be approved by the Agency CIO.

4. Application Integration Decision Tree

The application integration decision trees for new and existing applications establish the steps required to meet Agency integration requirements. The basic tenets of the Decision Tree are these:

First, the identities of all workers with application accounts shall be captured in IdMAX. Most identities are captured in IdMAX through the badging process. IdMAX contains workflows for IT Remote users, which are described in Section 5.4.1.

Second, all applications shall be integrated into NAMS for account management. NAMS integration assures a tie between the account established in the application and a vetted identity. NAMS also facilitates on-going account maintenance to assure that account access is granted only to those individuals who require it, and removed when access is no longer required.

Third, all applications shall be integrated into central authentication and authorization sources. The two primary means of authentication integration are through the NAF and through eAuthentication. Other methods of authentication should only be considered if the NAF or eAuthentication cannot be employed. Where alternate methods of compliance are employed, application owners must request a deviation.

Finally, applications shall perform any directory lookups against the NASA Enterprise Directory.

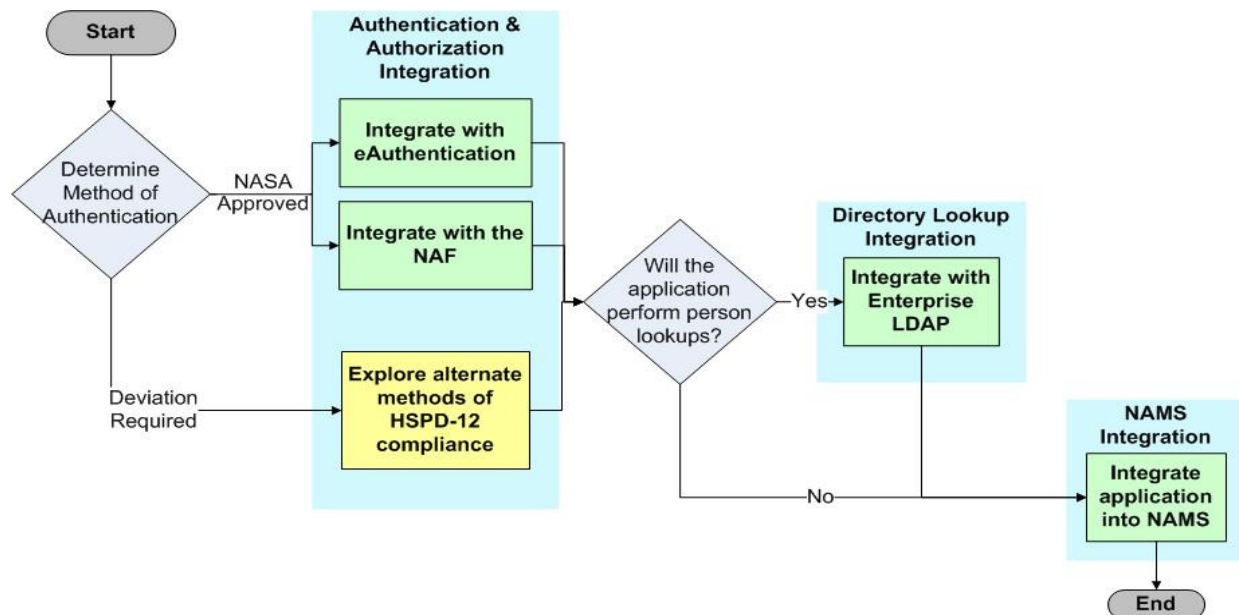


Figure 6: Application Decision Tree (New Applications)

For new applications (Figure 6), integration with central authentication and authorization sources and the NASA Enterprise Directory should occur during the development process. Test environments for eAuthentication and the NASA Enterprise Directory are available if needed. NAMS integration shall occur before the application becomes operational, and all initial and subsequent accounts to the new application shall be approved and provisioned using NAMS.

