

Okta for US Military

Accelerate mission with modern, Zero Trust Identity

DISA Technical Exchange Meeting (TEM)

Agenda



Ken Parrotte
Federal Sales Manager
DISA/4e



Tyler Briley
Sr. Systems Engineer
DoD

01 Introduction to Okta DISA Team

02 Okta in DoD Overview/Update

03 Demonstration

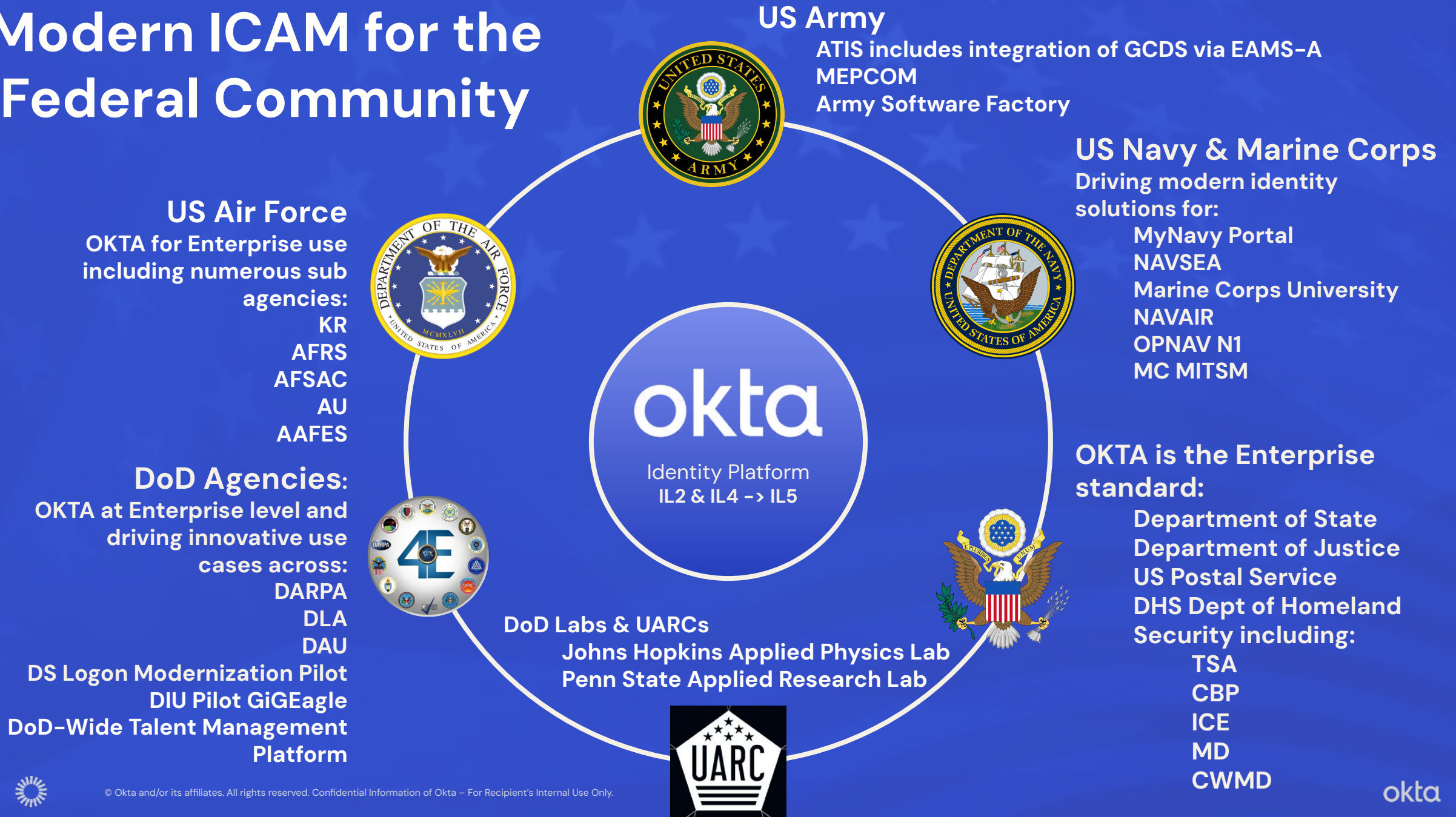


Our Value Proposition

Accelerate missions with modern, Zero Trust identity.



Modern ICAM for the Federal Community



Identity as a Service

Right Access, Right Time, Right Context.

