ICAM
DEPARTMENT OF THE AIR FORCE | IDENTITY, CREDENTIAL AND ACCESS MANAGEMENT

IDENTITY SOLUTIONS

Identity First

DAF Identity Credential and Access Management (ICAM) Enterprise Readiness

PA Release # 66ABG-2026-0031



Agenda

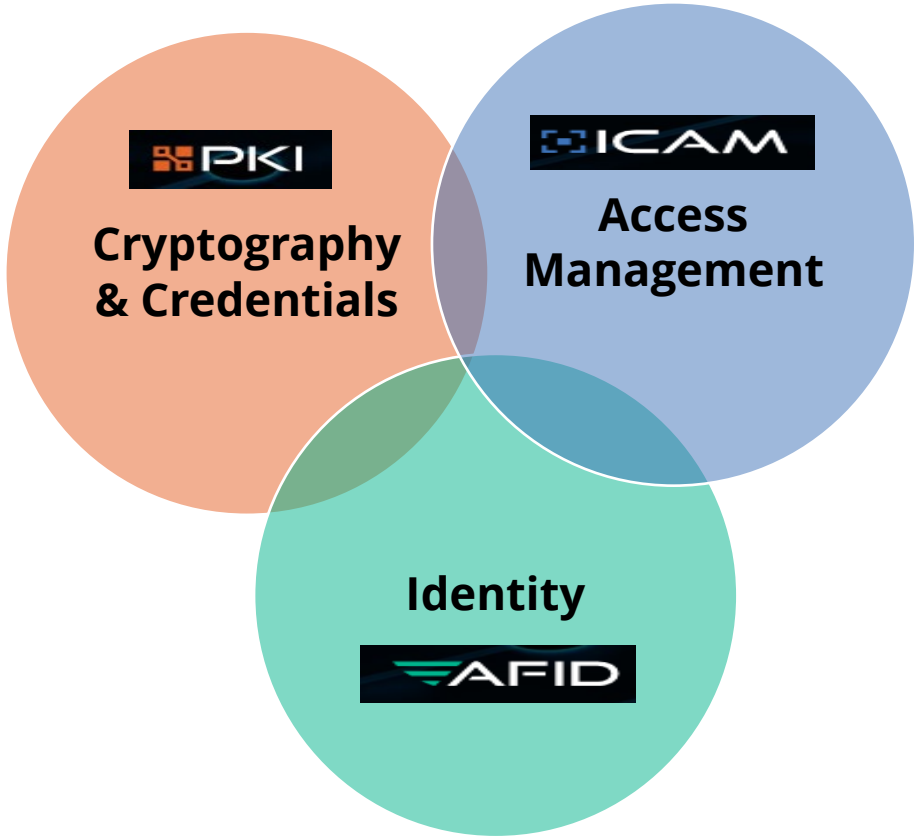
- HNID Identity Solutions Branch
- Identity Solutions Fundamentals
- DAF ICAM Today: Our Current Operational Posture
- Key Enhancements & Capabilities
- Enablement Process
- Q&A

HNID: Identity Solutions Branch

- The Air Force Life Cycle Management Center (AFLCMC) Identity Solutions Branch (HNID) is responsible for acquiring, developing and delivering capabilities to secure cyberspace through robust Identity, Credential, Access Management (ICAM), Public Key Infrastructure (PKI) solutions and Air Force Identity.

- Our core mission is to ensure secure, uninterrupted authentication and authorization to systems, data, and information.

- HNID is your partner in cyber defense. Whether you are a Wing Cybersecurity Liaison, a System Owner, or a Program Manager, our team is here to provide the tools, guidance, and cryptographic infrastructure needed to secure your systems and protect our warfighters.



The Fundamentals of Identity Solutions

IDENTITY

1

Ensure **identity and attribute information** is accurate and accessible for mission requirements

CREDENTIAL

2

Develop, deliver and sustain **cryptographically assured credentials**

ACCESS

3

Secure managed access to mission-specific applications, tools and systems

Priorities:

Enable Joint Force Interoperability: Standardizing identity assurance levels to allow seamless, secure collaboration across joint and coalition networks.

