National Aeronautics and Space Administration

Identity, Credential, and Access Management at NASA, from Zachman to Attributes

Office of the Chief Information Officer

Corinne Irwin

Dennis Taylor

VISION: Integrated, secure, and efficient information technology and solutions that support NASA

Agenda

- Based upon a paper that Corinne Irwin and I presented at IDtrust 2009 in April 2009 (*Identity, Credential, and Access Management at NASA, from Zachman to Attributes*)
- EA View
- Active Directory consolidation—authentication source to enable smartcard authentication
- LoA Requirements

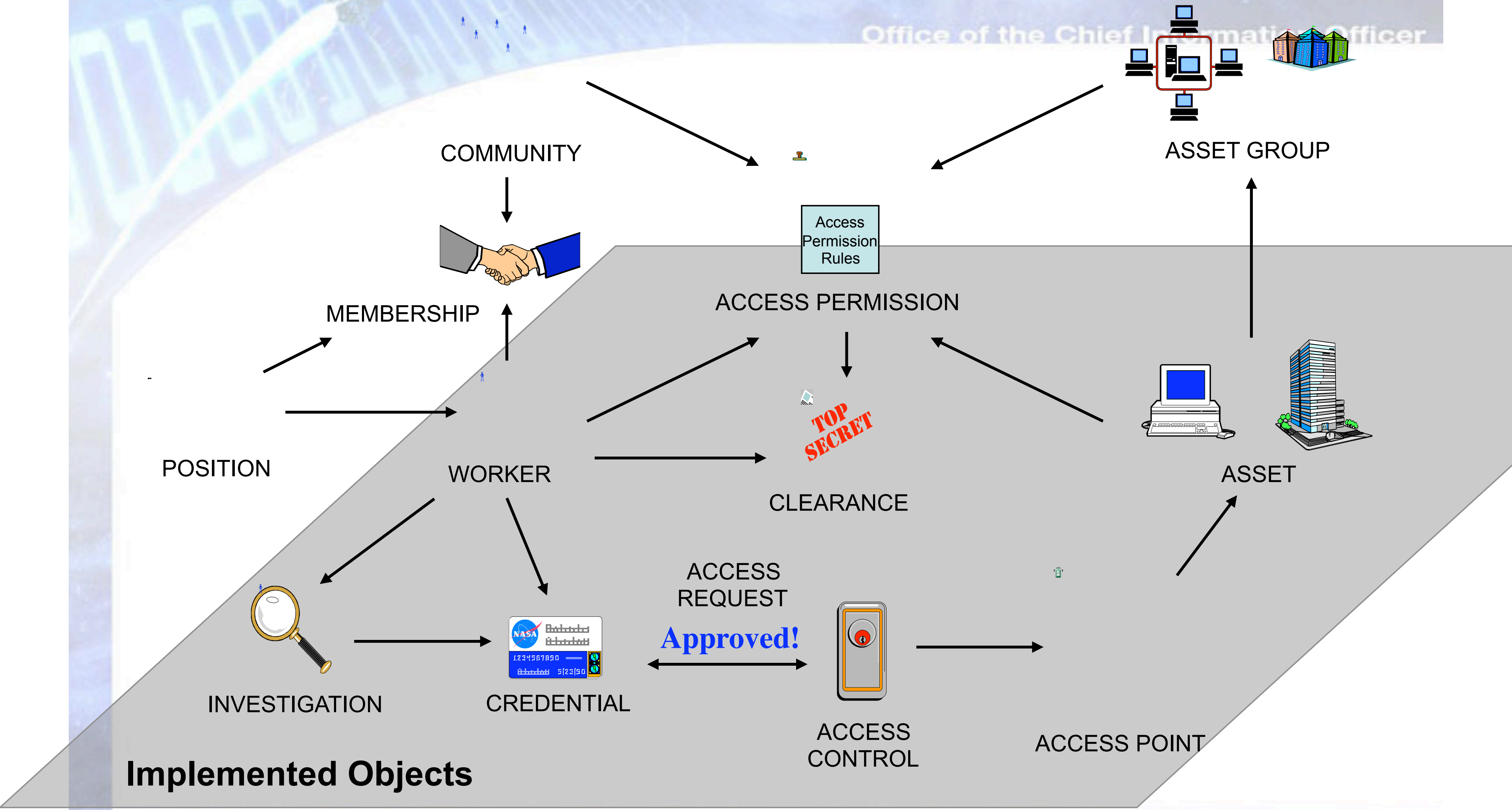
Introduction

- NASA includes:
  - 20,000 civil servant employees
  - 80,000 on-site contractors
  - Additional partners world-wide
- NASA's system/application landscape includes:
  - 3,000 applications, most built in-house
  - Mission control, research labs, product fabrication, more
  - Every flavor of every operating system, hardware, software….
- Historically, NASA has been:
  - Highly decentralized
  - Autonomous Centers with a B-to-B network infrastructure
  - Characterized by weak CIO governance
- HSPD-12 helped us:
  - Implement a robust Identity, Credential, and Access Management Architecture
  - Position NASA for use of ABAC and RBAC

Enterprise Architecture

- Enterprise Architecture (EA) frameworks provide structure for developing complex, integrated systems
- Ideally, one:
  - Develops an As-Is architecture
  - Develops a To-Be architecture
  - Performs gap analysis
  - Develops plan to move toward the To-Be architecture
- NASA used Zachman to develop its ICAM architecture starting in 2006

The Really Big Picture



COMMUNITY

ASSET GROUP

Access Permission Rules

ACCESS PERMISSION

MEMBERSHIP

POSITION

WORKER

CLEARANCE

ASSET

ACCESS REQUEST

Approved!

