DAF ENTERPRISE ICAM ROADMAP

Impact to the DAF

- Transition to convenient, automated access determinations
- Risk-based and behavioral-based dynamic access
- Enhanced auditability for our financial community

Publication: 12 JUL 2023

FY23	FY24	FY25 – FY28
Document Current State Lay Foundation of Enterprise Infrastructure Focus on App Onboarding - Prioritize FIAR Audit Topics	ICAM System Migration Application Adoption Focus on Deployed Access	Continue to Drive System Adoption Focus on Dynamic Access Decisions

Services and Strategic Narratives

Identity Provider (IdP)
Implement a singular representation of all DAF and federated entities with a separate IdP for PE and NPE.

Identity Data Service
Evolve current identity services to be increasingly flexible, cloud-native, and capable of handling complex attributes.

Attribute Management
Deploy an attribute management platform with the ability to manage and update data while protecting the integrity of the data repository.

Credential Lifecycle Management
Standardize on a set of supported credential options that meet the needs of the different DAF user communities and balances cost, risk, and convenience.

Federation
Develop standards and services that ensure seamless credential interoperability and attribute exchange between organizations.

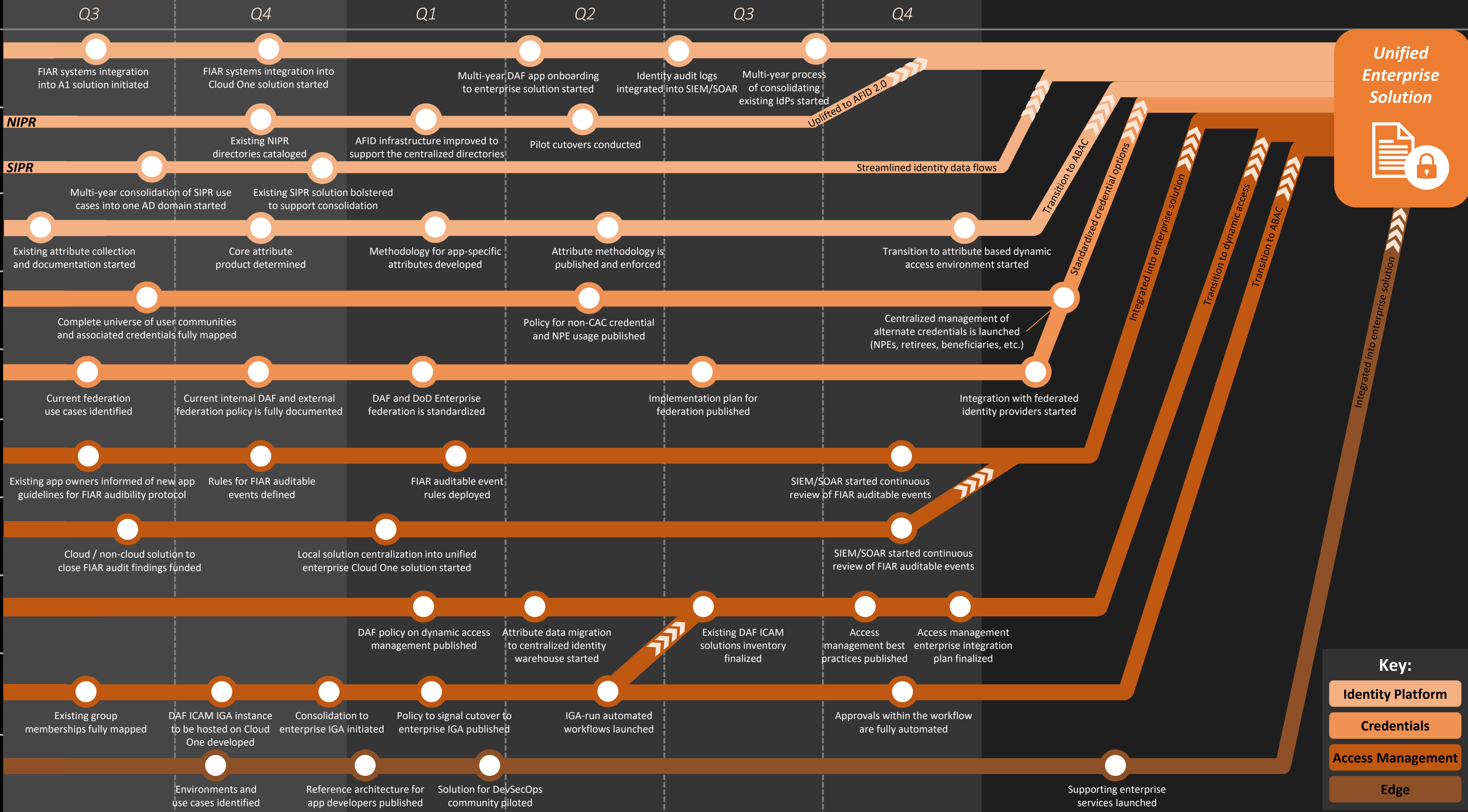
Functional Privileged Access Management
Evolve logging and delivery systems to provide auditability for sensitive application events.

