Cryptologic and Cyber Systems Division

OVERALL BRIEFING IS UNCLASSIFIED

Someone Scraped My Identity! Is There a Doctrine in the House?

AF Identity, Credential, and Access Management (ICAM)

August 2018

Mr. Richard Moon, GG-14
Ms. Andrea Kunz, MITRE
AFLCMC/HNCDI

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited. Other requests for this document shall be referred to AFLCMC/HNC, 230 Hall Blvd. Bldg 2028, San Antonio, TX 78243.

Overview

- BLUF
- Federal ICAM Services Framework
- ICAM Components
- ICAM Capability Example – PKI
- ICAM Capability Areas & Gaps
- Summary

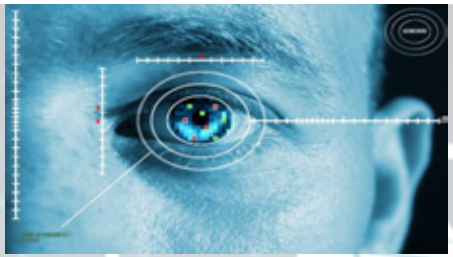
UNCLASSIFIED

BLUF

- **Problem:**
  Weak identity verification and inadequate data protection puts our people, networks, and data at risk of exploit
- **Current State:**
  AF has solutions in place but they need to be strengthened and support increasingly diverse operating environments
- **Future State:**
  An Identity Credential and Access Management (ICAM) strategy to evolve the AF

Authentication Technologies

RSA Token



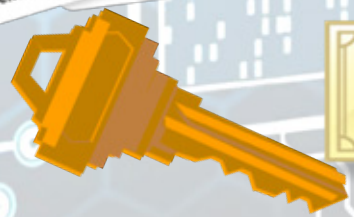
fido alliance

Yubikey

SafeNet Token

One-Time Password

OASIS



UNCLASSIFIED

ICAM

- **What Is ICAM?**

  "*the set of security disciplines that allows an organization to enable the right individual to access the right resource at the right time for the right reason*"[1]

- ***Is*** **There a Doctrine In The House? Yes.**

  – ***Federal ICAM Roadmap and Implementation Guidance, Dec 2011***

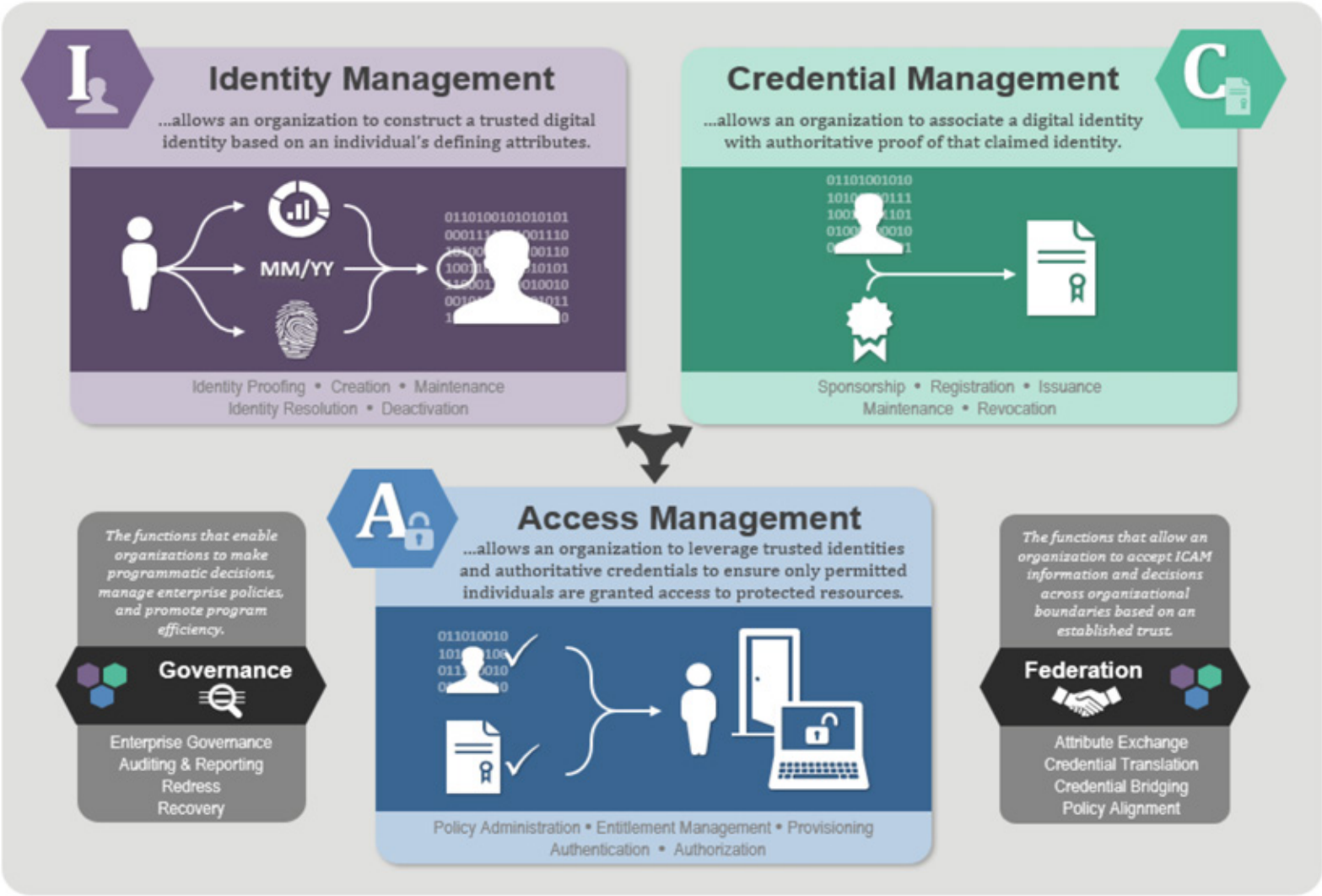
  – ***DoD ICAM Strategy (final draft)***