INVESTIGATION

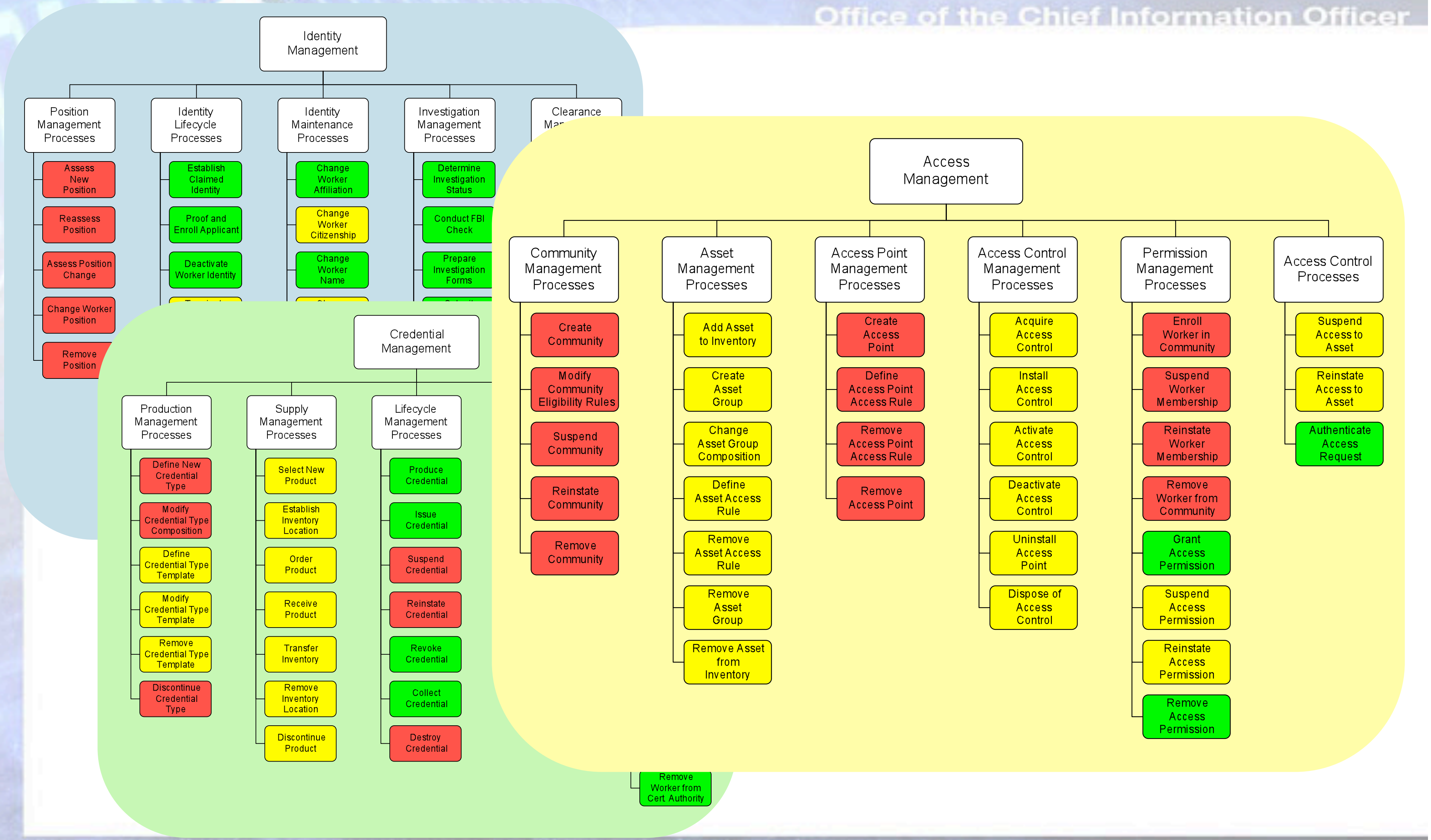
CREDENTIAL

ACCESS CONTROL

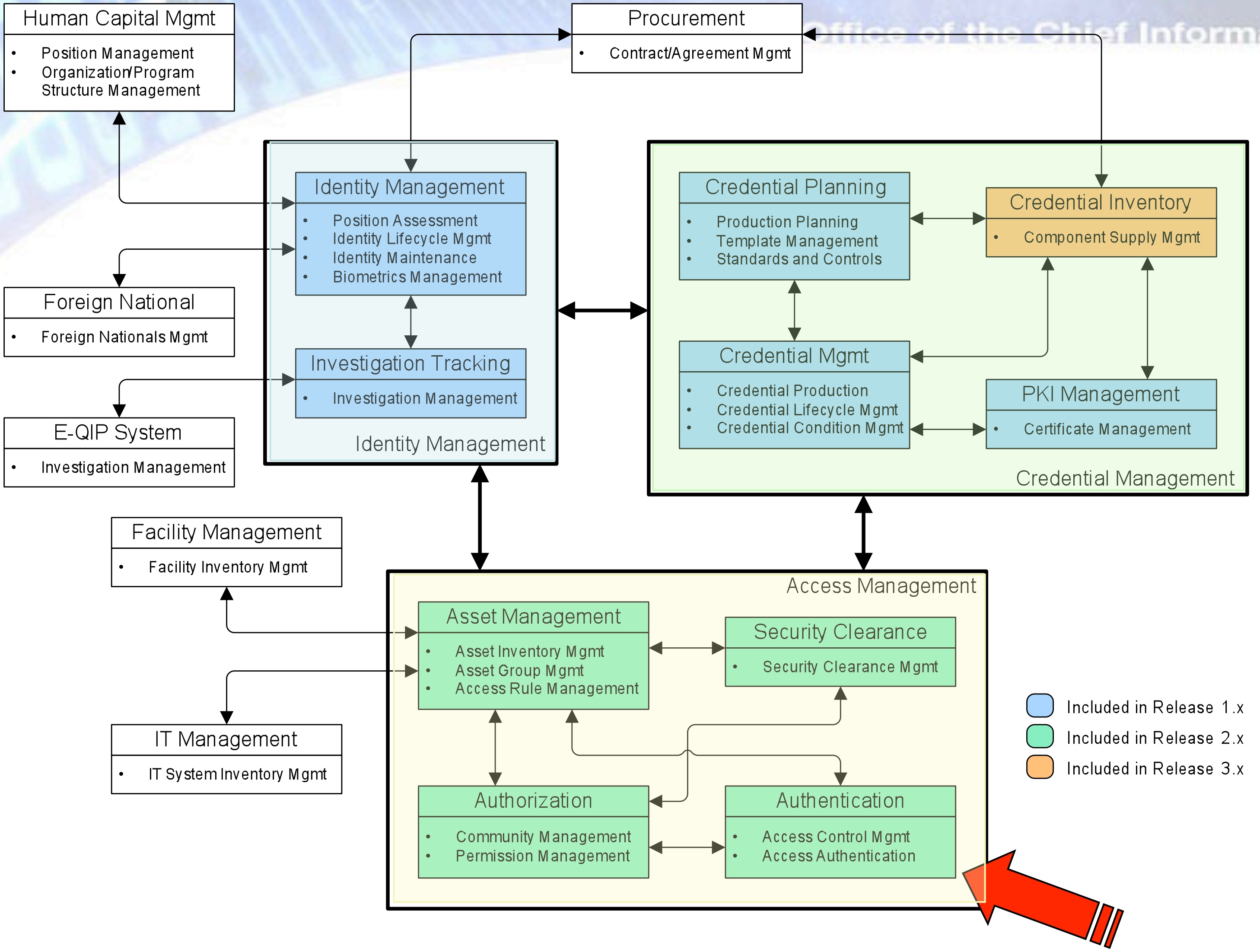
ACCESS POINT

Implemented Objects

ICAM Business Processes


Identity Management
Position Management Processes
Assess New Position
Reassess Position
Assess Position Change
Change Worker Position
Remove Position
Identity Lifecycle Processes
Establish Claimed Identity
Proof and Enroll Applicant
Deactivate Worker Identity
Identity Maintenance Processes
Change Worker Affiliation
Change Worker Citizenship
Change Worker Name
Investigation Management Processes
Determine Investigation Status
Conduct FBI Check
Prepare Investigation Forms
Clearance Man
Credential Management
Production Management Processes
Define New Credential Type
Modify Credential Type Composition
Define Credential Type Template
Modify Credential Type Template
Remove Credential Type Template
Discontinue Credential Type
Supply Management Processes
Select New Product
Establish Inventory Location
Order Product
Receive Product
Transfer Inventory
Remove Inventory Location
Discontinue Product
Lifecycle Management Processes
Produce Credential
Issue Credential
Suspend Credential
Reinstate Credential
Revoke Credential
Collect Credential
Destroy Credential
Remove Worker from Cert Authority
Access Management
Community Management Processes
Create Community
Modify Community Eligibility Rules
Suspend Community
Reinstate Community
Remove Community
Asset Management Processes
Add Asset to Inventory
Create Asset Group
Change Asset Group Composition
Define Asset Access Rule
Remove Asset Access Rule
Remove Asset Group
Remove Asset from Inventory
Access Point Management Processes
Create Access Point
Define Access Point Access Rule