AFID

Modernize PKI & Cryptography: Driving the transition to next-generation algorithms (CNSA 1.0) and preparing the DAF for the Post-Quantum Cryptography (CNSA 2.0) threat landscape.

PKI

Operationalize Zero Trust: Delivering the cryptographic and identity foundations required to achieve absolute data security across multi-domain operations.

ICAM

Timeline

Foundational Strategy Phase (2020-2021)

Establishing the baseline requirements and enterprise vision

Deployment & Operationalizing Phase (2021-2023)

Shifting from strategy to operational concepts, testing, deployment, and configuration of the system

ZT Alignment & Adoption Phase (2023-2025)

Mapping deployed capabilities to DoW Zero Trust capabilities and enabling DAF systems with the DAF ICAM Zero Trust identity capabilities

Compliance & Enhancements Phase (current)

Enforcing compliance, defining approved solutions, and executing the mandate

Operational Posture



Background

Delivers a foundation for Zero Trust

Supports Audit Readiness

Provides support for DAF personnel, non-CAC eligible personnel, and various DAF systems

Expands identity management to all users: Non-CAC, Administrators, and Non-Person Entities



Operational Scope

Delivers a centralized identity platform with a governance framework that enables automated enterprise authorization services

Provides the right access to the right entity for the right reason – anytime and anywhere