  – ***NIST SP 800-63, Digital Identity Guidelines, Dec 2017***

  – ***Air Force Manual 17-1304, AF ICAM (draft)***

[1] – *Federal ICAM Architecture*

Federal ICAM Services Framework



Source: Federal ICAM Architecture and is current as of 26 Jun 18

UNCLASSIFIED

ICAM Landscape – Identity

Source: Federal ICAM Architecture and is current as of 26 Jun 18

- **Identity Life Cycle**
  - Establish identity using trusted evidence
  - Create identity account
  - Provision account with required attributes
  - Update identity account over lifecycle
  - De-provision and delete identity
- **Governance:**
  - NIST SP 800-63, Digital Identity Guidelines
  - NIST SP 800-63A, Enrollment and Identity Proofing
  - Air Force Directory Services External Data Dictionary

UNCLASSIFIED

Identity Attributes

Air Force Directory Services

USAF

- Auth Src 1
- Auth Src 2
- Auth Src 3
- Auth Src 4
- Auth Src 5
- Auth Src 6

DoD

- Auth Src 7
- Auth Src 8
- Auth Src 9

Authoritative Attribute Data Sources

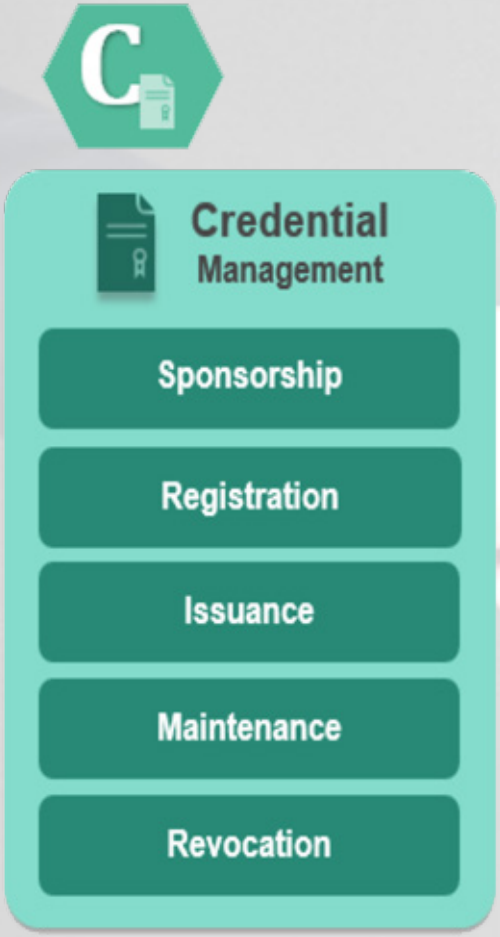
Harvest Authoritative Data

Auth Src 1	Auth Src 1	Auth Src 2	Auth Src 7	Auth Src 4	Auth Src 7	Auth Src 5
Rank	Name	IA Date	Citizenship	E4C Email	EDIPI	Duty Phone
Gen	Washington, George	2010119	US	george.washington@us.af.mil	0000000001	596-2304