ICAM for Every Use Case

okta

Identity
Platform

IL2 & IL4 → IL5

Employees &
contractors



Community
Members



Non-Person Entities



Infrastructure
(Cloud/On-Prem)



Applications
(Cloud/On-Prem)



APIs
(Public/Private)



Access
Gateway



Single
Sign-On



Adaptive
MFA



Lifecycle
Management



API Access
Management



Seamless
Integrations



Universal
Directory



Advanced
Server Access

What Okta offers “Defense in depth”

First line of defense – **Policies**

- Sign on policies: Manage and restrict access
- Enrollment and recovery policies

Second line of defense – **Authenticators**

- Hardware-backed, phishing-resistant authenticators

Third line of defense – **Contextual Access**

- Device (MDM & EDR) signals
- Device assurance checks
- Location / network zones, ThreatInsight
- Risk signals, behavior detection

Fourth line of defense – **Observability**

- Logging, reporting, and auditing
- Security workflow templates



Okta's FastPass Assertions on our journey toward AAL3 Accreditation

A SECURE ALTERNATIVE CREDENTIAL TO THE CAC

Phishing Resistance

FastPass performs origin binding and has been penetration tested against common phishing tactics

Multifactor

FastPass attests possession and inherence or knowledge as a second factor

Cryptographic Device

FastPass uses hardware backed TPM stores for all cryptographic functions

Realtime Device Posture Evaluation and is Platform Independent, in order to assist organizations in implementing a Zero Trust architecture.



ASSESSOR'S REPORT

Okta FastPass

June 5, 2024

Kuma, LLC, a global cybersecurity and audit firm, has assessed Okta's FastPass solution based on various identity, security and privacy frameworks and the statement of work executed between Kuma and Okta. The assessment was conducted between April 1, 2024, and June 5, 2024.

The Okta FastPass solution is a cryptographic multi-factor authenticator that provides passwordless authentication to any SAML, OIDC, or WS-FED applications in Okta.

In the course of our assessment, Kuma reviewed and tested the Okta FastPass solution including:

- Organizational controls, policies, and procedures
- Data and information security and privacy policies
- Data flows, User Journey's and overall Testing of the FastPass technical architecture and platform

Based on the information received from Okta throughout the course of the assessment, this letter provides reasonable assurance that Okta has designed and implemented appropriate safeguards and controls that allow Okta FastPass to be phishing resistant and align with NIST 800-63-3 AAL-2 and 3; as well as the draft guidance around NIST 800-63-4.



Enterprise



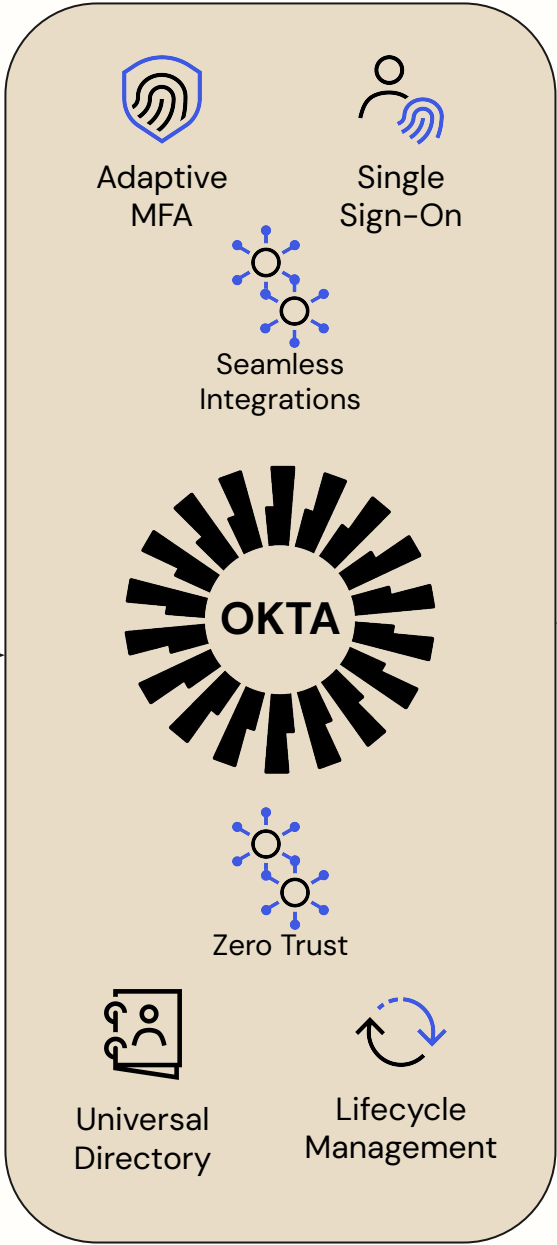
Public Clouds
(GOV Cloud)



Hybrid
Cloud



On-Premise
Data Center



1. Pre-Deployment

Forward deploy identities and attributes from Okta's Enterprise ICAM to support DDIL and Tactical Edge

2. Deployed & Connected

Two-way sync while connected. Local IAM stack integrated with Okta. Local Federation Service forwards authentication requests to Okta while connected

3. Disconnected

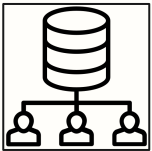
Cache changes while disconnected and authentication using local IAM stack

4. Re-Connected

Policy based one-way/two-way synchronization. Rapid turnaround for next mission.

Tactical Edge

Local Identity Management Stack



Local Directory Store



Local Federation Service





Demonstration