Increases cybersecurity by automating user provisioning/deprovisioning



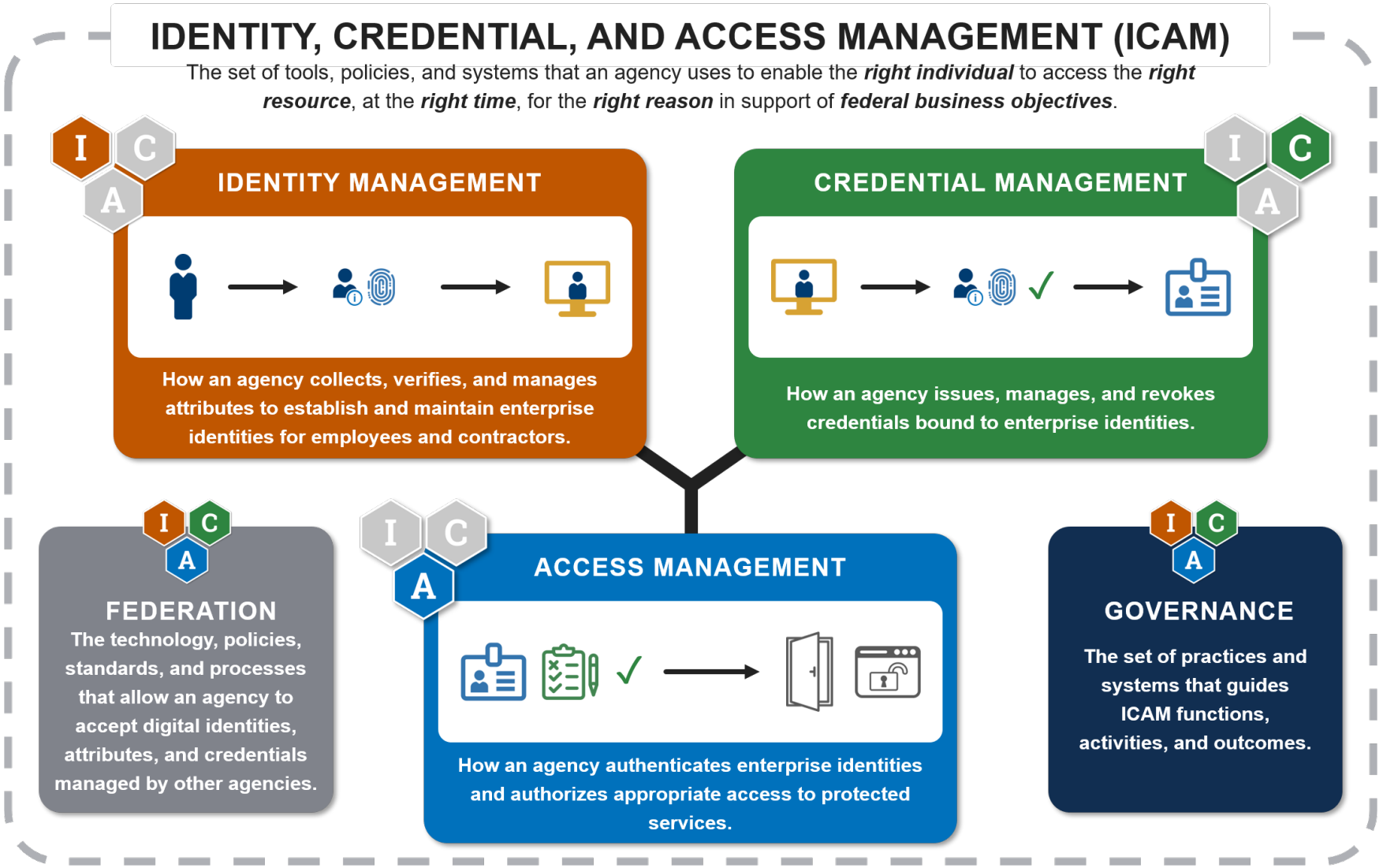
Operational Capability

Building single identity platform capability across networks

Singular identity instance enables federation and single view of a user's profile

Provides capability to automate provisioning and de-provisioning users from systems

ICAM Services Framework



Source: Federal ICAM Architecture, 30 Jun 2023

Capabilities and Readiness

Seamless and Secure Access

- Sign-On
- Faster access

Trust and Confidence

- Right access, right reason
- Enterprise solution



Consistent User Experience

- Unified login interface
- Reduced lockouts

Promotes Efficiency

- Right access, right time
- Reduced Help Desk tickets
- Automatic deprovisioning