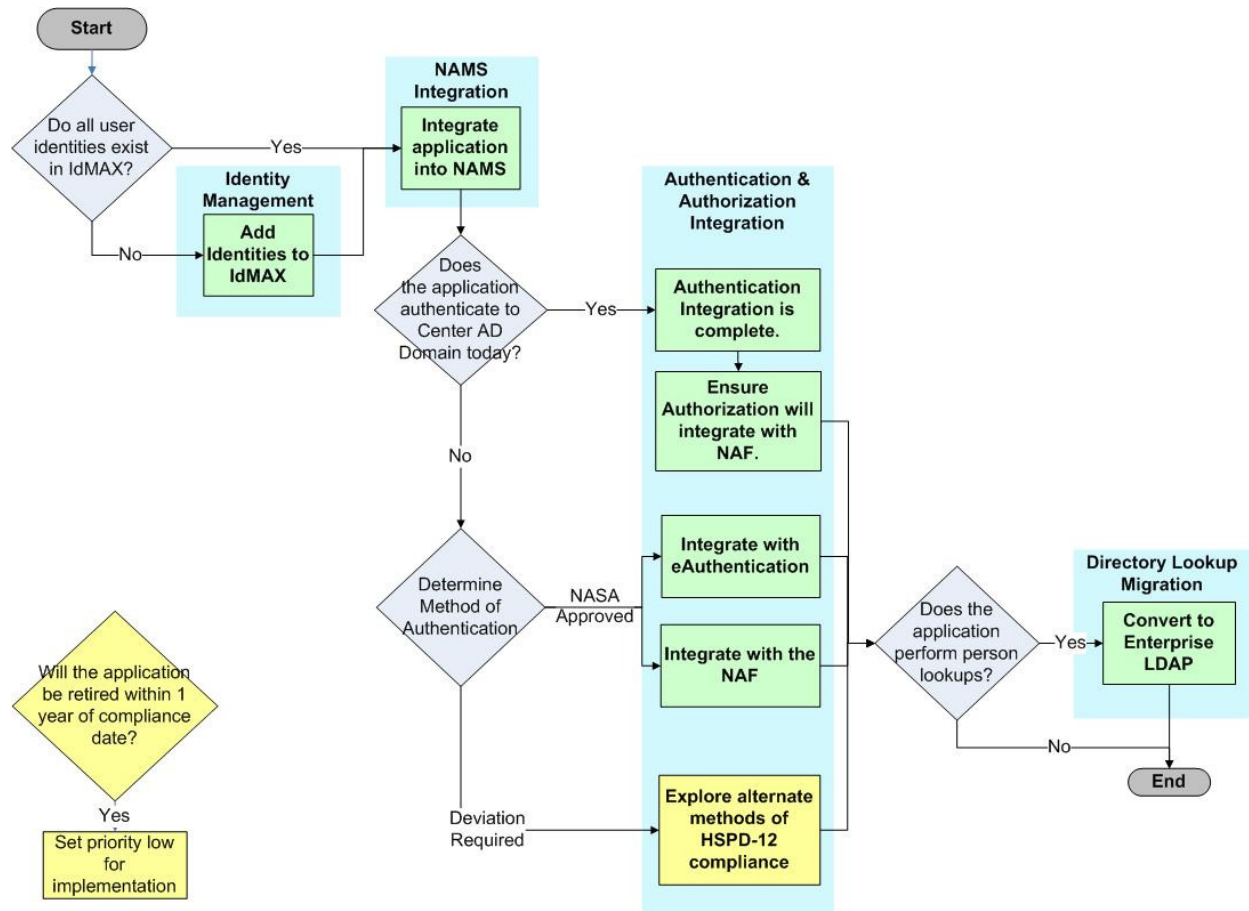


Figure 7: Application Decision Tree (Existing Applications)

For existing applications (Figure 7), NAMS integration should occur before integration with other components of the infrastructure. A key activity of NAMS integration for existing applications is ensuring that any remote users of the application have identities captured in IdMAX. This activity is described in more detail in Section 5.4.1. NAMS integration is a prerequisite for eAuthentication integration, and supports NAF integration.

5. NAMS Integration

The **NASA Account Management System (NAMS)** is an online service used to request access to NASA applications. Ultimately, NAMS will completely replace the paper process for requesting access to NASA IT systems.

Per NPR 2810.1A, all NASA applications must manage accounts through NAMS. Detailed NAMS documentation is available on the Authentication and Authorization website referenced in Section 1.3.

5.1. NAMS Workflows

NAMS manages account request, approval, and provisioning through workflows. A workflow is simply an automated business process.

The Agency has established a generic workflow that meets most application owners' needs for account management. Given the burden of workflow development and maintenance, it is **highly recommended** that application owners request a custom workflow only after a thorough analysis of the capabilities of the generic workflow. A deviation request must be submitted and approved before a NAMS Custom workflow may be used.

5.2. NAMS Provisioning

Once an account is approved, it can be provisioned in the application. There are two major methods of Provisioning: Manual and Automatic.

When Manual Provisioning is utilized, an e-mail is sent to the provisioner(s) once the final approval is granted. The Provisioner is expected to manually add, modify, or delete the account in accordance with the approved request, and then record in NAMS that the account was provisioned.

Manual provisioning poses less risk to the application; however, reconciliation is more labor-intensive under manual provisioning.

When Automatic Provisioning is utilized, a Resource Adapter is developed between NAMS and the application. Once the final approval for an account is granted, the account is automatically added, modified, or deleted. The Resource Adapter records the action taken in NAMS for reporting and audit purposes.

Given the burden of Resource Adapter development, it is **highly recommended** that application owners select Automatic Provisioning only for select Agency-wide applications.