Remove Access Point Access Rule
Remove Access Point
Access Control Management Processes
Acquire Access Control
Install Access Control
Activate Access Control
Deactivate Access Control
Uninstall Access Point
Dispose of Access Control
Permission Management Processes
Enroll Worker in Community
Suspend Worker Membership
Reinstate Worker Membership
Remove Worker from Community
Grant Access Permission
Suspend Access Permission
Reinstate Access Permission
Remove Access Permission
Access Control Processes
Suspend Access to Asset
Reinstate Access to Asset
Authenticate Access Request

ICAM Systems Model



Human Capital Mgmt
- Position Management
- Organization/Program Structure Management

Procurement
- Contract/Agreement Mgmt

Foreign National
- Foreign Nationals Mgmt

E-QIP System
- Investigation Management

Facility Management
- Facility Inventory Mgmt

IT Management
- IT System Inventory Mgmt

Identity Management

Identity Management
- Position Assessment
- Identity Lifecycle Mgmt
- Identity Maintenance
- Biometrics Management

Investigation Tracking
- Investigation Management

Credential Management

Credential Planning
- Production Planning
- Template Management
- Standards and Controls

Credential Inventory
- Component Supply Mgmt

Credential Mgmt
- Credential Production
- Credential Lifecycle Mgmt
- Credential Condition Mgmt

PKI Management
- Certificate Management

Access Management

Asset Management
- Asset Inventory Mgmt
- Asset Group Mgmt
- Access Rule Management

Security Clearance
- Security Clearance Mgmt

Authorization
- Community Management
- Permission Management

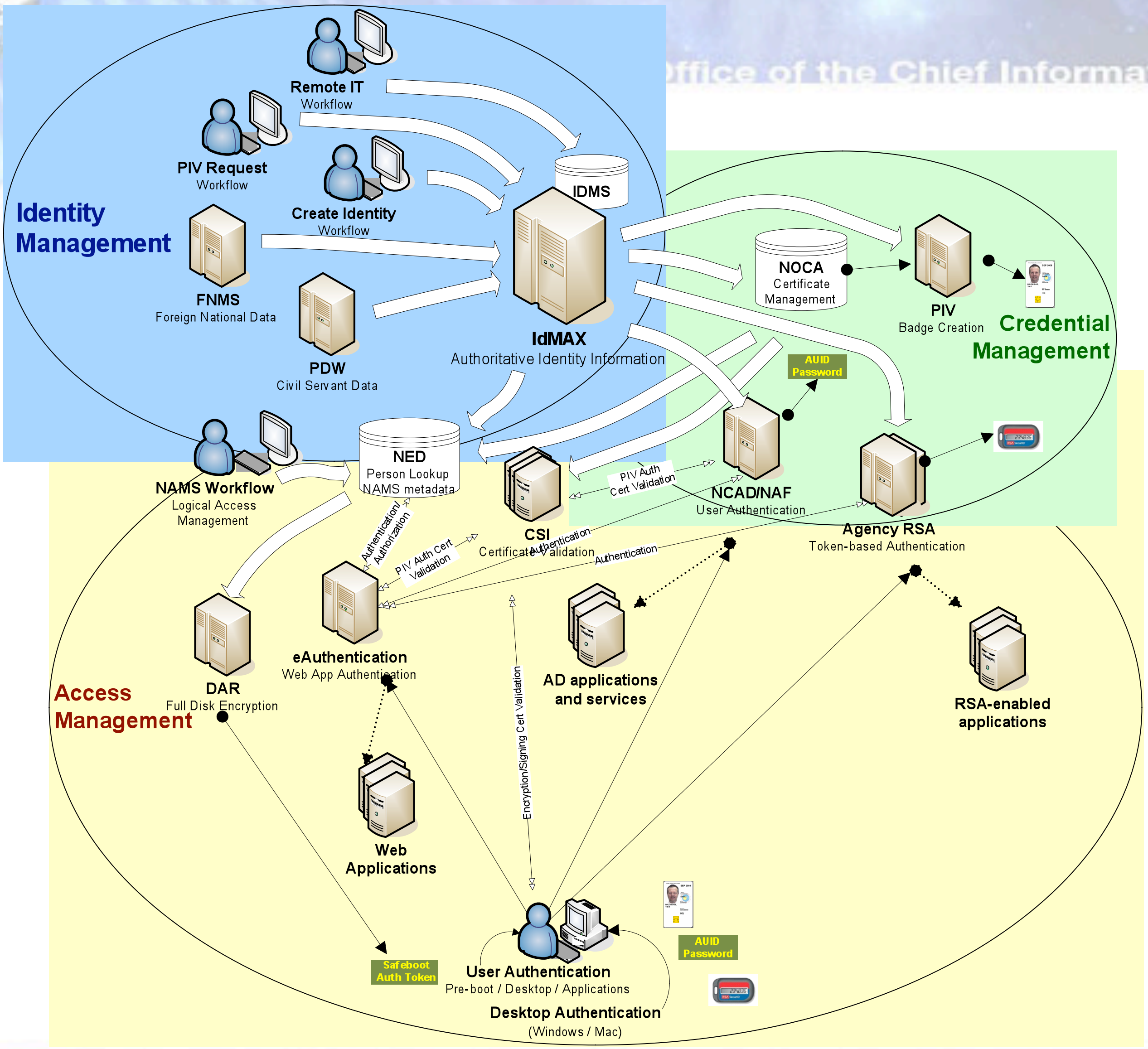
Authentication
- Access Control Mgmt
- Access Authentication