Digital Identity Record

UNCLASSIFIED

ICAM Landscape – Credential



Source: Federal ICAM Architecture and is current as of 26 Jun 18

- **Credential Life Cycle**
  - Establish sponsor need for user credential
  - Register user in identity database
  - Issue credential
  - Maintain credential for required duration
  - Revoke credentials and add to revocation list
- **Governance:**
  - DoDI 8520.03, Identity Authentication for Information Systems
  - NIST SP 800-63, Digital Identity Guidelines

UNCLASSIFIED

ICAM Landscape – Access

Source: Federal ICAM Architecture and is current as of 26 Jun 18

- **Access Management is the set of practices and services for ensuring only those with proper permissions can interact with a given resource**
  - **Access Control policies at all levels govern requirements for access**
  - **Authentication verifies that a claimed identity is genuine based on valid credentials**
  - **Authorization is the decision to grant or deny access to a resource based on policy**

Authentication – Validating Identity

- **Three Authentication Factors**
  - *Something you know (e.g., password, PIN)*
  - *Something you have (e.g., ID badge)*
  - *Something you are (e.g., fingerprint)*
- **Authentication Frameworks**
  - Current: Active Directory / PKI
  - Emerging:
    - Fast Identity Online (FIDO)
    - OAuth – OpenID Connect
- **Governance:**
  - DoDI 8520.02, Public Key Infrastructure & Public Key Enabling
  - NIST SP 800-63B, Authentication & Lifecycle Management

UNCLASSIFIED

Authorization – Access Decision

- Access control policies define who / what may act upon a resource
- The authorization service validates identity attributes to ensure the claimant is allowed to access a resource
- Authorization Frameworks
  - Current:
    - Active Directory / Role-Based
    - Common Computing Environment (CCE) / Global Content Delivery Service (GCDS)
  - Future: Attribute-Based / Enterprise Level Security
- Governance:
  - Enterprise Identity Attribute Service (EIAS)
  - Air Force Directory Services External Data Dictionary

ICAM Capability Example – PKI

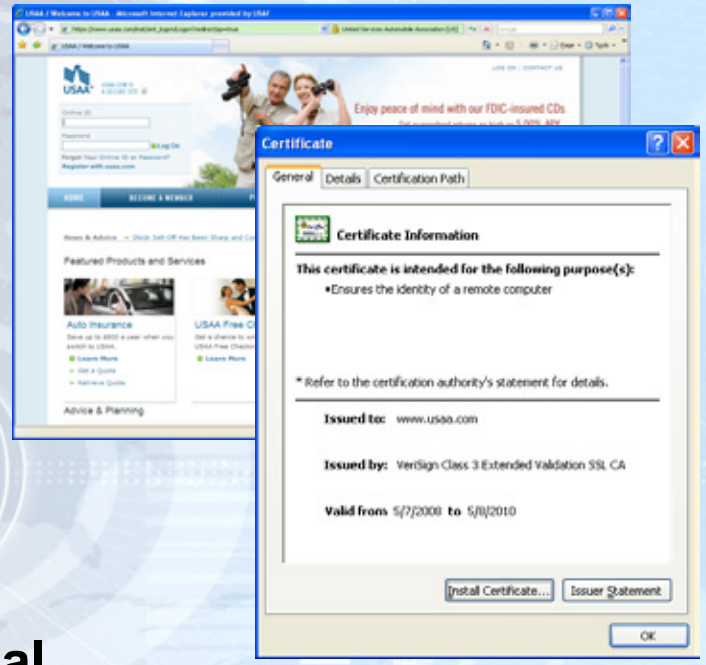
- **PKI – framework for trust within an environment**

- **PKI issued certificate credential *digitally binds user's identity* to their public key**
- **Certificate *credential* stored on the CAC used to assert identity during *authentication***
- **Identity assertion used to verify attributes prior to *authorization decision***

CAC Not Going Away

- Public Key technology is used EVERYWHERE
- Large infrastructures exist
  - Department of Defense
  - Federal Government
  - Foreign Governments (i.e., Asia)
- Policies mandate its use
  - HSPD 12
  - DoD Directives
  - Health Insurance Portability and Accountability Act (HIPAA)
- CAC is the anchor for logical & physical access within DoD for foreseeable future