5.3. Reconciliation

The application owner shall reconcile all accounts recorded in NAMS with the accounts on the application source. During reconciliation, mis-matches between the account list in NAMS and the account list in the application must be analyzed and dispositioned so that NAMS accurately reflects approved access to the application. Reconciliation shall be conducted on an annual basis.

5.4. Migration of User Authorization Data into NAMS

Owners of new applications will begin establishing accounts in NAMS once their application is operational, and therefore will not need to migrate user authorization data as part of NAMS integration.

Owners of existing applications must first ensure that all identities of existing users are captured in IdMAX, and then determine the best method for the migration of user authorization data.

5.4.1. Ensure Identities of Existing Users are in IdMAX

Identities for all permanent, NASA-badged workers are captured in IdMAX as part of the badging process.

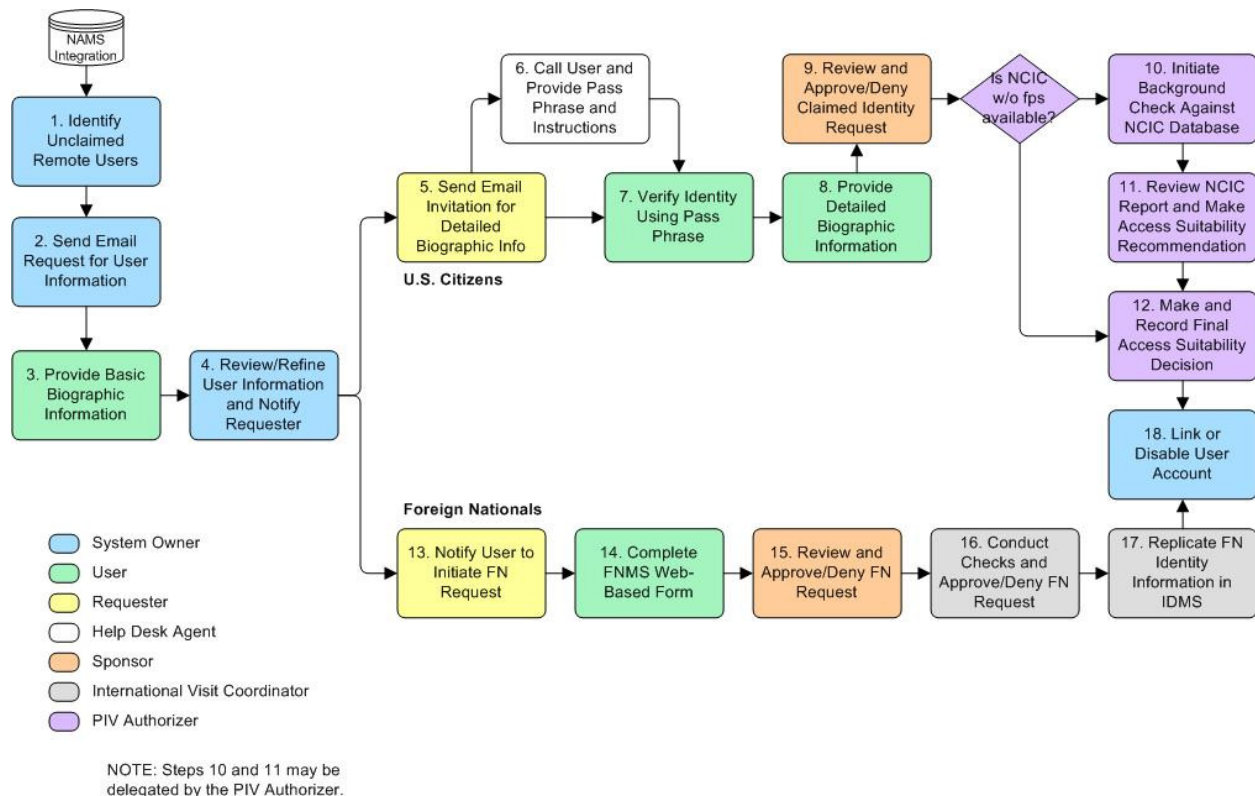


Figure 8: IT Remote User Workflow

Identities for IT Remote Users must also exist in IdMAX to allow for account management through NAMS and for central authentication. IT Remote Users are often discovered during the process of NAMS user migration. The IT Remote User workflow (Figure 8) explains the responsibilities of the System Owner in the IT Remote User Identity Management process.

5.4.2. Determine User Authorization Data Migration Method

Owners of existing applications have several options for establishing the baseline accounts that NAMS will manage for the application after migration. The options are described below.

Bulk Migration

When an existing application is integrated into NAMS, application owners may elect to migrate existing users in bulk into NAMS to establish the baseline set of accounts that will be managed.