🟦 Included in Release 1.x

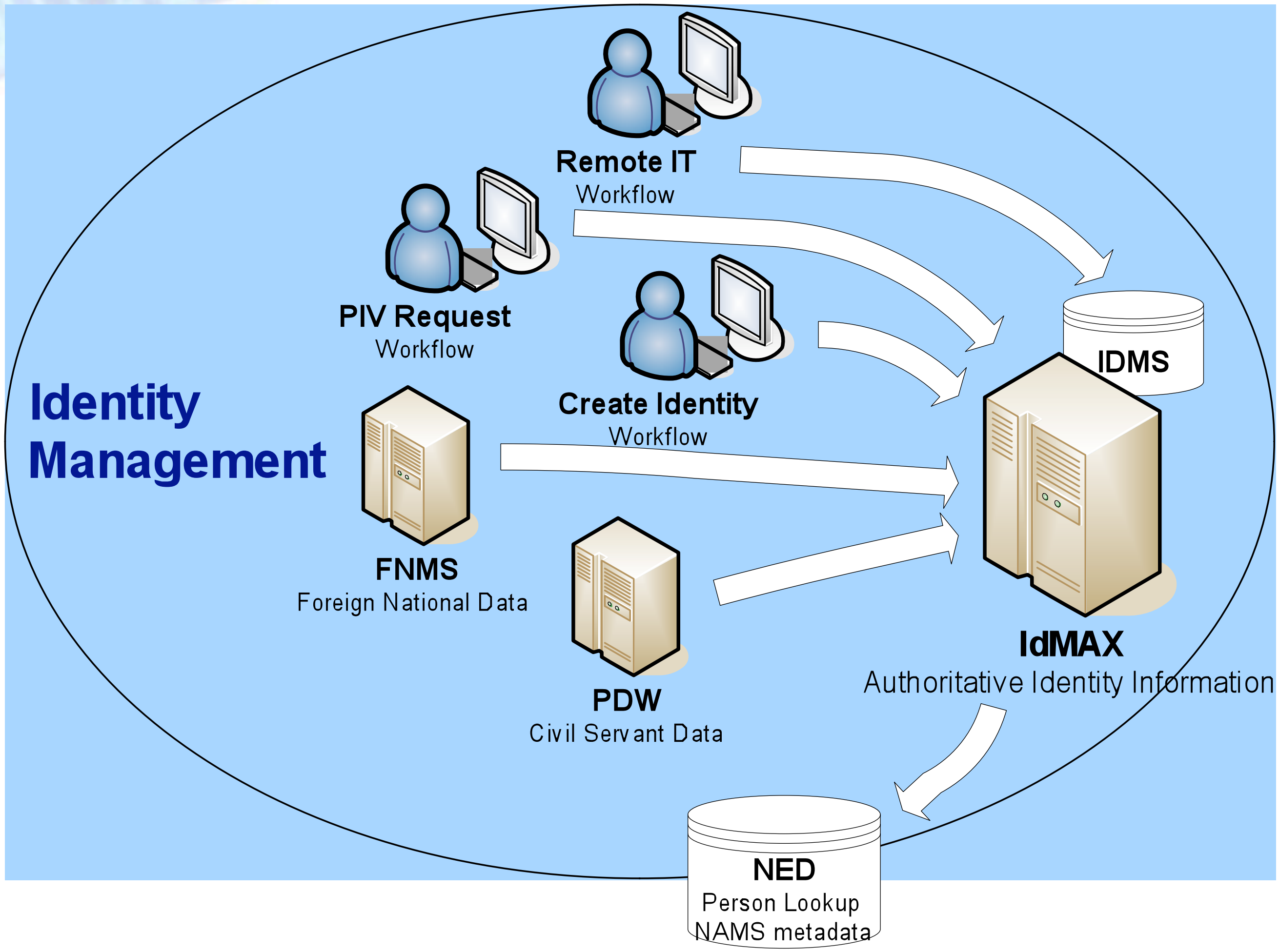
🟩 Included in Release 2.x

🟧 Included in Release 3.x

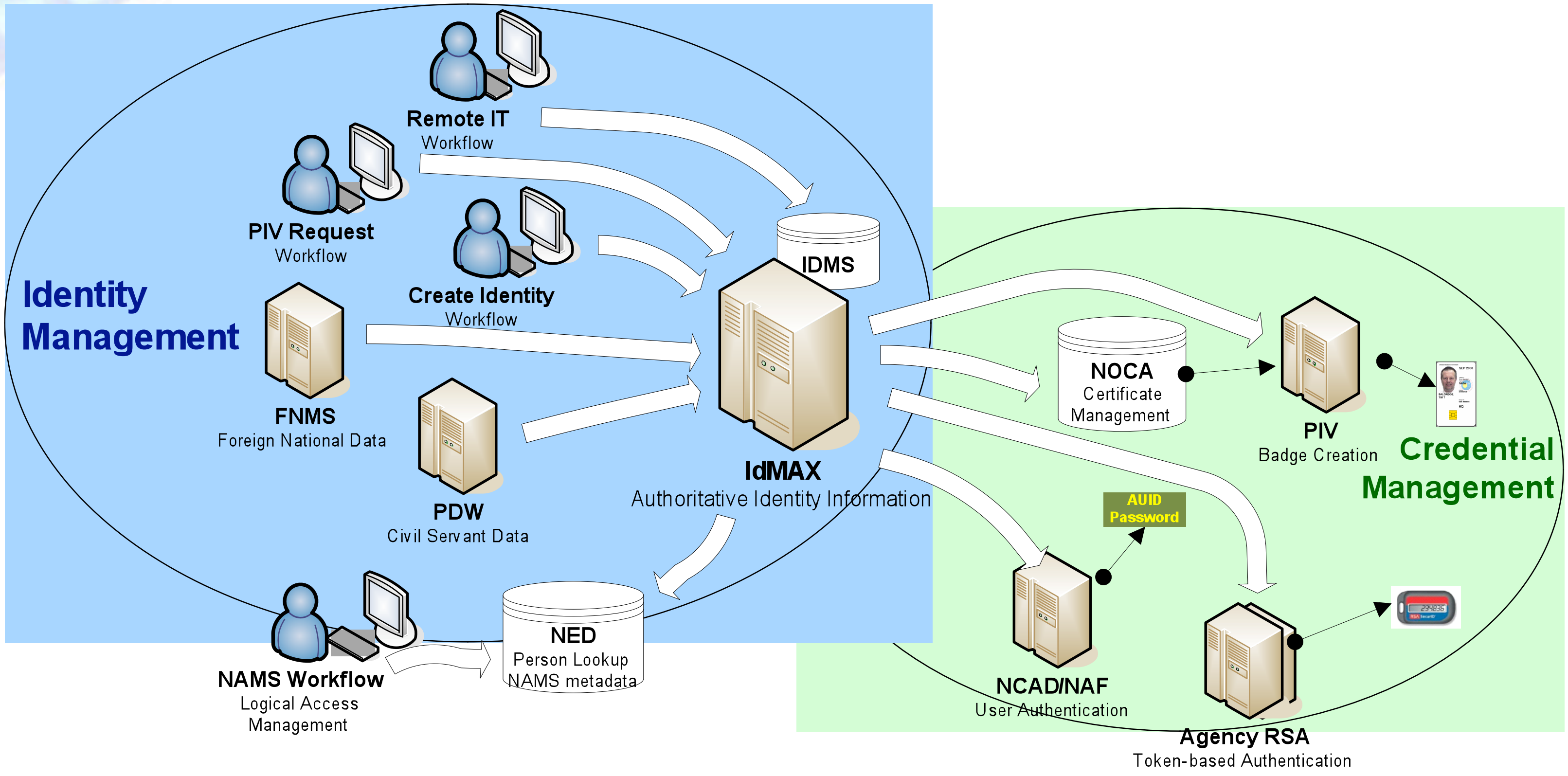
Technology Model



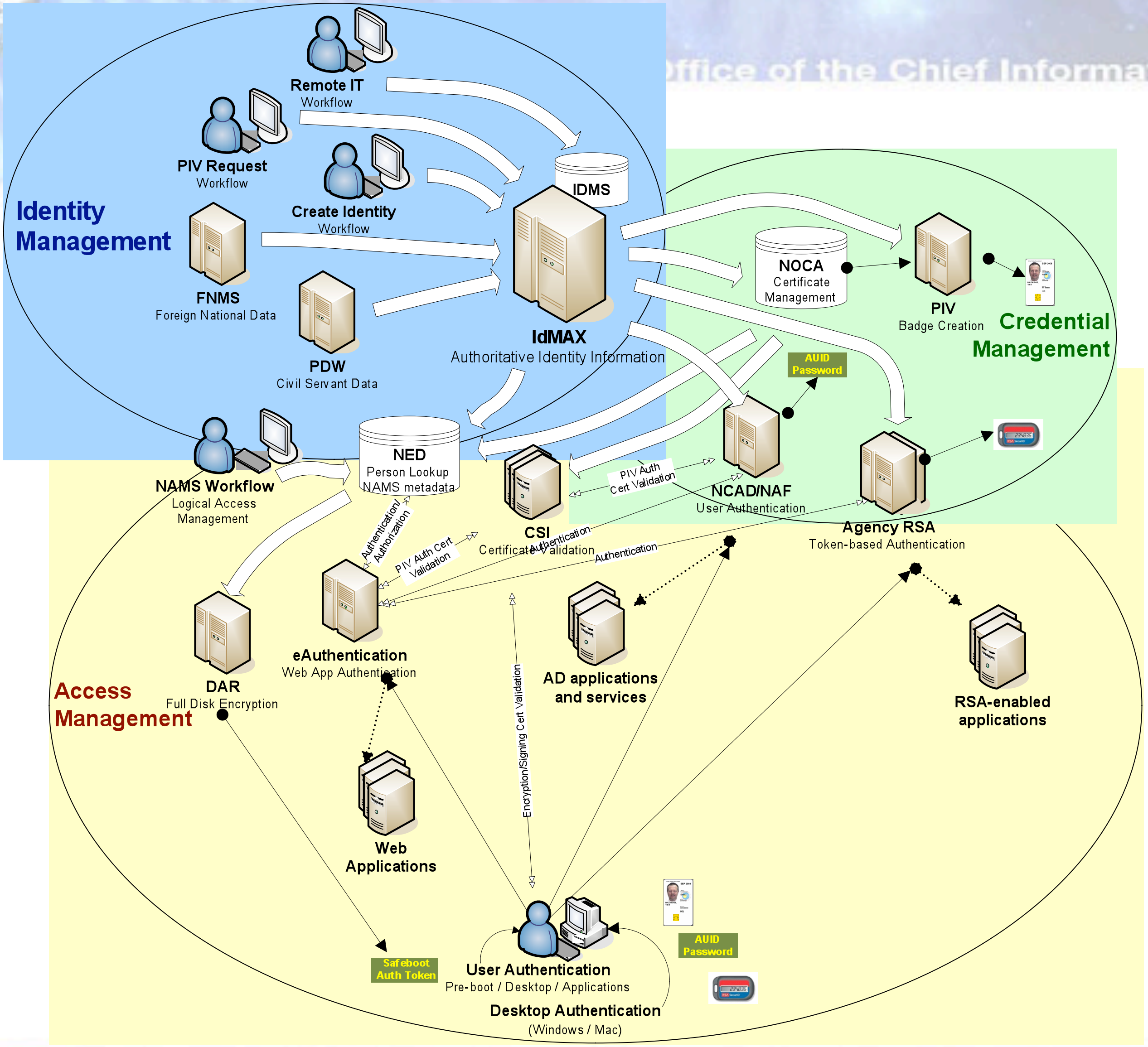
Identity Management



Identity and Credential

