DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

Innovations in Identity & Access Management (IdAM)

Lee Taylor
Chief, Infrastructure Applications Branch

Disclaimer

The information provided in this briefing is for general information purposes only. It does not constitute a commitment on behalf of the United States Government to provide any of the capabilities, systems or equipment presented and in no way obligates the United States Government to enter into any future agreements with regard to the same. The information presented may not be disseminated without the express consent of the United States Government.

Topics

- Overview of IdAM
- Current Architecture
- Recent IdAM Enhancements
- IdAM Roadmap

Identity & Access Management (IdAM)

What is IdAM?

IdAM is a combination of technical systems, policies, and processes that create, define, and govern utilization/safeguarding of identity info.

IdAM solutions are divided into three distinct areas

- Management of Digital Identities
- Authentication of Users
- Authorizing Access to Resources

DoD IdAM

Who provides Enterprise IdAM?

The Defense Information Systems Agency (DISA), Defense Manpower Data Center (DMDC), and the National Security Agency (NSA) combine resources to provide IdAM solutions to the Department of Defense.

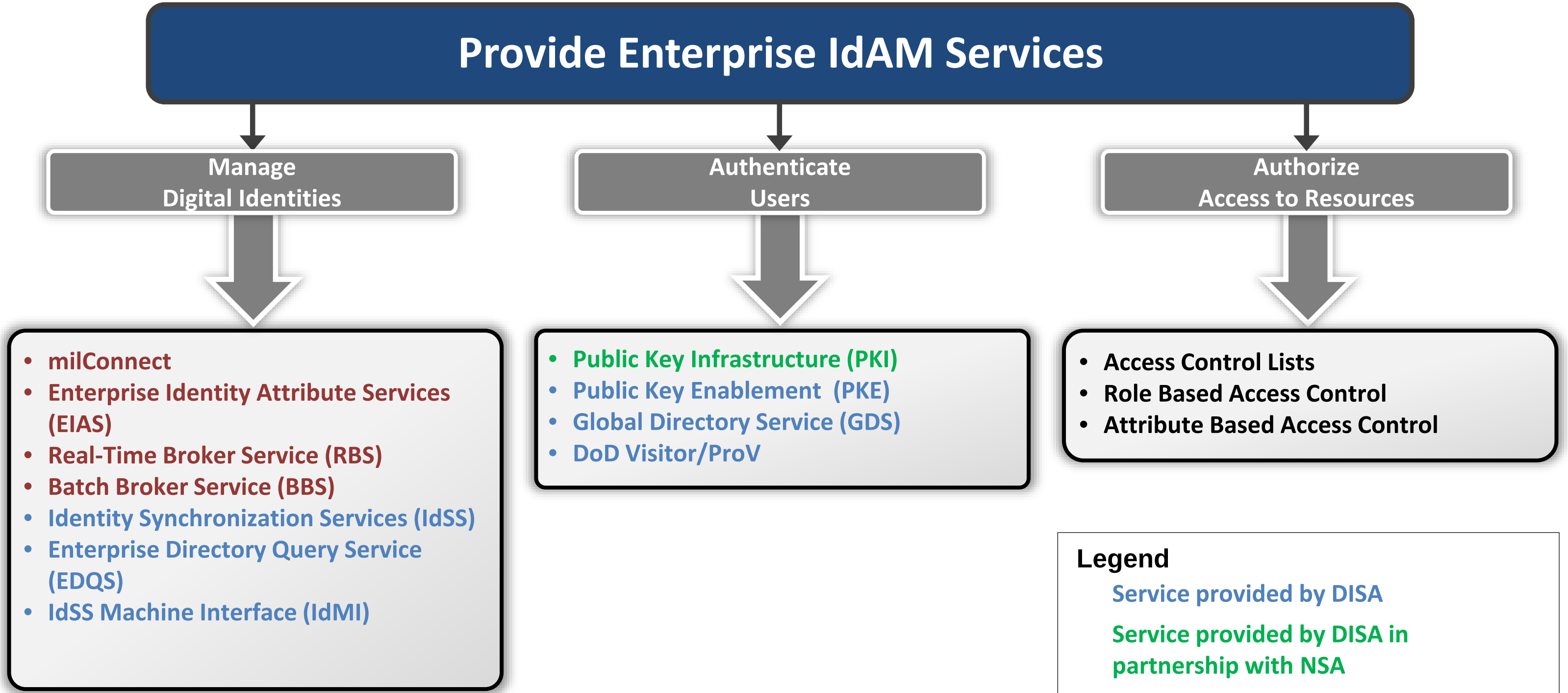
Why Do We Have it?