Bulk migration is a good option to select when:

- The user base is well-known
- The likelihood of inactive accounts in the application is low

When this method is selected, the application owner must associate the Universal Uniform Personal Identification Code (UUPIC) (See Section 6.2.1.1) of the person who owns the account with the account name used in the application. UUPICs can be found in the NASA Enterprise Directory and at <https://webdir.nasa.gov/dir/index.html>. A UUPIC association tool is available in NATT which allows bulk UUPIC associations. Additionally, some centers have developed UUPIC association tools based on center locator systems.

No Migration

Application Owners may elect not to migrate user accounts into NAMS, and instead have all current users re-apply through NAMS for account access. Choosing not to migrate user accounts is a good option when:

- There are only a few accounts
- There is a likelihood of many inactive accounts in the application
- There is high risk to allowing non-managed identities to have account access

When this method is selected, application owners should inform current application users to apply through NAMS for accounts to the application during a specific period of time. After that time period has ended, the application owner shall perform a baseline reconciliation of application accounts against NAMS, and remove any accounts not established in NAMS.

NCAD/NAF Migration

Since NASA is migrating to the NASA Agency Forest (NAF), and all NAF user accounts are associated with managed identities with assigned UUPICs, NCAD migration is an option for some application owners. This method is a good option when:

- The application uses Active Directory for authentication and authorization

- The access control lists (ACLs) in Active Directory are current
- The application integration compliance deadline occurs after Center NCAD migration

When this method is selected, the application owner waits for the center desktop migration to the NAF for all users of the application to be complete. At this point, the application owner shall retrieve the user account list from the NAF, and provide it to NAMS to establish the baseline user accounts.

6. Authentication and Authorization Integration

NASA is providing the infrastructure discussed in Section 5 to support central authentication and authorization. Multiple authentication sources and credentials are being provided in order to meet the diverse needs of NASA. Application owners shall determine which components of the infrastructure can be used by their application to meet Federal and Agency requirements.

The Logical Access Control framework illustrates the components of authentication and authorization. Requirements for logical access control are grouped according to framework elements.