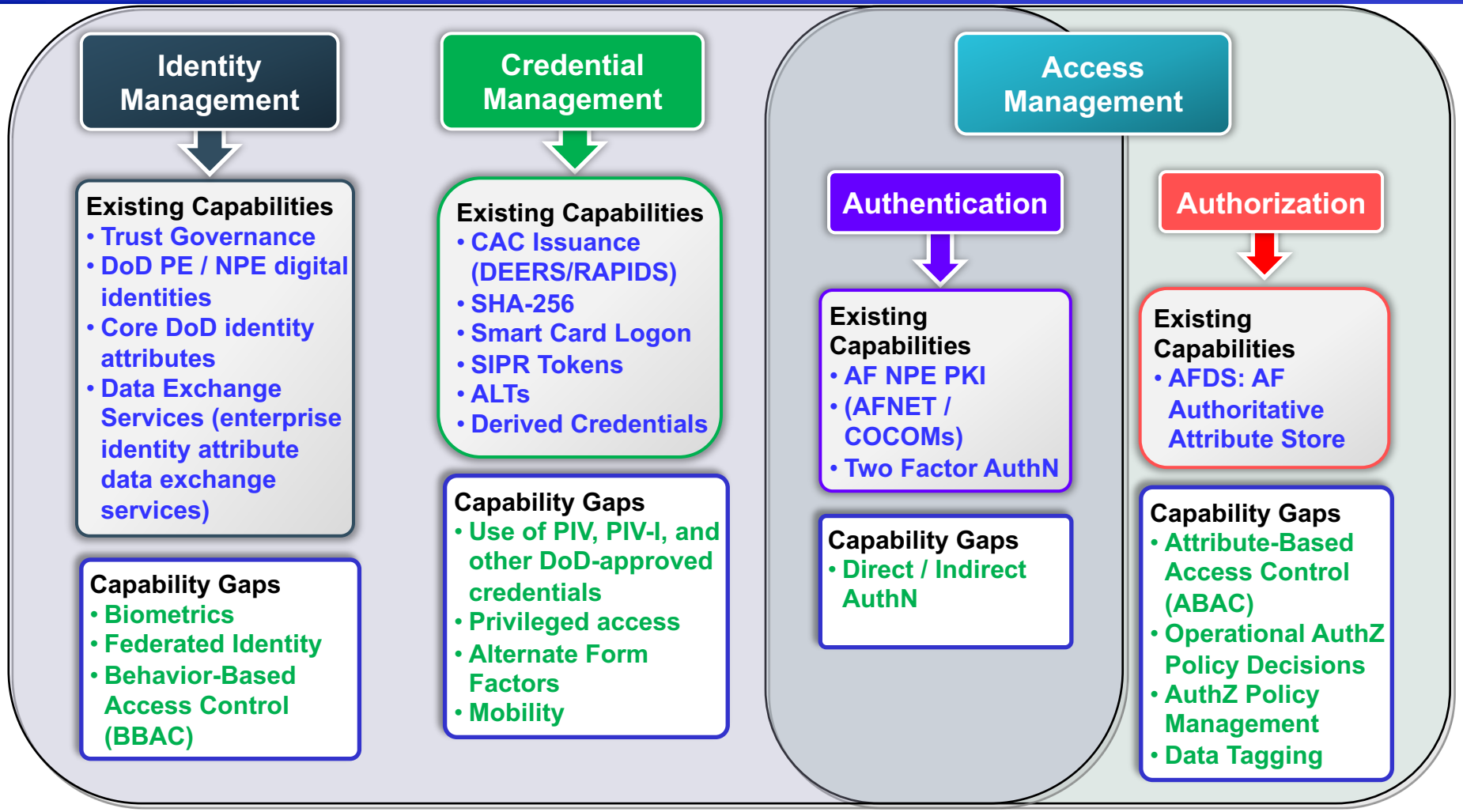
Primary DoD-approved Credential



CAC ENABLES us to use other form factors for mobile and tactical environments!

UNCLASSIFIED

ICAM Capability Areas & Gaps



UNCLASSIFIED

Summary

- AF – partner in DoD ICAM evolution
  - Working to address mission needs
  - Close capability gaps
- Standards-based approach for interoperability
- Future of authentication: bring your own device?
- Find more and better ways to provide
  - secure access
  - assured identities
  - defense against unauthorized entities

… and make ICAM work for you!

For more information, contact the Air Force PKI Help Desk at

Commercial: (210) 925-2521

DSN: 945-2521

afpki.helpdesk@us.af.mil

UNCLASSIFIED

Sources

- Federal Identity, Credential, and Access Management (FICAM) Architecture
- DoD Cybersecurity Discipline Implementation Plan, Feb 2016
- DoD IdAM Portfolio Description v2.0, Aug 2015
- DoDD 8521.01E, DoD Biometrics, Aug 2017
- DoD Identity and Access Management (IdAM) Strategy v1.0, Nov 2014
- DoDI 8500.01, Cybersecurity, Mar 2014
- DoDI 8520.02, Public Key Infrastructure and Public Key Enabling, May 2011
- DoDI 8520.03, Identity Authentication for Information Systems, May 2011
- NIST SP 800-63, Digital Identity Guidelines, Dec 2017

UNCLASSIFIED