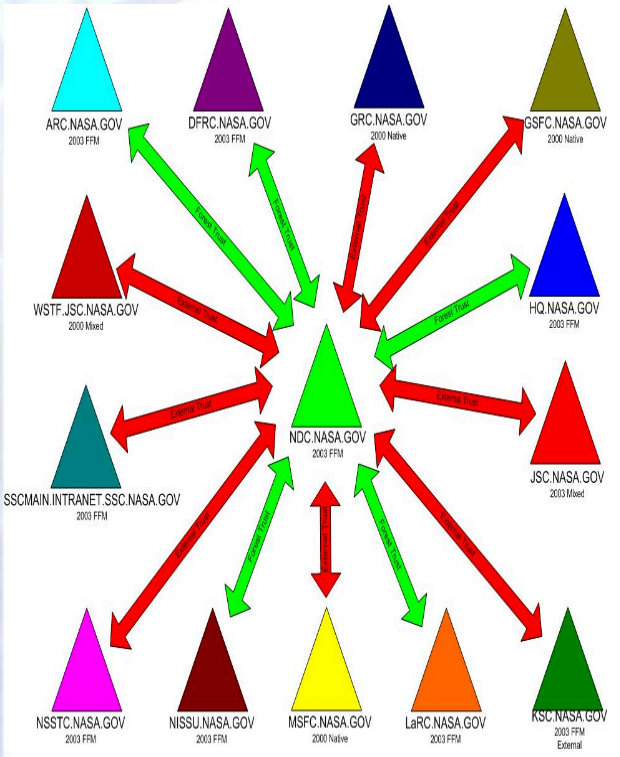


Full ICAM Model

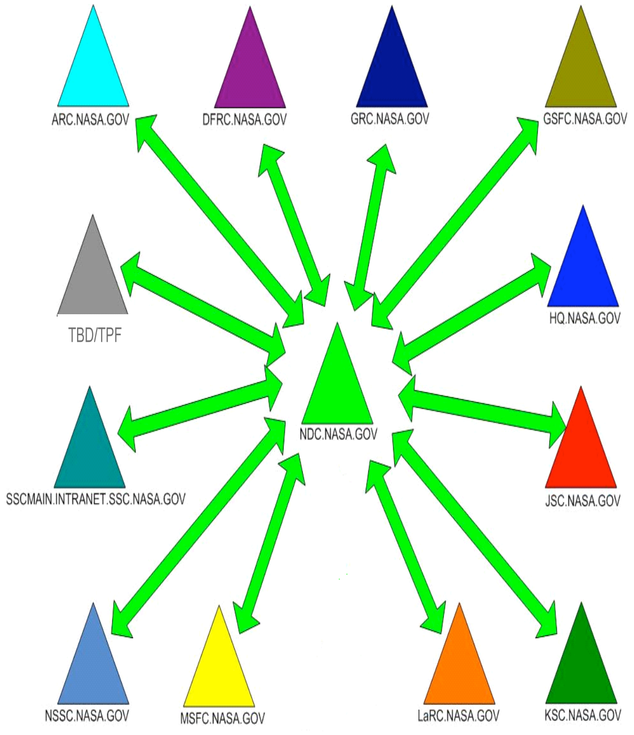


NCAD—Active Directory Forest and Domain Structure

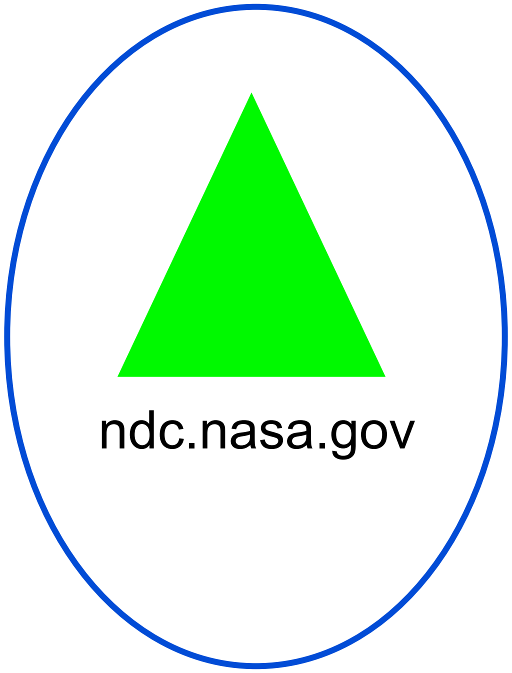
As-Is Structure



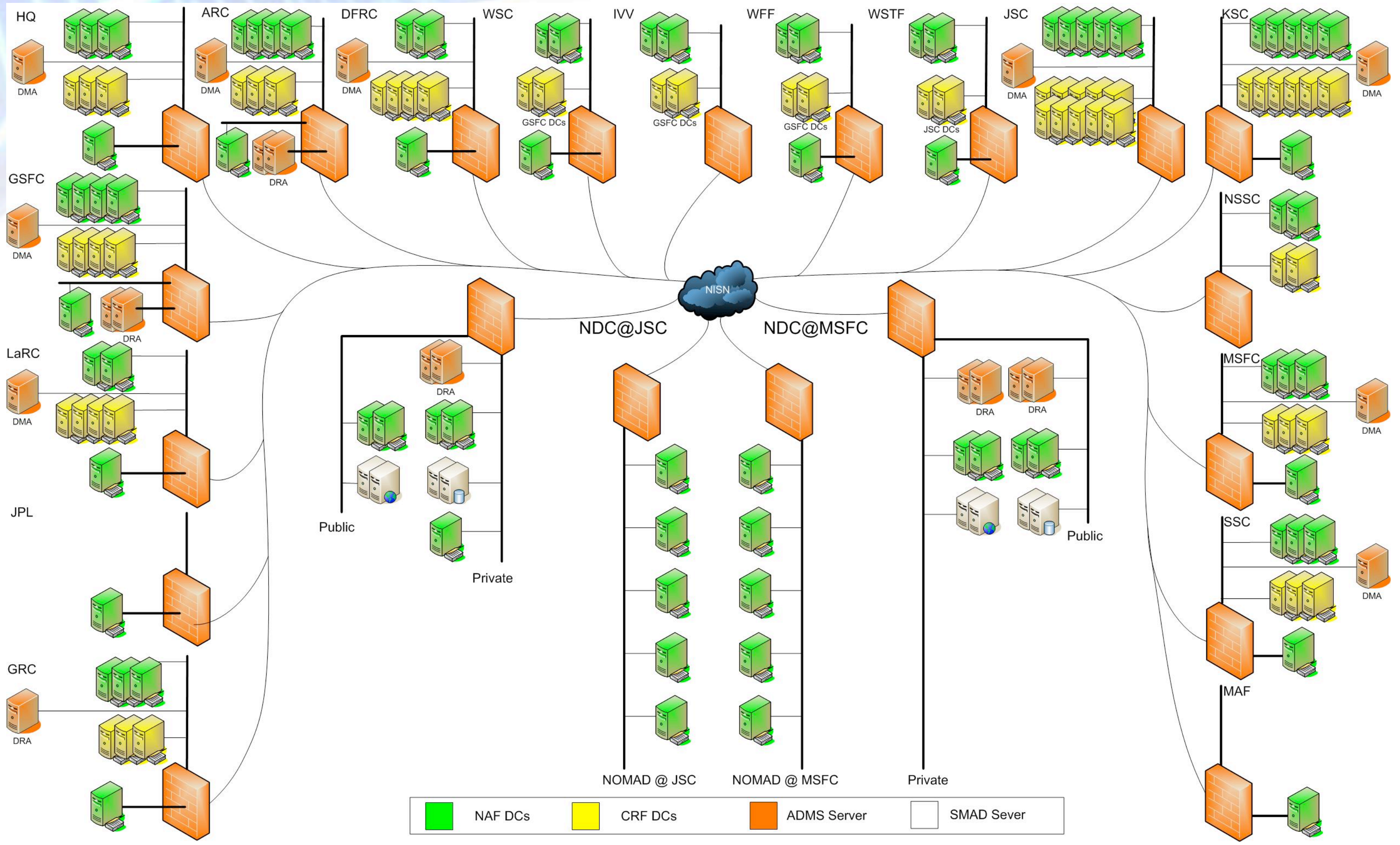
To-Be CDR Structure
Supports Migration Activities