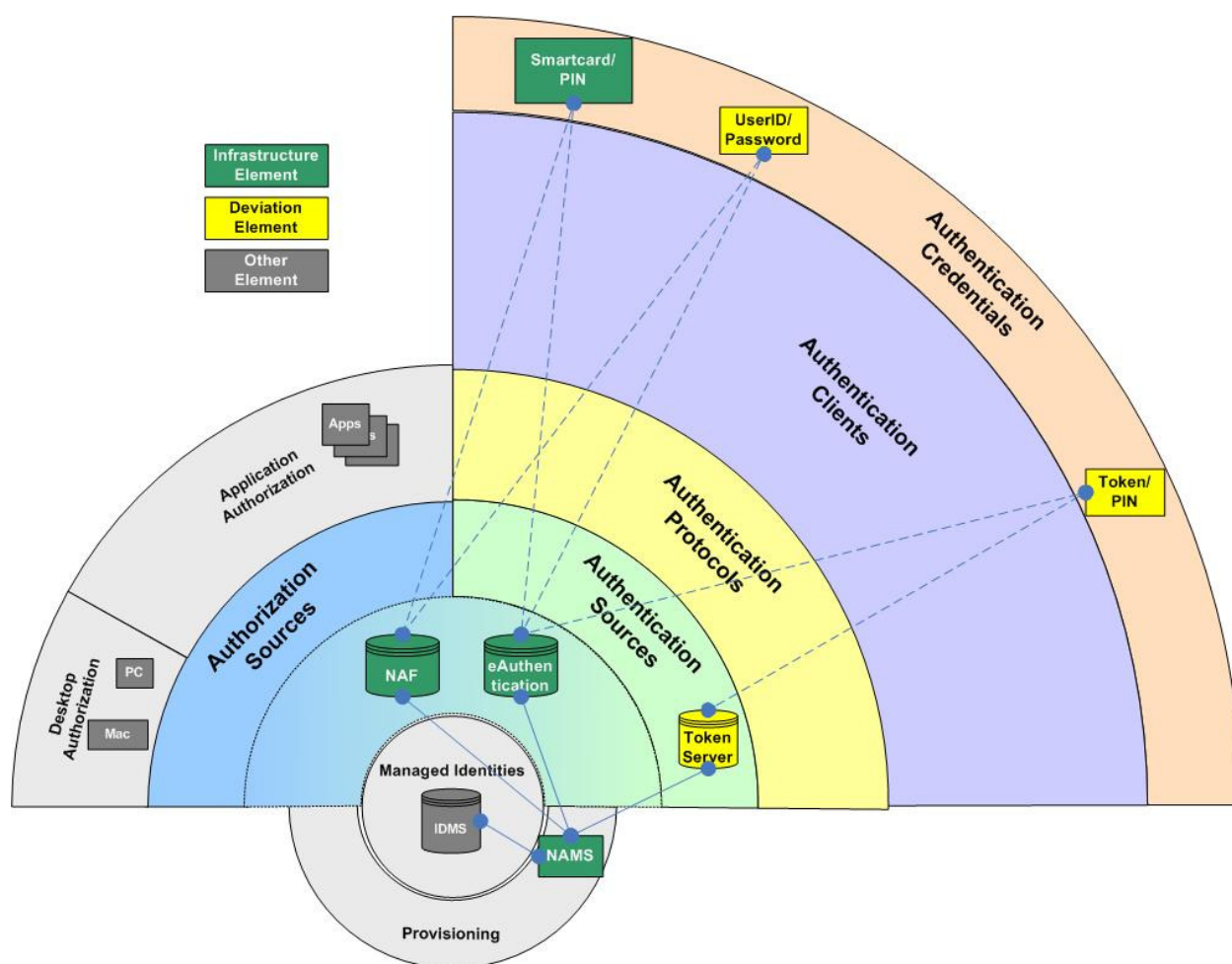


Figure 9: Logical Access Control Framework

The agency is providing central authentication sources that support three credential types (smartcard/PIN, UserID/Password, and Token/PIN) as depicted in Figure 9. (For simplicity, other components in the framework are not displayed.)

Application owners must select the appropriate Authentication and Authorization sources, and the Authentication credential that meets Federal and Agency requirements. Selection of particular tools and services will be influenced by several factors discussed in Section 6.1.3.

6.1. Authentication Integration

Applications shall be integrated into a central authentication source utilizing smartcard authentication unless a deviation request has been submitted and approved.

6.1.1. Authentication Sources

Central authentication sources validate the authentication credential presented by the user, and allow access to an authorization source. The following authentication sources are approved for NASA use and will support the following authentication credentials:

Authentication Sources	Supported Credentials		
	Userid/ Password	RSA Token/ PIN	Smartcard/ PIN
NAF	With Deviation	No	Yes
eAuthentication	With Deviation	With Deviation	Yes
RSA/Radius (Deviation)	With Deviation	With Deviation	No

Table 1: Authentication Sources

6.1.1.1. Integration with the NAF

Integration with the NAF requires the use of Kerberos-based authentication to Active Directory. LDAP-based authentication to the NAF does not meet Authentication Requirements for persistence and avoidance of Man-in-the-Middle attacks.

If authentication integration occurs prior to Center migration to the NAF, application owners shall migrate application authentication to their Center's AD Domain. During NCAD migration, the userIDs and ACLs will be migrated, maintaining access to the application. If a local user table is utilized for role-based access, care should be taken to ensure that potential changes from a Center UserID to the AUID do not remove access that should be allowed.

The NASA Agency Forest (NAF) will be smartcard-enabled. Center desktop migration to the NAF must be completed before an AD-aware application can utilize smartcard authentication.

6.1.1.2. Integration with eAuthentication

Integration with eAuthentication requires the installation of a Policy Agent on the application's web container. Application Owners shall complete an eAuthentication Questionnaire to begin the process of eAuthentication integration.

eAuthentication will be smartcard-enabled in FY2008. Applications that are integrated into eAuthentication can smartcard-enable their applications as soon as their users have the desktop components necessary to support smartcard use. The schedule for desktop component installation is tied to the NCAD migration schedule.

6.1.1.3. Authentication Deviations

Deviations are required for any application that is not integrated with an approved authentication source and smartcard-enabled. For applications that cannot be smartcard-enabled using the NAF or eAuthentication, the following deviation solutions should be considered:

Integration with RSA SecurID Tokens

NASA is developing an Agency RSA infrastructure for applications that cannot be smartcard-enabled but require two-factor authentication. Prior to implementation of the Agency RSA infrastructure, existing RSA infrastructures that have been integrated into NAMS are acceptable for two-factor enablement. RSA Tokens may be a good alternative when the user base extends beyond NASA workers with smartcards.

Placement Behind a Smartcard-enabled Enforcement Point

Some applications that cannot easily be two-factor enabled may be able to use an external enforcement point to meet authentication requirements. This method can be used if the application owner can ensure that access to the application can only occur through the enforcement point employed.

An eAuthentication-enabled web server can serve as an enforcement point. Network appliances are available on the market which can integrate with the NAF or eAuthentication. These appliances can be configured to require particular authentication credentials such as a smartcard or RSA token in order to grant access.

A smartcard-enabled physical access point, such as an electronic door reader on a facility, can also serve as a smartcard-enabled enforcement point, if the application is only accessible by those who enter the smartcard-enabled physical access point. Isolated labs and networks are examples of systems that may house applications that cannot be smartcard-enabled at the application layer, but can be protected by a smartcard-enabled physical access point.

Smartcard-Enablement of the Application Itself

In rare cases, smartcard-enablement of the application itself may be an acceptable deviation. Smartcard-enabling an application is complex, and the overall cost and risk to the Agency is very high. It is for this reason that the Agency is providing central authentication sources for

application integration. Application owners should ensure that direct integration is the only possible approach for meeting authentication requirements.