IT Privileged Access Management
Centralize IT PAM practices into a set of services that meet audit guidelines & security best practices.

Dynamic Access Management
Evolve to have user attributes determine access based upon a centralized entitlements management system, enabling automatic provision and deprovisioning.

Identity Governance and Administration
Replace DD2875 process with a combination of standardized SAAR workflows (in an enterprise IGA tool) and dynamic access (when policy rules can be defined, and attributes are available).

Deployed & Disadvantaged
Launch extension of enterprise access management to cover scenarios where disconnection is likely or there is no centralized enterprise presence.



Identity Provider (IdP):
- FIAR systems integration into A1 solution initiated
- FIAR systems integration into Cloud One solution started
- Multi-year DAF app onboarding to enterprise solution started
- Identity audit logs integrated into SIEM/SOAR
- Multi-year process of consolidating existing IdPs started
- Uplifted to AFID 2.0

Identity Data Service:
- NIPR: Existing NIPR directories cataloged
- NIPR: AFID infrastructure improved to support the centralized directories
- NIPR: Pilot cutovers conducted
- SIPR: Multi-year consolidation of SIPR use cases into one AD domain started
- SIPR: Existing SIPR solution bolstered to support consolidation
- Streamlined identity data flows

Attribute Management:
- Existing attribute collection and documentation started
- Core attribute product determined
- Methodology for app-specific attributes developed
- Attribute methodology is published and enforced
- Transition to attribute based dynamic access environment started
- Transition to ABAC

Credential Lifecycle Management:
- Complete universe of user communities and associated credentials fully mapped
- Policy for non-CAC credential and NPE usage published
- Centralized management of alternate credentials is launched (NPEs, retirees, beneficiaries, etc.)
- Standardized credential options

Federation:
- Current federation use cases identified
- Current internal DAF and external federation policy is fully documented
- DAF and DoD Enterprise federation is standardized
- Implementation plan for federation published
- Integration with federated identity providers started

Functional Privileged Access Management:
- Existing app owners informed of new app guidelines for FIAR audibility protocol
- Rules for FIAR auditable events defined
- FIAR auditable event rules deployed
- SIEM/SOAR started continuous review of FIAR auditable events
- Integrated into enterprise solution

IT Privileged Access Management:
- Cloud / non-cloud solution to close FIAR audit findings funded
- Local solution centralization into unified enterprise Cloud One solution started
- SIEM/SOAR started continuous review of FIAR auditable events

Dynamic Access Management:
- DAF policy on dynamic access management published
- Attribute data migration to centralized identity warehouse started
- Existing DAF ICAM solutions inventory finalized
- Access management best practices published
- Access management enterprise integration plan finalized
- Transition to dynamic access

Identity Governance and Administration:
- Existing group memberships fully mapped
- DAF ICAM IGA instance to be hosted on Cloud One developed
- Consolidation to enterprise IGA initiated
- Policy to signal cutover to enterprise IGA published
- IGA-run automated workflows launched
- Approvals within the workflow are fully automated
- Transition to ABAC