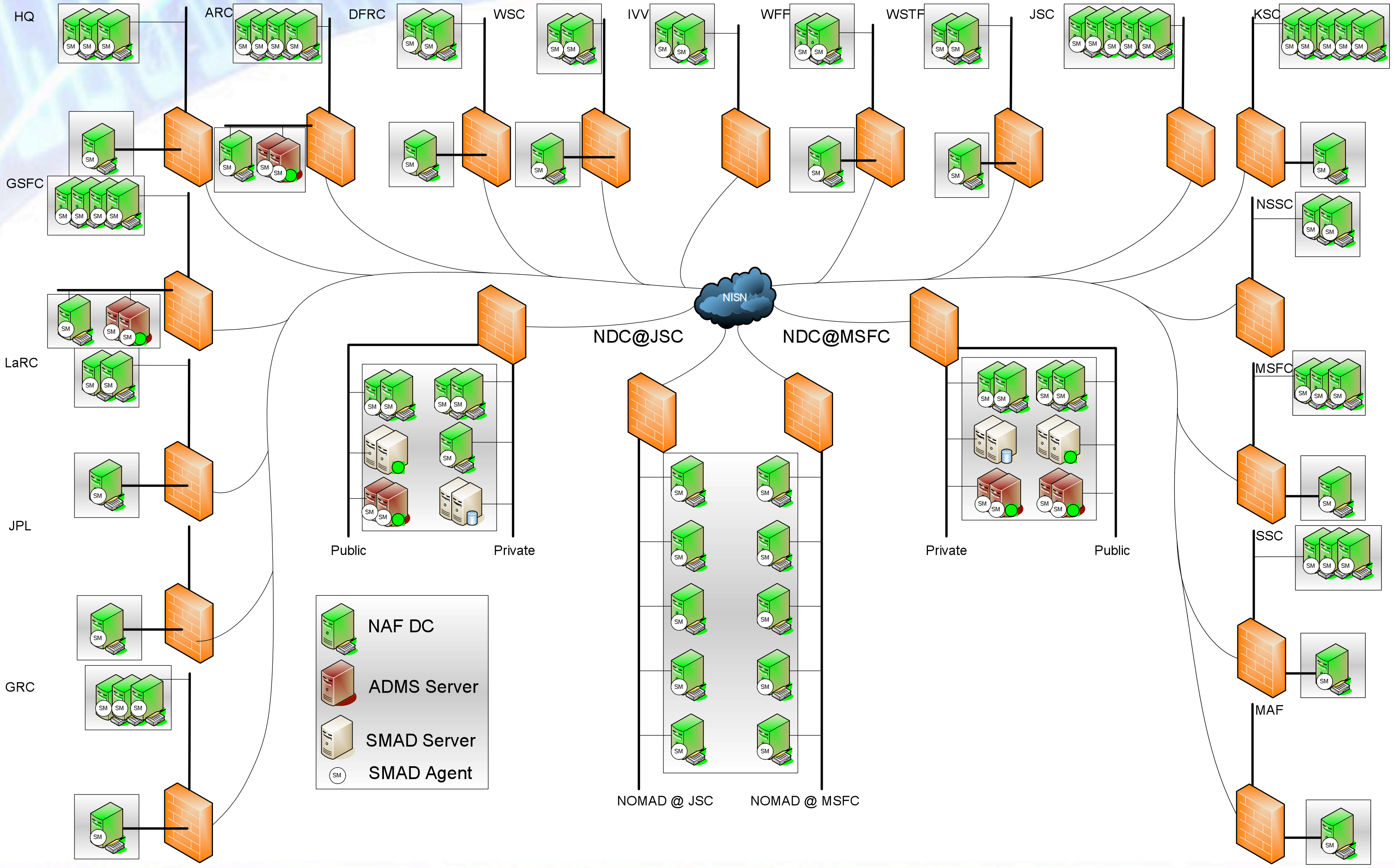
To-Be Structure:
One Forest
One Domain



NCAD—Interim/Current Topology



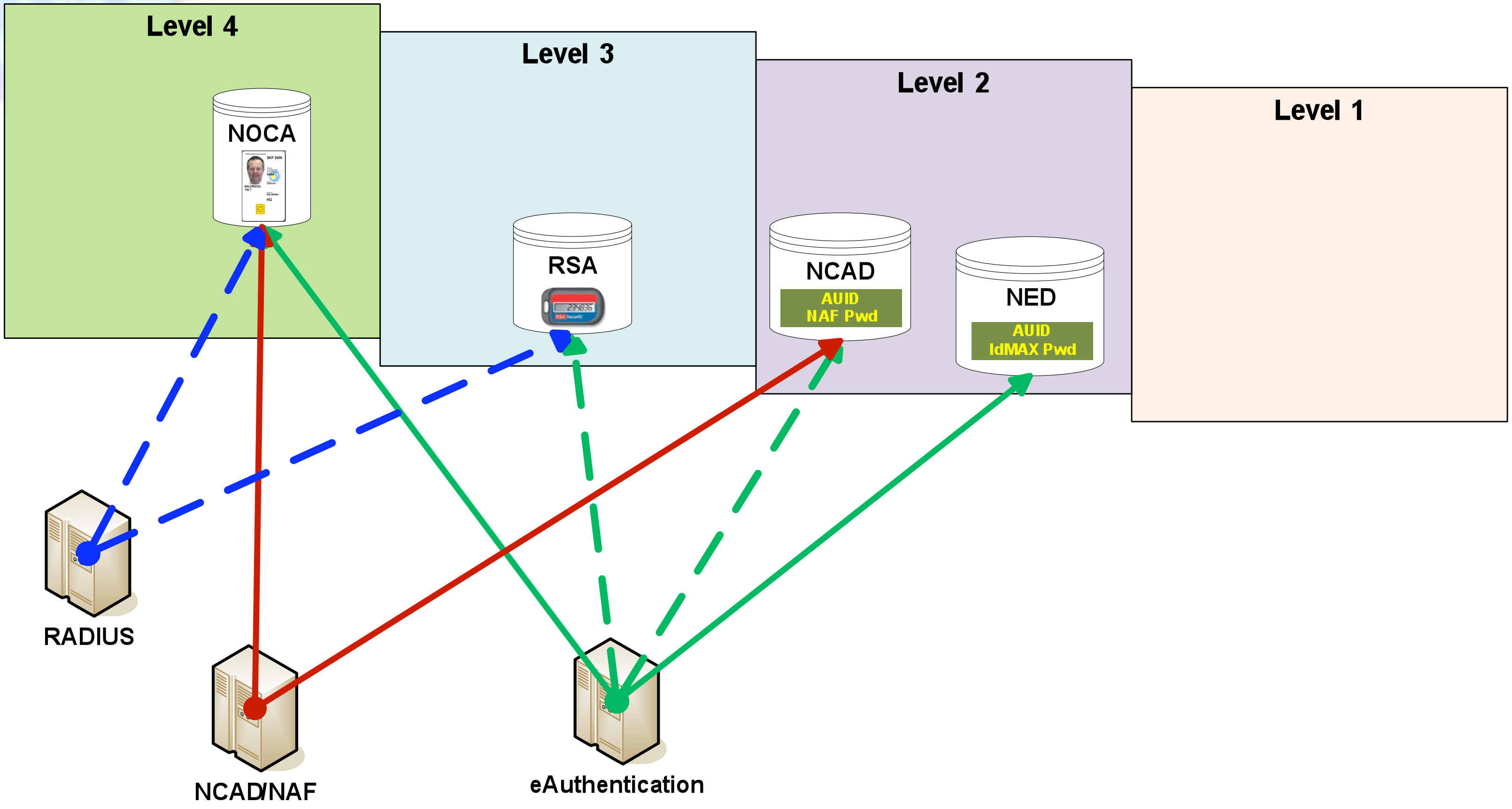
NCAD TO-BE Topology



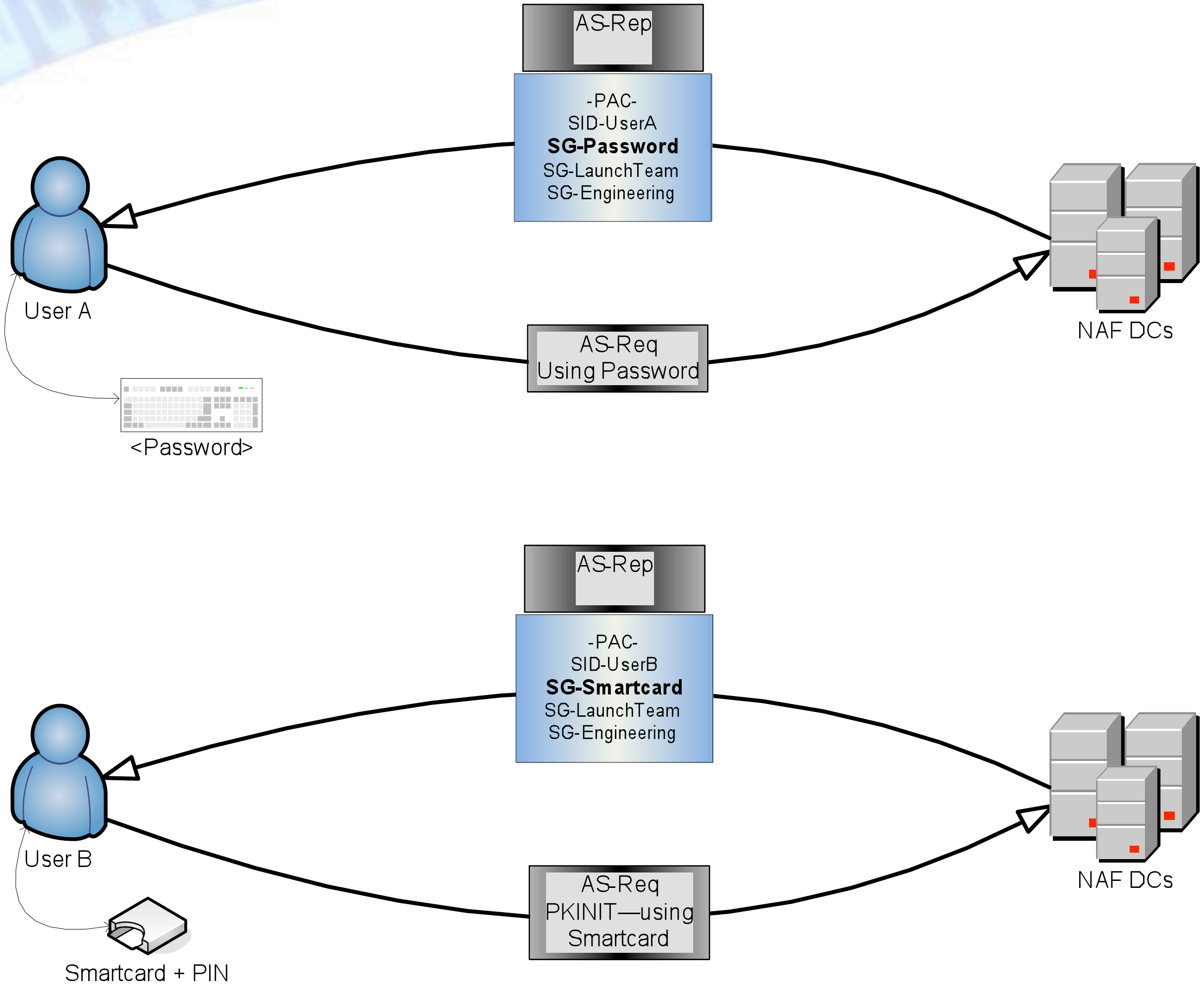
AD Consolidation Summary

- Finally top-down versus grass-roots
- Formal project methodology
  - System Engineering Methodology per NASA NPR 7123
  - Project Management Lifecycle per NASA NPR 7120.7
- Detailed large project plan with linked tasks
  - Project plan maintained by an experienced project scheduler
- Formality in test-set development
  - SIR-TP, SATS, ORTS, all with traceability
- Project Manager experienced in large engineering development; experienced program managers for two major contractors leading effort
- Brought in personnel with experience in similar consolidation efforts at Army, AF, and Navy-Marines
- All eggs in one basket argument…SIEM