6.1.2. Authentication Credentials

Authentication Credentials are presented by the user to verify identity and gain access to a particular resource. The credential is usually a combination of two or more elements, such as a userid and password, or a smartcard and personal identification number (PIN).

OMB Memo M-05-24 requires that smartcards be used for access to all on-site systems by all permanent, on-site employees.

Systems that are accessed from a non-Federally controlled facility are governed by NIST SP 800-63 and OMB Memo M-04-04. NPR 1600.1 provides Security Vetting requirements for different types of NASA workers.

Table 2 overlays the guidance provided in OMB Memo M-05-24 with NIST guidance provided in SP 800-63:

NIST 800-63 Authentication Credential Requirements with M-05-24 Overlay					
Accessed From	Application Type	Minimum Acceptable Credentials	Identity Check		
			Self proclaimed identity	Identity Validation	Security Vetting
Non-Federally controlled facility	Public	None or Anonymous UserID/Password	Acceptable	Acceptable	Acceptable
	FIPS Low	UserID/Password		Required	Acceptable
	FIPS Moderate	Two-factor, such as: RSA Token Smartcard			Required
	FIPS High	Hard Crypto token, such as: Smartcard			Required
Federally controlled facility	Any Application	Smartcard			Required

Table 2: Authentication Credentials

6.1.3. Selection of Authentication Sources and Credentials

Several factors will influence the selection of the appropriate Authentication Source and credentials that meet Federal and Agency Requirements:

6.1.3.1. FIPS Categorization

Applications inherit the FIPS 199 category assigned to its governing system as part of the IT Security Planning process. This categorization is a major factor to consider in determining

appropriate methods of authentication and authorization. FIPS categories drive the assurance levels required for authentication credentials. Federal Information Processing Standards (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, is the standard used by federal agencies to categorize all information and information systems according to a range of risk levels.

The FIPS 199 category assigned to an IT security plan represents the overall risk of the entire system. It is possible for an application within a particular system to have a lower overall risk than the system. In general, however, applications should be considered to belong to the same FIPS risk category as the overall IT system, and should employ the same security controls, including those for authentication.

Assurance levels have been established as part of the e-Authentication initiative, detailed in OMB Memo M-04-04 and NIST SP 800-63, and presented in Table 2. Application owners must select an authentication credential that meets the Assurance Level required based on their applications FIPS 199 Risk category and Sensitivity of Data.

6.1.3.2. Sensitivity of Data or Information Types

Information is categorized according to its information type. NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, provides information type identification and security categorization guidelines. An information type is a specific category of information such as privacy, proprietary, or financial information. In some instances, a specific law or regulation governs the collection and maintenance of a particular information type. The sensitivity of the data or information type processed by applications is important in determining the appropriate authentication mechanisms for that system and should be considered by application owners.

6.1.3.3. Credentials Issued to User Communities

Appropriate authentication methods are dependent on which credentials can be issued to the user community accessing the application. Application owners should strive to implement the strongest authentication credential available to all of the application's users.

NASA Smartcard-Badged workers

All workers who access NASA facilities for longer than 180 days will receive a smartcard. NASA will issue the smartcard unless the worker is a federal employee at another Agency. NASA badged workers are also able to receive RSA tokens and to activate accounts for eAuthentication and the NAF.

External Partners or Remote Users

User communities that include external partners or remote users who are not issued Federal smartcards can obtain accounts with eAuthentication. Accounts with the NAF can also be obtained; however, there may be limitations to their use outside of NASA networks. Where two-factor authentication is required, RSA tokens can be issued to external partners and remote users of NASA applications.

Transient Users

For applications that are accessible by users who are “transient in nature” and only rely on identity information claimed by the user, a one-factor method of authentication, such as userid/password, is sufficient to meet authentication requirements. Only applications with public information available to the general public can rely on a claimed identity only. eAuthentication can provide userID/password credentials based on claimed identity only.

6.1.3.4. Geographical Location of User Communities

The geographical location of users while accessing NASA applications will also influence which authentication methods are feasible.

Access from NASA Networks

Any application that is accessed solely by NASA badged workers while on-site at a NASA center or facility are required to provide smartcard-based authentication to their application, unless another factor in Section 6.1.3 creates an impediment to smartcard use. This includes access through a Center VPN to a NASA Network.

Access from a non-NASA Network

User communities that access NASA resources from a non-NASA network may not be able to utilize NAF authentication. eAuthentication is generally the best option for access from a non-NASA network. Where two-factor authentication is required, smartcards and RSA tokens can be used with eAuthentication.

Access from a non-NASA computer

User communities who are not issued NASA computers in order to access NASA resources may not have the card reader and middleware necessary for smartcard authentication. Where two-factor authentication is required, RSA tokens can be used with eAuthentication.