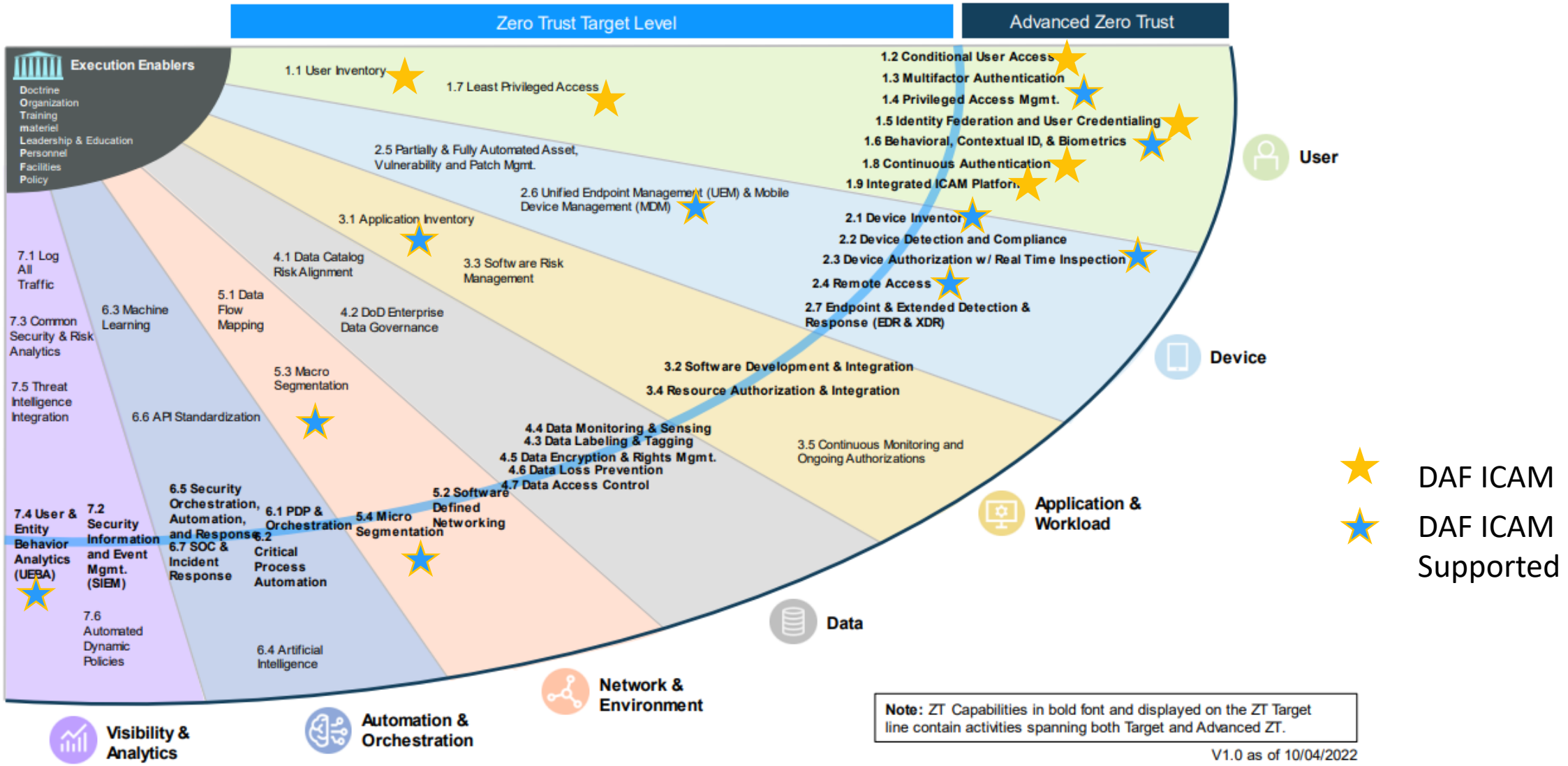
Enhanced Security

- Stronger authentication
- Right access, right entity

Personalized Experience

- Self-service capabilities
- Role-based and attribute-based access

DAF Zero Trust Integration



Identity Vetting and Authentication Pathways

DEERS Enrollment & RAPIDS

Foundational identity database and terminal interface used to verify eligibility and biometrics.

login.gov

Secure, centralized login service used for non-DoD or public-facing federal systems.

Common Access Card (CAC)

Physical smart card embedded with PKI cryptographic certificates for Multi-Factor Authentication access.