LoA Introduction: Tokens



Missing—Capture of LoA on Logon



AS-Rep

-PAC-
SID-UserA
SG-Password
SG-LaunchTeam
SG-Engineering

User A

<Password>

AS-Req
Using Password

NAF DCs

AS-Rep

-PAC-
SID-UserB
SG-Smartcard
SG-LaunchTeam
SG-Engineering

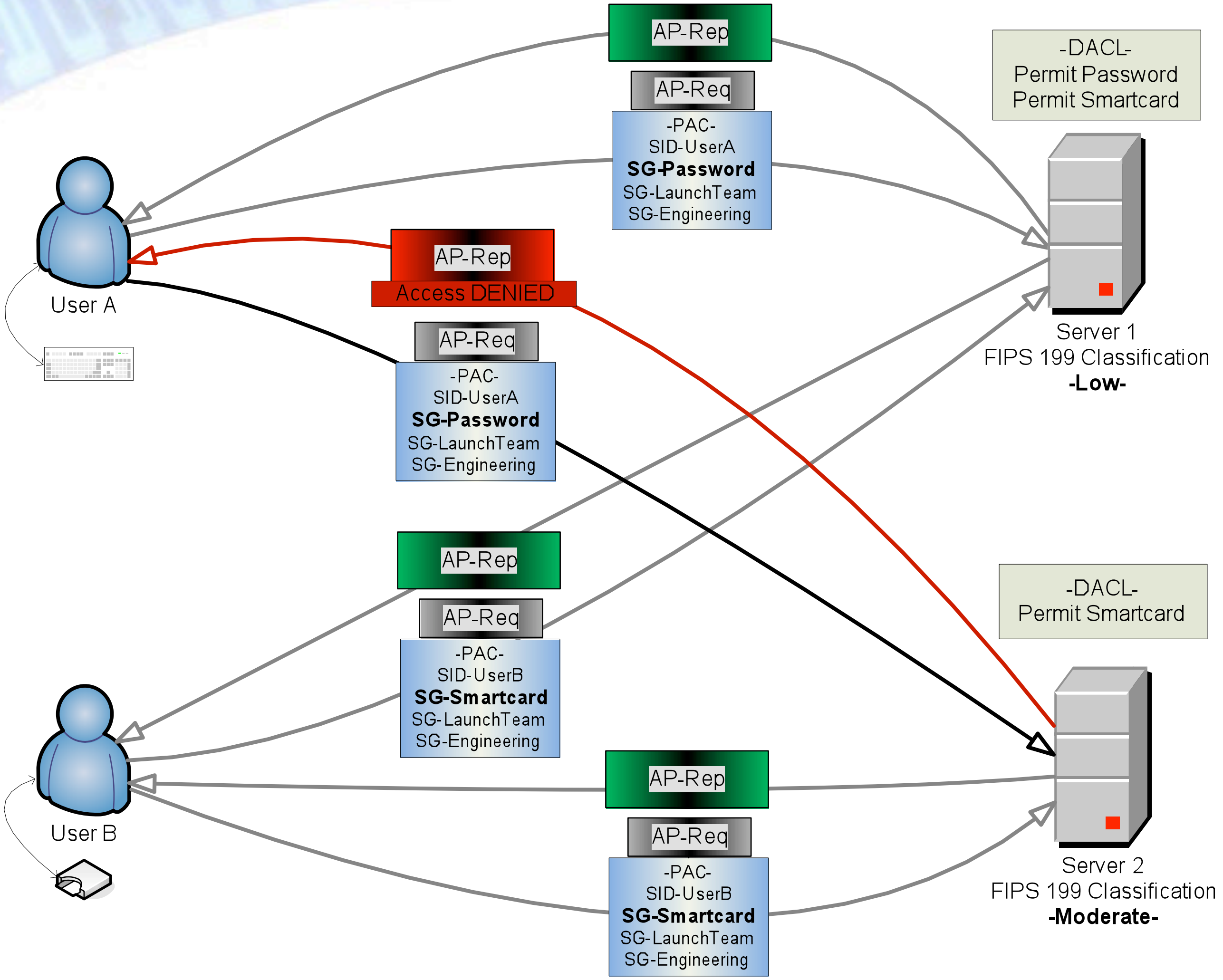
User B

Smartcard + PIN

AS-Req
PKINIT—using
Smartcard

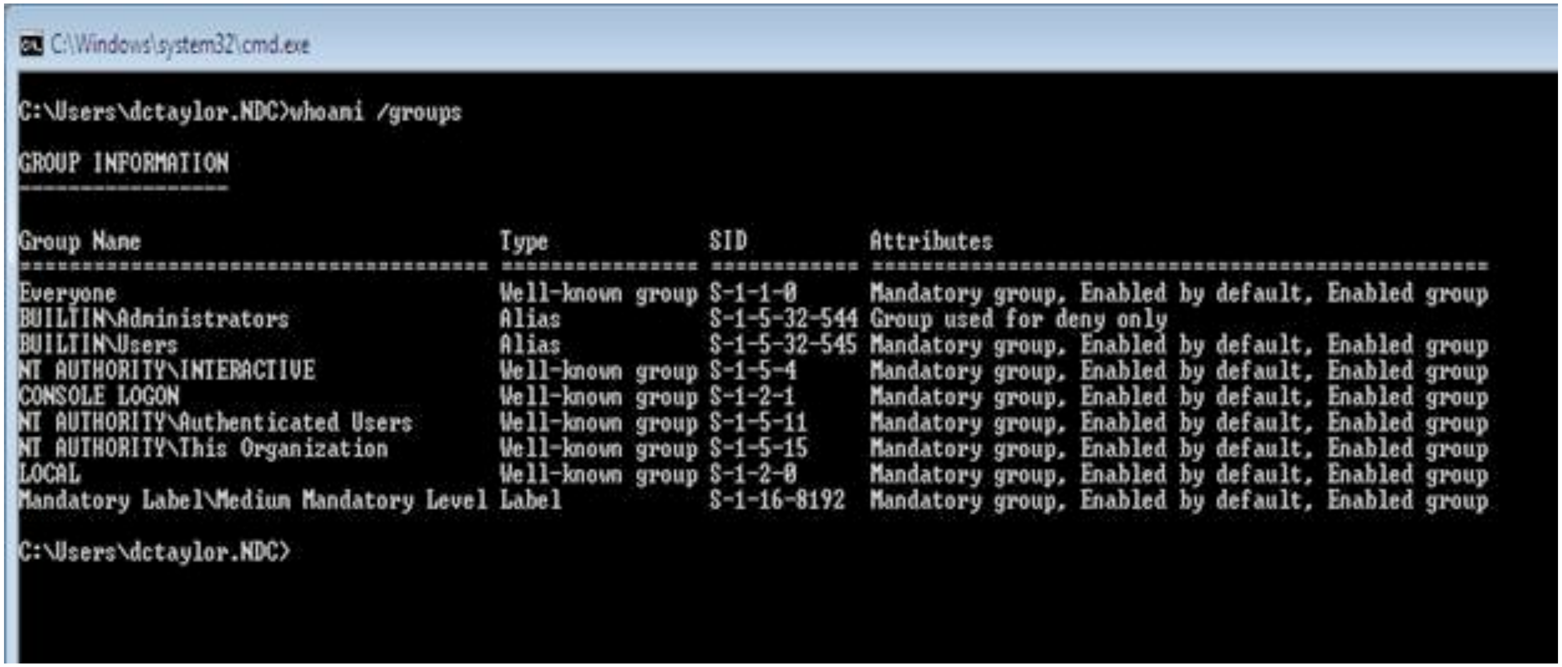
NAF DCs

Missing—AuthZ based upon LoA



New Developments Since April
Windows 2008 R2

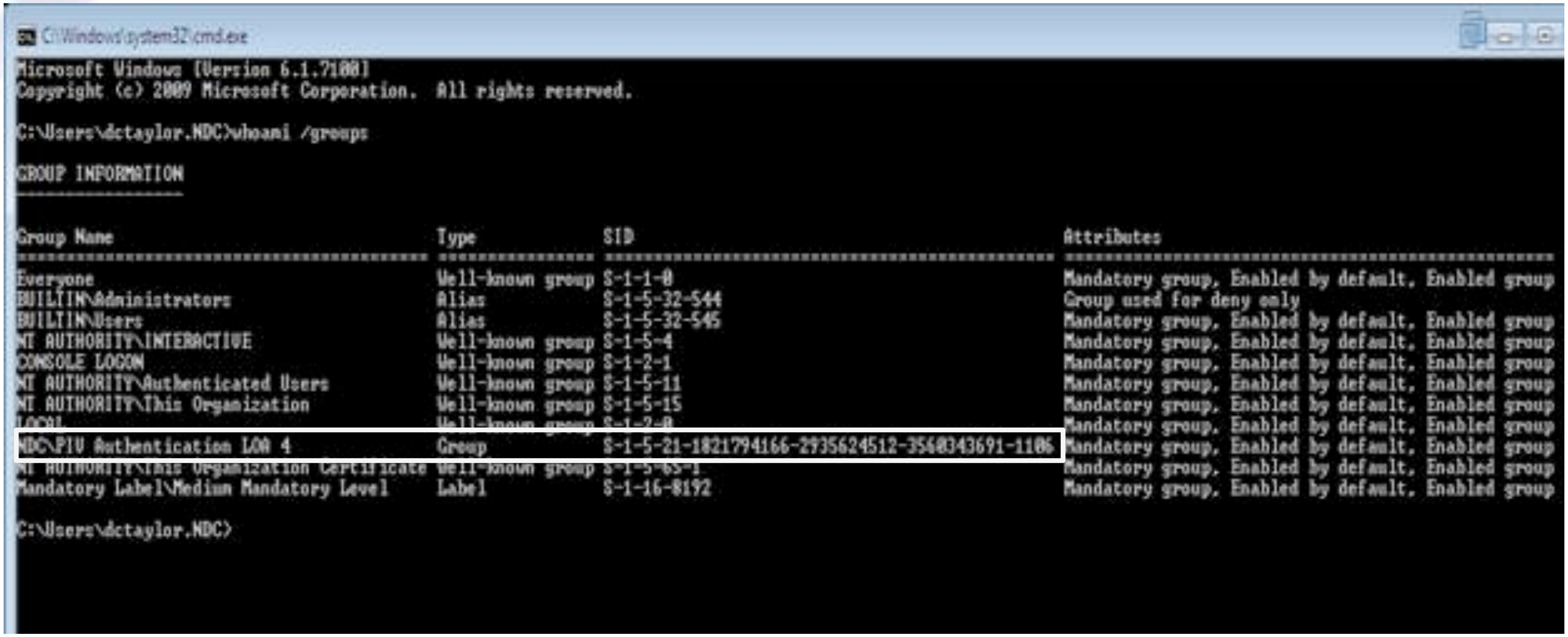
- Windows domain logon on an XP workstation using password



```
C:\Users\dctaylor.NDC>whoami /groups

GROUP INFORMATION
-----------------

Group Name                             Type             SID          Attributes
====================================== ================ ============ ==================================================
Everyone                               Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled group
BUILTIN\Administrators                 Alias            S-1-5-32-544 Group used for deny only
BUILTIN\Users                          Alias            S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\INTERACTIVE               Well-known group S-1-5-4      Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON                          Well-known group S-1-2-1      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users       Well-known group S-1-5-11     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization         Well-known group S-1-5-15     Mandatory group, Enabled by default, Enabled group
LOCAL                                  Well-known group S-1-2-0      Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Mandatory Level Label            S-1-16-8192  Mandatory group, Enabled by default, Enabled group

C:\Users\dctaylor.NDC>
```

New Developments Since April Windows 2008 R2

- Windows domain logon on an XP workstation using smartcard (PIV)



```
Microsoft Windows [Version 6.1.7100]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\dctaylor.NDC>whoami /groups

GROUP INFORMATION
-----------------

Group Name                                 Type             SID                                            Attributes
========================================== ================ ============================================== ==================================================
Everyone                                   Well-known group S-1-1-0                                        Mandatory group, Enabled by default, Enabled group
BUILTIN\Administrators                     Alias            S-1-5-32-544                                   Group used for deny only
BUILTIN\Users                              Alias            S-1-5-32-545                                   Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\INTERACTIVE                   Well-known group S-1-5-4                                        Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON                              Well-known group S-1-2-1                                        Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users           Well-known group S-1-5-11                                       Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization             Well-known group S-1-5-15                                       Mandatory group, Enabled by default, Enabled group
LOCAL                                      Well-known group S-1-2-0                                        Mandatory group, Enabled by default, Enabled group
NDC\PIV Authentication LOA 4               Group            S-1-5-21-1821794166-2935624512-3560343691-1106 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization Certificate Well-known group S-1-5-65-1                                     Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Mandatory Level     Label            S-1-16-8192                                    Mandatory group, Enabled by default, Enabled group

C:\Users\dctaylor.NDC>
```

Reference: http://technet.microsoft.com/en-us/library/dd378897.aspx

LoA Summary

- We are going to be using a mix of primarily passwords and smartcards for a long time
- We need our authentication service to provide an LoA attribute to our authorization mechanism
  - Authorization based upon strength of authentication
- Our eAuth service (based upon Sun Access Manager) can provide this attribute through SAML like structures
- We need Microsoft Active Directory to provide a similar functionality in their logon (KINIT, PKINIT) and resultant PAC authorization data
- We need capability to map particular policy OID to security group
  - id-fpki-common-authentication means PIV card (only real measure)