DISA provides IdAM for Enterprise Services as the security discipline that enables the right individuals to access the right resources at the right times for the right reasons.

Policy and Guidance

Developed by DoD CIO in coordination with DISA and DMDC;
Mandates usage of some enterprise IdAM services and defines relevant processes and procedures.

IdAM Portfolio High-Level Capability Model



Provide Enterprise IdAM Services

Manage Digital Identities

- milConnect
- Enterprise Identity Attribute Services (EIAS)
- Real-Time Broker Service (RBS)
- Batch Broker Service (BBS)
- Identity Synchronization Services (IdSS)
- Enterprise Directory Query Service (EDQS)
- IdSS Machine Interface (IdMI)

Authenticate Users

- Public Key Infrastructure (PKI)
- Public Key Enablement (PKE)
- Global Directory Service (GDS)
- DoD Visitor/ProV

Authorize Access to Resources

- Access Control Lists
- Role Based Access Control
- Attribute Based Access Control

Legend

Service provided by DISA

Service provided by DISA in partnership with NSA

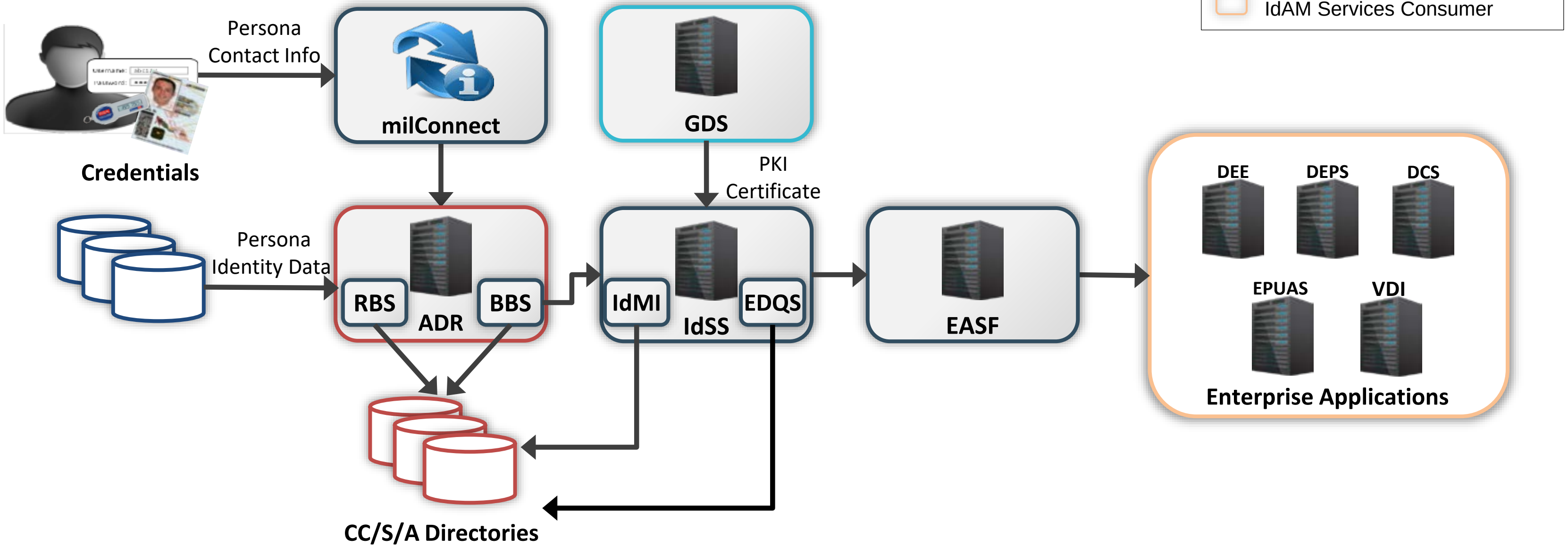
Service provided by DMDC

Service provided at system level

Current EDS Architecture

Legend

- □ Identity Service
- □ Authentication Service
- □ Authorization Service
- □ Service External to IdAM
- □ IdAM Services Consumer



Recent IdAM Enhancements

Privileged Users

Implemented Enterprise Privileged User Authentication Service (EPUAS), to provide Public Key Infrastructure (PKI) certificate based two factor authentication for privileged user access to DISA hosted computing workload.

Provisioning

EDS provisioning updates to support EPUAS and Virtual Desktop Infrastructure (VDI).

Directory Sharing

Piloting replication of directory information among Multi-National Mission Partners.

IdAM Road Map

FY- 2018

- Assured Identity Pilot
- Pure Bred Mobile Security Credentials
- Conditional attributes to reduce PII proliferation

FY- 2019

- Develop attributes for the Unified Capabilities effort
- Certificate Reduction

FY- 2020