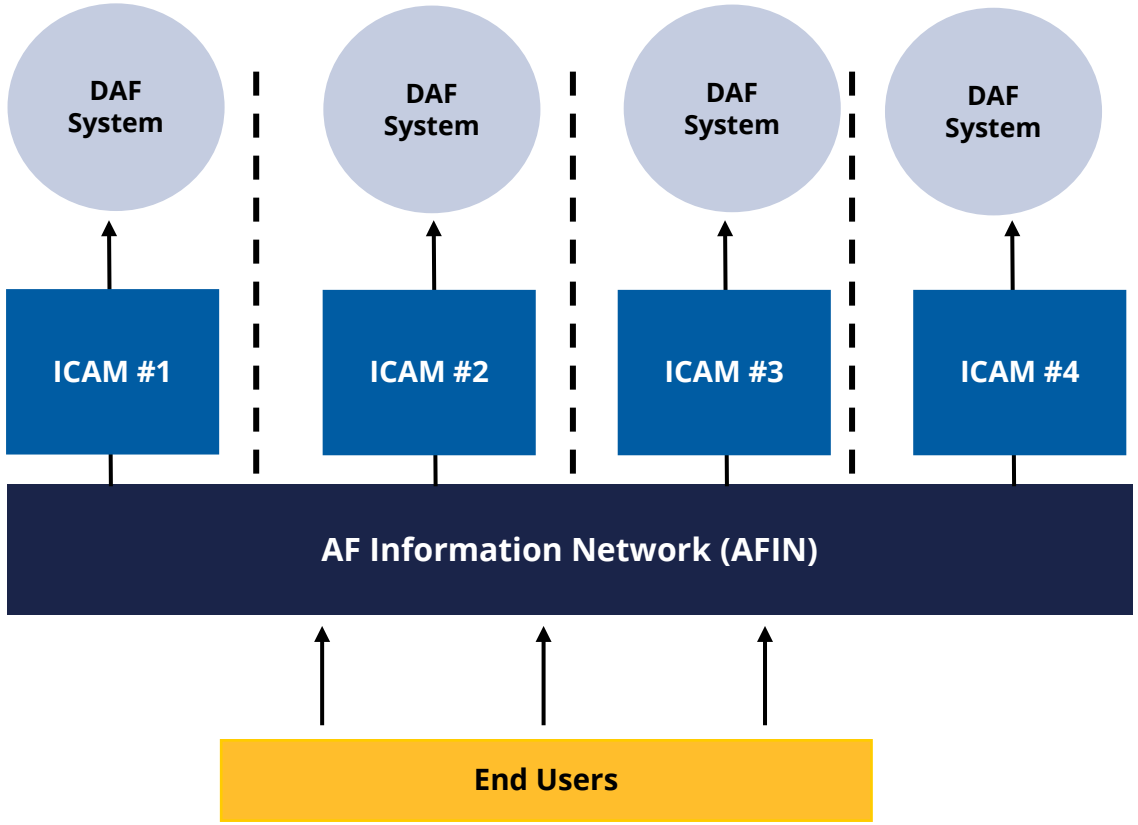
myAuth

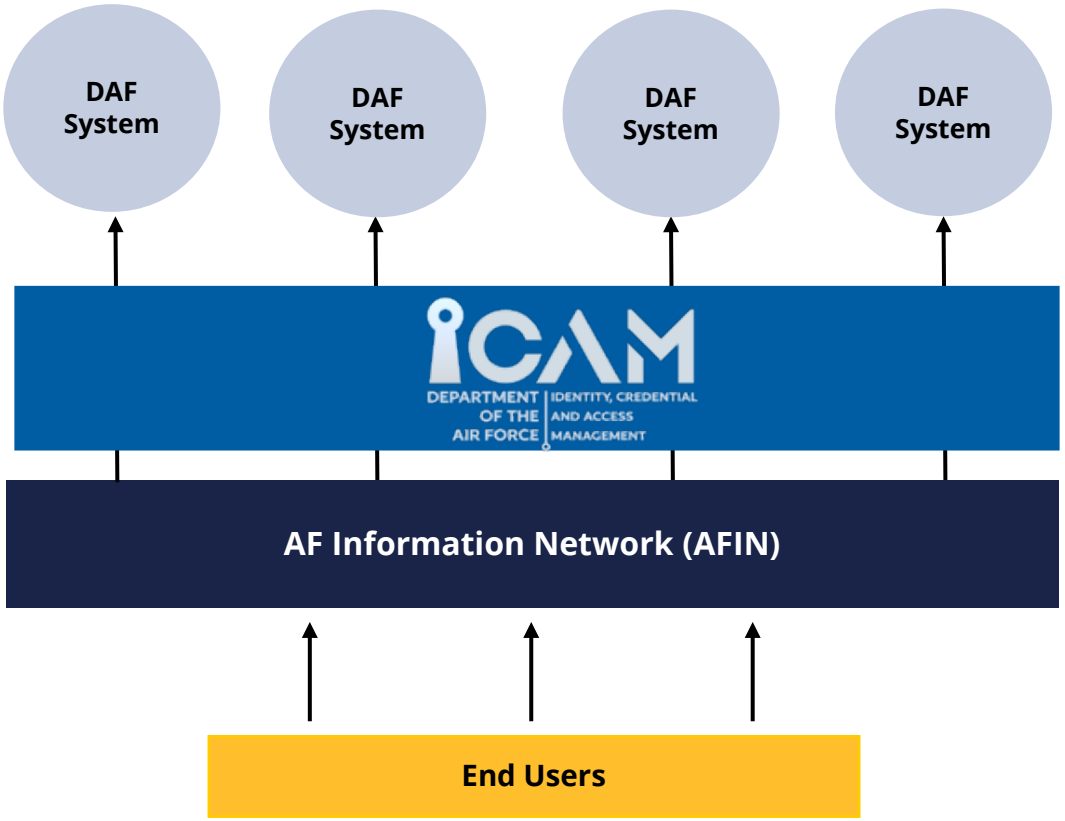
DMDC-managed login portal consolidating legacy systems into a secure entry point.