National Aeronautics and Space Administration

Backup

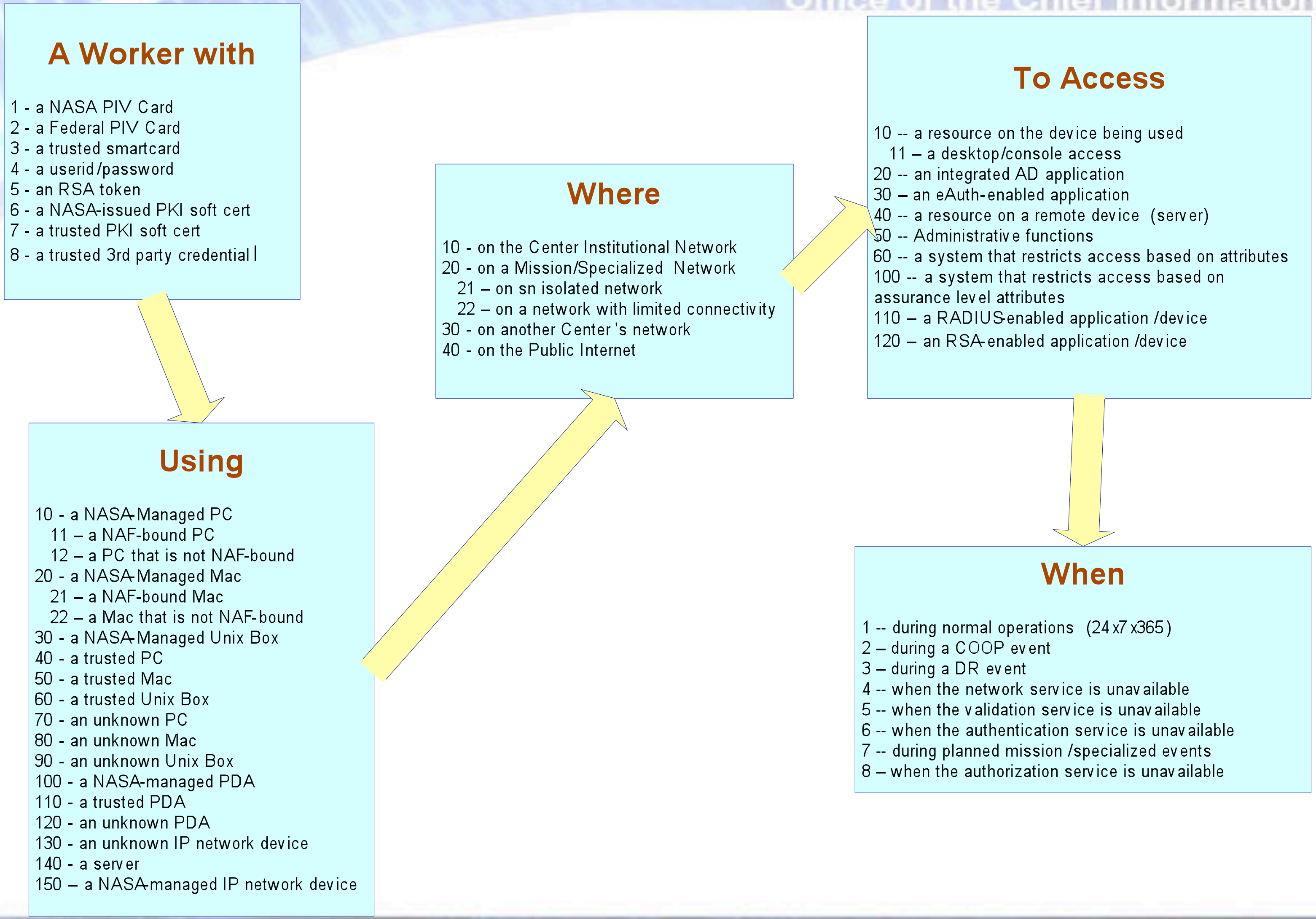
Office of the Chief Information Officer

VISION: Integrated, secure, and efficient information technology and solutions that support NASA

Conclusions

- A well-developed Enterprise Architecture is essential to ICAM implementation
- NASA must implement Position and Community Management modules in order to support robust ABAC
- Integrated data flow means data is only authoritative at the source, and changes can only occur at the source
- Identity federation and LoA require additional maturity in the market
- Technology is sometimes tricky, but politics is harder!
- Single sign-on is a strong motivator for migration

Use Cases



A Worker with

1 - a NASA PIV Card
2 - a Federal PIV Card
3 - a trusted smartcard
4 - a userid/password
5 - an RSA token
6 - a NASA-issued PKI soft cert
7 - a trusted PKI soft cert
8 - a trusted 3rd party credential

Using

10 - a NASA-Managed PC
   11 – a NAF-bound PC
   12 – a PC that is not NAF-bound
20 - a NASA-Managed Mac
   21 – a NAF-bound Mac
   22 – a Mac that is not NAF-bound
30 - a NASA-Managed Unix Box
40 - a trusted PC
50 - a trusted Mac
60 - a trusted Unix Box
70 - an unknown PC
80 - an unknown Mac
90 - an unknown Unix Box
100 - a NASA-managed PDA
110 - a trusted PDA
120 - an unknown PDA
130 - an unknown IP network device
140 - a server
150 – a NASA-managed IP network device

Where

10 - on the Center Institutional Network
20 - on a Mission/Specialized Network
   21 – on sn isolated network
   22 – on a network with limited connectivity
30 - on another Center's network
40 - on the Public Internet

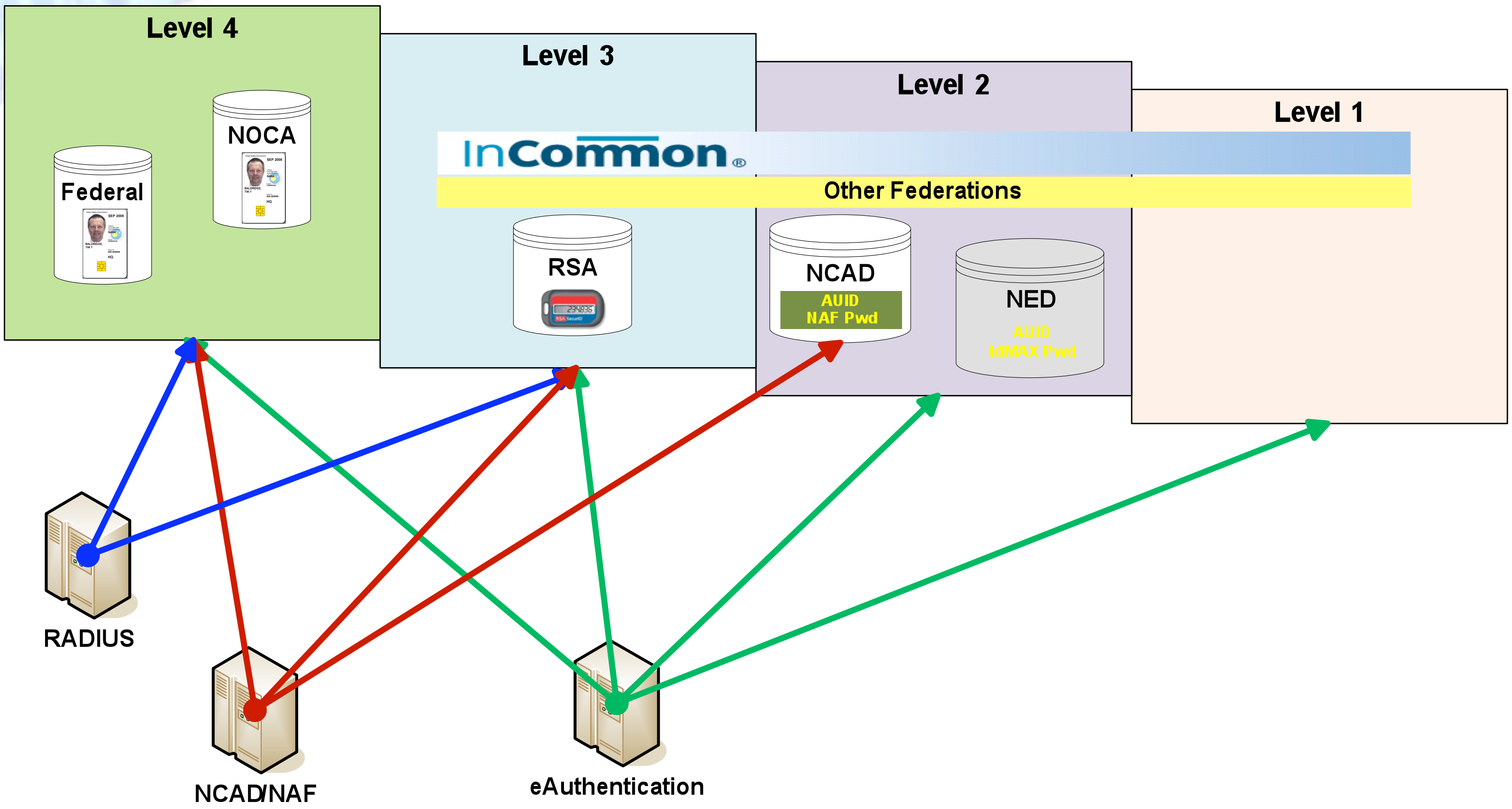
To Access

10 -- a resource on the device being used
   11 – a desktop/console access
20 -- an integrated AD application
30 – an eAuth-enabled application
40 -- a resource on a remote device (server)
50 -- Administrative functions
60 -- a system that restricts access based on attributes
100 -- a system that restricts access based on assurance level attributes
110 – a RADIUS-enabled application/device
120 – an RSA-enabled application/device

When

1 -- during normal operations (24x7x365)
2 – during a COOP event
3 – during a DR event
4 -- when the network service is unavailable
5 -- when the validation service is unavailable
6 -- when the authentication service is unavailable
7 -- during planned mission/specialized events
8 – when the authorization service is unavailable

Future LoA Tokens



Level 4

Federal

NOCA

Level 3

RSA

Level 2

NCAD

AUID
NAF Pwd

NED

AUID
IdMAX Pwd

Level 1

InCommon®

Other Federations

RADIUS

NCAD/NAF

eAuthentication