- Certificate Transparency
- Global Force Management Data Initiative (GFMDI) organization server as a feeder to DMDC's Person Data Repository (PDR) and Enterprise Identity Attribute Service EIAS

IdAM Innovations

Pure Bred Mobile Security Credential

- Derived Credentials
- Comprised of a key management server and set of apps
- Separates key management from device management

Assured Identity

- Types of Authentication
- Biometrics and its uses
- Constructing an Assured Identity

Types of Authentication

Accepting proof of identity

- Trusted Verifier - credible person with first-hand evidence the identity is genuine
- PGP (pretty good privacy), public certificate authorities, peer-based trust

Comparing the attributes

- Compare object itself against what is known about objects of that origin
  - Currency, financial instruments, watermarks, holographic imagery

Documentation and External Affirmations

- Certificates of authenticity, evidence log, key card, trademark

Biometrics and its uses

What are Biometrics?

Metrics related to human characteristics

Computer Science/Security uses:

- Form of ID
- Access Control

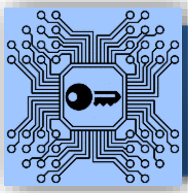
Physiological (shape of the body)

Examples include: fingerprint, palm veins, face recognition, palm print, hand geometry, iris recognition, and retina

Behavioral (patterns of behavior)

Including typing rhythm, gait, and voice

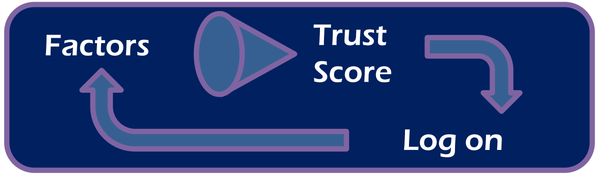
Constructing an Assured Identity



Key burned into the hardware provides a root of trust for sensor data

Continuous multifactor authentication constantly verifies identity

- Facial Recognition
- Gait
- Voice
- Peripherals
- GPS
- Device Orientation
- Network



Factors

Trust Score

Log on

Questions?

rate us

take the **3-question** survey
available on the AFCEA 365 app

visit us

DISA Booth # **443**

follow us

Facebook/USDISA

Twitter/USDISA

www.disa.mil

DISA

DEFENSE INFORMATION SYSTEMS AGENCY

The IT Combat Support Agency

www.disa.mil **/USDISA** **@USDISA**