6.1.3.5. SCADA Systems

Supervisory Control And Data Acquisition (SCADA) Systems have unique requirements which place them outside the scope of traditional authentication methods. NIST SP 800-82, *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security*, was written to address these unique requirements and provide systems security guidance. This publication should be consulted when considering integration of real-time systems such as power, water, and HVAC management, mission control, satellite data acquisition, and systems that perform testing functions.

6.2. Authorization Integration

The NAF and the NASA Enterprise Directory serve as central Authorization Sources for the Agency. Applications which authenticate using eAuthentication will use the NASA Enterprise Directory as a primary Authorization Source. Applications which authenticate to the NAF will also use the NAF as a primary Authorization Source. NAF-integrated applications can reference the NASA Enterprise Directory for additional authorization.

Authorization of a worker to a particular asset has historically been handled by the local application. It is expected that the architecture for fine-grained application authorization will not change in the near future. However, the Authentication source must be able to pass access rights to an authorization source using a unique identifier of the holder of the authenticated credential. When the authentication credential is successfully verified at the authentication source, a unique identifier may be passed to the application which allows it to use local user tables to grant authorization to specific functions of the application.

6.2.1. NASA Identifiers

NASA provides two identifiers that can be used to uniquely identify the worker and grant authorization to an asset.

6.2.1.1. Universal Uniform Personal Identification Code (UUPIC)

The UUPIC is a randomly assigned nine-digit number that is unique across NASA. A UUPIC is assigned when an identity is created in IdMAX. UUPICs never change, and cannot be re-used. Therefore, the UUPIC remains constant even when other attributes such as name, organizational affiliation, or citizenship change.

By policy, a UUPIC cannot be used for user logon and cannot be displayed on any user accessible application or web site without prior approval from the CBACS CCB. The UUPIC can only be used to positively identify individuals within and across information systems.

Application owners should add the UUPIC to their local user table to allow for fine-grained authorization within the application.

7. Agency User ID (AUID)

Each identity is also assigned an AUID at the time of identity creation. The AUID is also unique across NASA. The AUID is assigned based on an algorithm to associate closely to the person's name. The algorithm selects the first unique value found in this order:

- First Initial, Last Name (e.g. Jsmith)
- First Initial, Middle Initial, Last Name (e.g. JRSmith)
- First Initial, Middle Initial, Last Name, Unique Number (e.g. JRSmith1)

AUIDs are no longer than eight characters in order to support legacy applications that have an eight-character limit. The AUID forms the prefix of the user principal name (UPN) on NASA-issued smartcards.

AUIDs can change due to life events of the individual. Therefore, while AUIDs are used for one-factor login, AUIDs should not be used for system-to-system communication about an individual.

Deprecated userIDs should be converted to AUID as part of application migration wherever possible. Where this is not possible, legacy applications may be able to utilize the AUID for central authentication, and then pass the deprecated userID to the application.

New applications shall use AUID for login, and UUPIC for system-to-system communication.

7.1.1.1. User Principal Name (UPN)

The UPN is the identifier used on smartcards to enable authentication. All NASA-issued smartcards contain a UPN in the form AUID@ndc.nasa.gov. Agency Authentication sources will map the UPN from NASA- and other federal agency-issued smartcards to the account information used to grant access to applications.

7.2. Basic Levels of Entitlement (BLEs)

Basic Levels of Entitlement (BLEs) can be established for applications that are available to anyone who meets certain identity criteria that are managed through IdMAX. BLEs can be established for communities such as:

- All NASA Civil Servants
- All [Center] workers
- All US Persons

A workflow for registering BLEs in NAMS will be established so that accounts to these applications can be managed to the same degree that applications with explicit account application and approval are. Application owners must identify the criteria used to grant access, the approving official, and the reason for the BLE.

8. Directory Lookup Integration

The NASA Enterprise Directory is NASA's online phone and information directory. Over time, the NASA Enterprise Directory will replace X.500 systems.

All applications that perform lookups of worker information shall use the NASA Enterprise Directory to perform that function. Worker information includes attributes such as Name, Organization, Building, Room, and Phone Number.

8.1. Worker Lookup Migration (x.500 to NASA Enterprise Directory)

Applications that perform lookups against the NASA x.500 directory must migrate those lookups to the NASA Enterprise Directory. At the time of publication, a sunset date for the x.500 infrastructure had not been established. It is expected that the x.500 infrastructure will be retired within two years of publication of this standard.