Deployed & Disadvantaged:
- Environments and use cases identified
- Reference architecture for app developers published
- Solution for DevSecOps community piloted
- Supporting enterprise services launched
- Integrated into enterprise solution

Unified Enterprise Solution

Key:

- Identity Platform
- Credentials
- Access Management
- Edge

SAF/CN
7/12/2023

DAF ENTERPRISE ICAM ROADMAP

RELEASE NOTES

EDITORIAL NOTES

Following publication in February 2023, SAF/CN updated this roadmap to accurately reflect the status of DAF Enterprise ICAM as a "snapshot in time" so that it can continue to serve as a guide to the transition and integration to an enterprise ICAM solution.

To ensure this update aligned with how we plan to get to the desired end state for enterprise ICAM, we streamlined the organization of services on the left side of the roadmap and re-engaged extensively with ICAM DAF stakeholders, industry partners, and other government stakeholders. Their feedback gave clarity on sequencing of milestones and alignment of the grouping of services. This collaborative effort led us to not only rethink and refine a variety of milestones, but also our roadmap update processes as well.

The next iteration will leverage DAF Zero Trust FMO's task management system (out of ACC/A60) to ensure that updates are streamlined and based off real-time data.

✓ WHAT'S BEEN ACCOMPLISHED?

- Solution selected for IT PAM, awaiting final review, and funding
- Began ICAM FIAR integrations for first two groupings of FIAR systems

NEXT QUARTER'S PRIORITIES…

- Development of DAF ICAM IGA instance hosted on Cloud One
- Development of enterprise architecture for AFID
- Kickoff DevSecOps architecture sprints

WHAT'S CHANGED?

SERVICE(S)	UPDATES TO ROADMAP
THEME: Reorganization of Services & Grouping	
Identity Governance, Administration	Changed "Group Management" service name to "Identity Governance and Administration (IGA)" to better align with industry standard terminology; updated strategic narrative to better explain the end goal; shifted milestone "DAF ICAM IGA instance to be hosted on Cloud One developed" from IdP service to IGA service and moved back to Q4 (delayed pending review & decision of DB solution to align with A1 solution in Q4)
Functional PAM, IT PAM, Dynamic Access Management, IGA	Changed key from "PAM" to "Access Management", which now includes Functional PAM, IT PAM, Dynamic Access Management, and IGA
Functional PAM, IT PAM	Shifted milestone "SIEM/SOAR started continuous review of FIAR auditable events" to FY24 Q4
Dynamic Access Management	Shifted existing milestones to the right so that they are occurring after IGA deployment; added earlier milestone to identify policy for Dynamic Access Management first
Identity Provider	Shifted existing milestones to the right; dependent on IGA deployment
THEME: Clarity, Specificity, & Consistency	
Federation	Added additional milestone in FY23 to better understand internal and external federation
Dynamic Access Management	Added additional details to strategic narrative and milestones throughout to align with Enterprise ICAM Transformation Journey created by HNID
Identity Provider	Added milestone in FY23 to clarify progress on integration into A1 solution prior to migration to enterprise solution

DAF ENTERPRISE ICAM ROADMAP | *ACRONYMS AND DEFINITIONS*

Acronym/Term	Definition
ABAC	Attribute based access control
AD	Active Directory
AFID	Air Force Intelligence Directorate
BYOAD	Bring your own approved device
CAC	Common access card
COTS	Commercial Off-The-Shelf software
DAF	Department of the Air Force
DD2875	Form for system authorization access request
DevSecOps	Development, Security, and Operations
FIAR	Financial Improvement and Audit Readiness
ICAM	Identity, Credential, and Access Management
IdP	Identity provider
IGA	Identity Governance and Administration
MFA	Multi factor authentication
NIPR	Non-secure Internet Protocol Router
NPE	Non-person entity

Acronym/Term	Definition
PAM	Privileged Access Management
PE	Person entity
Purebred	Credential issuance system for DoD that allows users to access DoD PK-enabled sites from their mobile devices
SAAR	System Authorization Access Request
SIEM	Security Information & Event Management
SIPR	Secure Internet Protocol Router
SOAR	Security Orchestration, Automation and Response