Fastpass

Okta's phishing-resistant, device-level Multi-Factor Authentication (MFA) client.

End State





Current State → End State

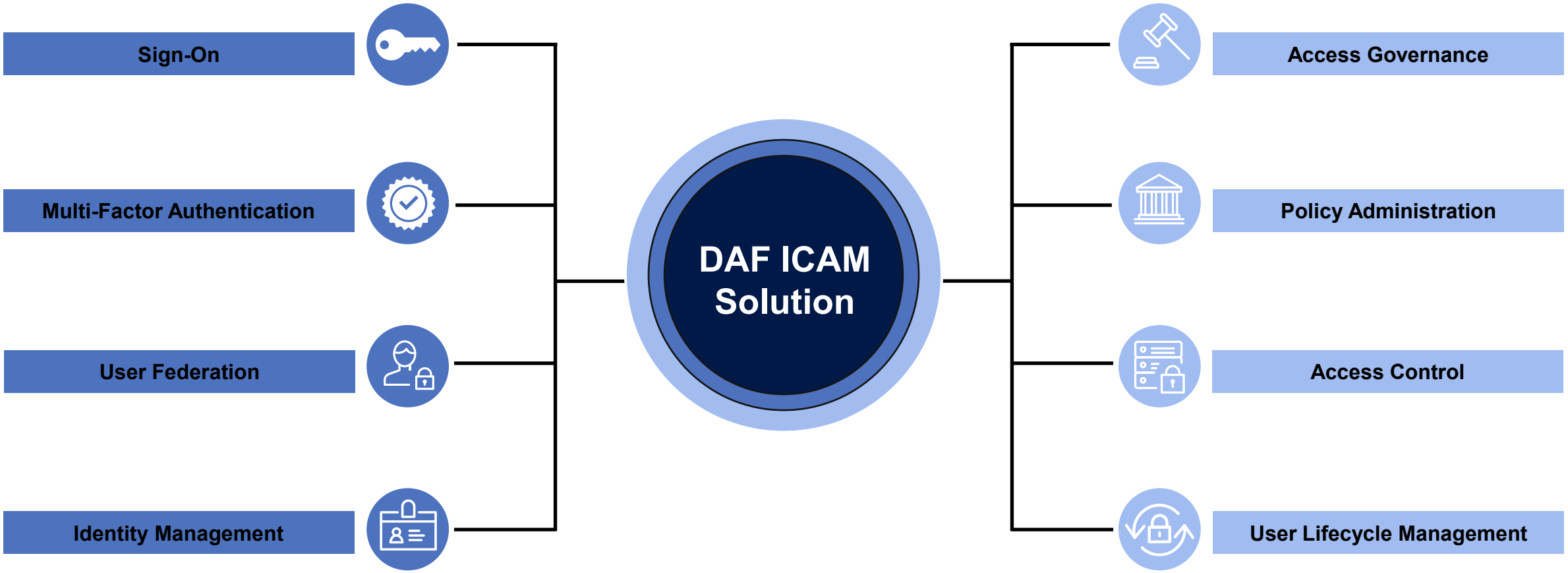
The Solution

Identity Provider (IdP)

okta

Proves who you are

- Sign-On
- Multi-Factor Authentication
- User Federation
- Identity Management



Identity Governance & Administration (IGA)

SailPoint

Manages what you can access

- Access Governance
- Policy Administration
- Access Control
- User Lifecycle Management