The table below provides a mapping of x.500 attributes to the NASA Enterprise Directory attributes:

Table 3: NASA Enterprise Directory/x.500 Attribute Mapping

NASA Enterprise Directory		x.500		Comments
Attribute	(S)ingle or (M)ulti-valued	Attribute	(S)ingle or (M)ulti-valued	
Cn		cn	M	Common Name
Sn		Surname	M	Last name
givenName		n/a		First name
displayName	S	cn	M	displayName is used in the NOMAD GAL
x500UID	S	UniqueIdentifier	S	
Uid	M	n/a		Contains all uids including x500UID and agencyUID
agencyUID	S	n/a		
employeeNumber	S	n/a		employeeNumber = UUPIC
Street mailStop l St	S S S S	PostalAddress	S	I = City
postalCode	S	PostalCode	S	Zip Code
telephoneNumber		TelephoneNumber	M	
Mail	M	mail	M	e-mail addresses
nasaOrgCode	S	UserClass	S	
nasaEmployer	S			
facsimileTelephoneNumber		FacsimileTelephoneNumber	M	

NASA Enterprise Directory		x.500		Comments
Attribute	(S)ingle or (M)ulti- valued	Attribute	(S)ingle or (M)ulti- valued	
n/a		Title	S	
nasaBuilding roomNumber	S S	RoomNumber	S	
Street	S	StreetAddress	S	
n/a		userCertificate	S	

Appendix A. Acronyms

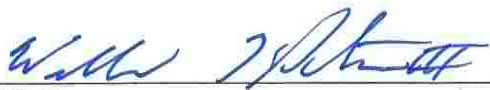
ACL	Access Control List
AD	Active Directory
ARC	Ames Research Center
AUID	Agency User ID
BLE	Basic Level of Entitlement
CBACS	Common Badging and Access Control System
CIO	Chief Information Officer
COTS	Commercial Off The Shelf
CRL	Certificate Revocation List
DFRC	Dryden Flight Research Center
FIPS	Federal Information Processing Standard
GRC	Glenn Research Center
GSFC	Goddard Space Flight Center
HQ	Headquarters
HSPD-12	Homeland Security Presidential Directive 12
HTTP	Hypertext Transfer Protocol
I&A	Identity and Authentication
ID	Identifier
IdMAX	Identity Management and Account eXchange System
IIS	Internet Information Server
IT	Information Technology
ITAR	International Traffic in Arms Regulations
IVV	Independent Verification and Validation Facility
JPL	Jet Propulsion Laboratory
JSC	Johnson Space Center
KSC	Kennedy Space Center
LDAP	Lightweight Directory Access Protocol
LDAP-S	LDAP over SSL
LARC	Langley Research Center
Mac	Macintosh Computer
MAF	Michoud Assembly Facility
MSFC	Marshall Space Flight Center
NAF	NASA Agency Forest
NAMS	NASA Account Management System
NASA	National Aeronautics and Space Administration
NATT	NASA Application Tracking Tool
NCAD	NASA Consolidated Active Directory
NDC	NASA Data Center
NISE	NASA Integrated Services Environment
NIST	National Institute of Standards and Technology
NIST SP	NIST Special Publication

NOCA	NASA Operational Certificate Authority
NOMAD	NASA Operational Messaging and Directory
NPR	NASA Procedural Requirement
NSPR	NASA Security Procedure Requirement
NSSC	NASA Shared Services Center
OCSF	Online Certificate Status Protocol
ODIN	Outsourcing Desktop Initiative for NASA
OMB	Office of Management and Budget
OS	Operating System
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
RSA	Remote Secure Access
SAML	Security Access Markup Language
SCADA	Supervisory Control And Data Acquisition
SSC	Stennis Space Center
SSL	Secure Socket Layer
SP	Special Publication
UserID	User Identifier
UUPIC	Universal Uniform Personal Identification Code
VPN	Virtual Private Network
WFF	Wallops Flight Facility
WSC&TF	White Sands Complex & Test Facility

Appendix B. Reference Documents

- EA-SOP-0004, Procedures for Submitting an Application Integration Deviation Request and Transition Plan
- FIPS 199, Standards for Security Categorization of Federal Information Systems
- FIPS 201-1, Personal Identity Verification (PIV) of Federal Employees and Contractors
- HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors
- NASA-STD-2804L, Minimum Interoperability Software Suite
- NASA-STD-2805L, Minimum Hardware Configurations
- NIST SP 800-63, Electronic Authentication Guideline
- NIST SP 800-53, Recommended Security Controls for Federal Information Systems
- NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories
- NPR 2810.1A, Security of Information Technology
- NPR 1600.1, NASA Security Program Procedural Requirements
- NSPR 1600-1, Universal Uniform Personal Identification Code (UUPIC) Policy
- OMB M-05-24, Implementation of HSPD 12
- OMB M-06-16, Protection of Sensitive Agency Information
- OMB M-04-04, E-Authentication Guidance for Federal Agencies
- ITS-SOP-0004, Procedures for Submitting an Application Integration Deviation Request and Transition Plan
- Federal Public Key Infrastructure Policy Authority, X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework, Version 3647 - 1.3

Approval



Willard F. Peters
NASA Enterprise Architect

8-5-08

Date