Enablement



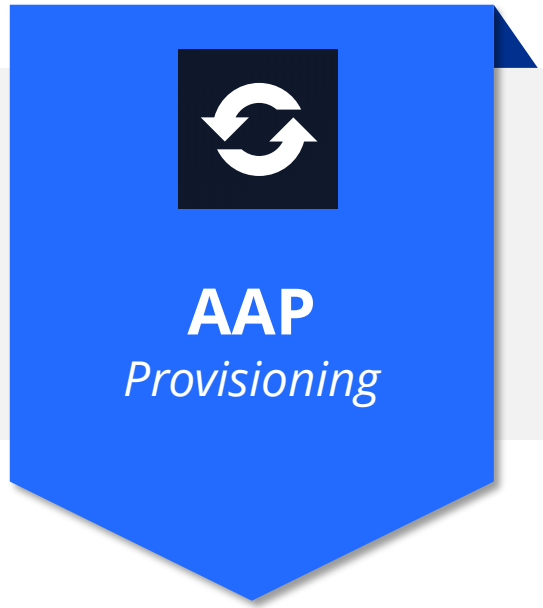
IdP
Authentication

Verification – Identity verification using DoW PKI or approved MFA solution



IGA
Authorization

Lifecycle Management – Policy driven SAAR, provisioning, and recertification campaigns



AAP
Provisioning

AAP Enforcement – Automates secure downstream account provisioning at local systems

Future Capabilities

NPE

Non-Person Entity

Robust governance, lifecycle management, and secure authentication for NPEs through a phased implementation approach

CDOL

Contested, Degraded, and Operationally Limited

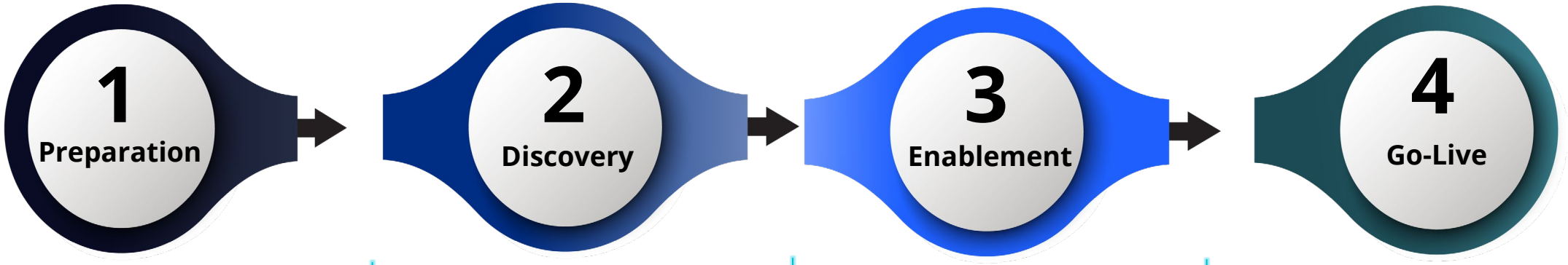
Extending secure ICAM capabilities to Denied, Disrupted, Intermittent, and Limited (DDIL) environments

ITP

Identity Threat Protection

Leveraging behavior heuristics and cyber threat intelligence to automatically detect and block anomalous and malicious activity

Enablement Process



- ✓ Complete Registration, Enablement Questionnaire, and Memorandum for Record (MFR)
- ✓ DAF ICAM hosts Discovery Session to review use cases, integration patterns, and enablement timeline
- ✓ Integration activities and UAT
- ✓ Application prepares users for go-live and DAF ICAM deploys application to production

System Owners: Visit the DAF ICAM SharePoint site and submit your initial registration to receive the Enablement Questionnaire

Functional Leaders & End Users: Support Enablement - Champion the adoption of the enterprise solution within your directorate

Call to Action



View our Resources

View our website: https://usaf.dps.mil/sites/DAF-ICAM/

Please refer to the About ICAM, Getting Started, Enablement Process, and User Support pages for relevant resources related to DAF ICAM

Registration

Navigate to the website and select the “Register” button to register for the application onboarding process

Prepare for ZT Migration

See ZT.AF.MIL for further details

Acronyms

- AAP – Automated Account Provisioning
- CDOL - Contested, Degraded, and Operationally Limited
- DAF – Department of the Air Force
- DoW – Department of War
- ICAM – Identity, Credential and Access Management
- IdP – Identity Provider
- IGA – Identity Governance & Administration
- NPE – Non-Person Entity
- PKI – Public Key Infrastructure
- SAAR - System Authorization Access Request
- SOD – Segregation of Duties
- ZT – Zero Trust