

# DoD Identity & Access Management (IdAM) Portfolio Overview

---

**DISA Enterprise Services Directorate (ESD)**

**17 July 2013**



Overview

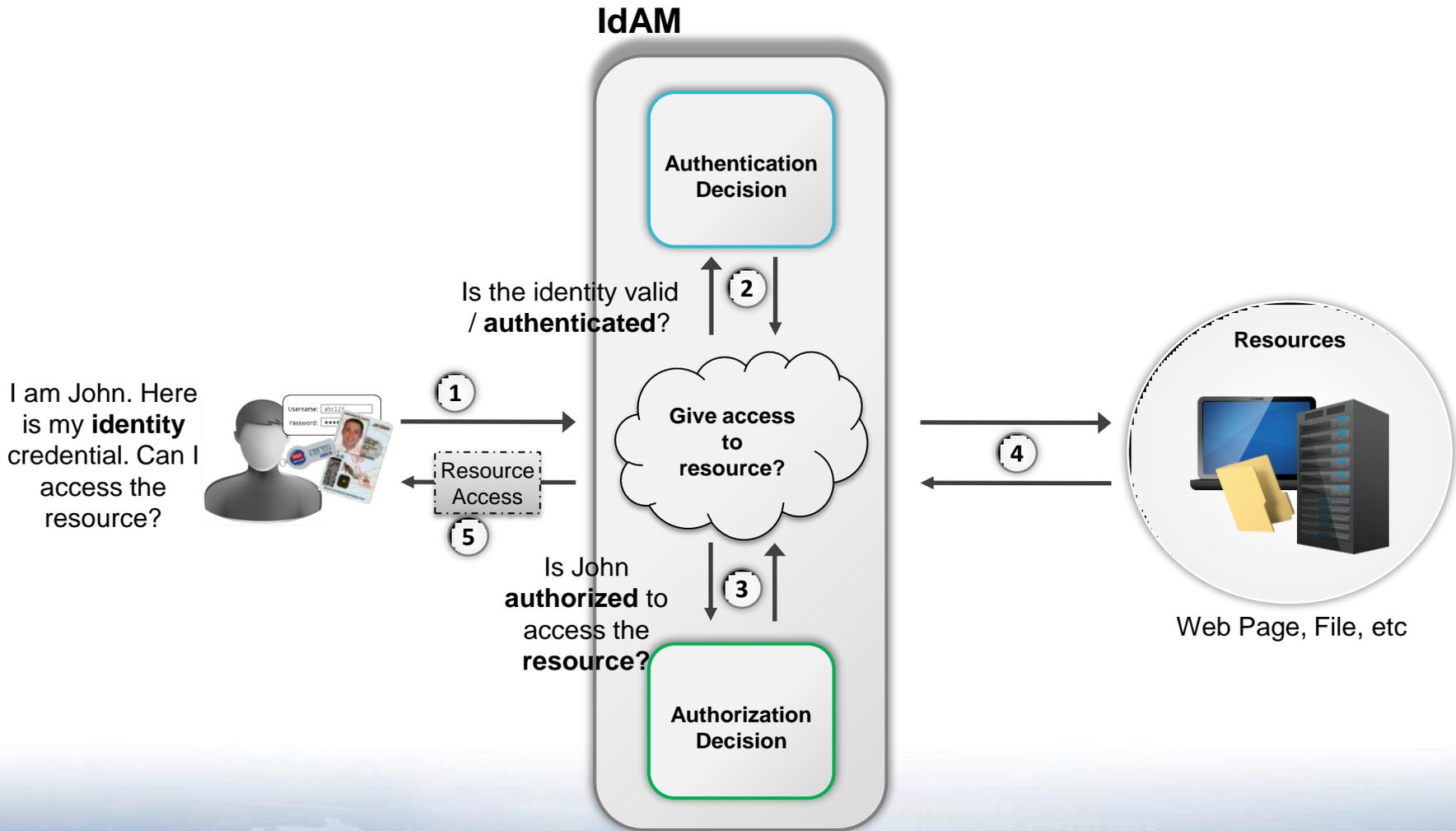
# IdAM Concepts & IdAM Portfolio



# IdAM Overview

- **Identity and Access Management (IdAM)** is the combination of technical systems, policies and processes that create, define, and govern the utilization and safeguarding of identity information, as well as managing the relationship between an entity and the resources to which access is needed.
- IdAM can be divided into three fundamental capabilities: Manage Digital Identities, Authenticate Users, and Authorize Access to Resources.
- **IdAM supports the warfighter by creating assured identity and access management services for the DoD Enterprise.**

# IdAM in a Nutshell



- **Digital Identity:** the electronic representation of an individual's identity
- **Authentication:** process of verifying that a claimed identity is genuine and based on valid credentials
- **Authorization and Access:** processes of granting or denying specific requests for obtaining and using information processing services or data

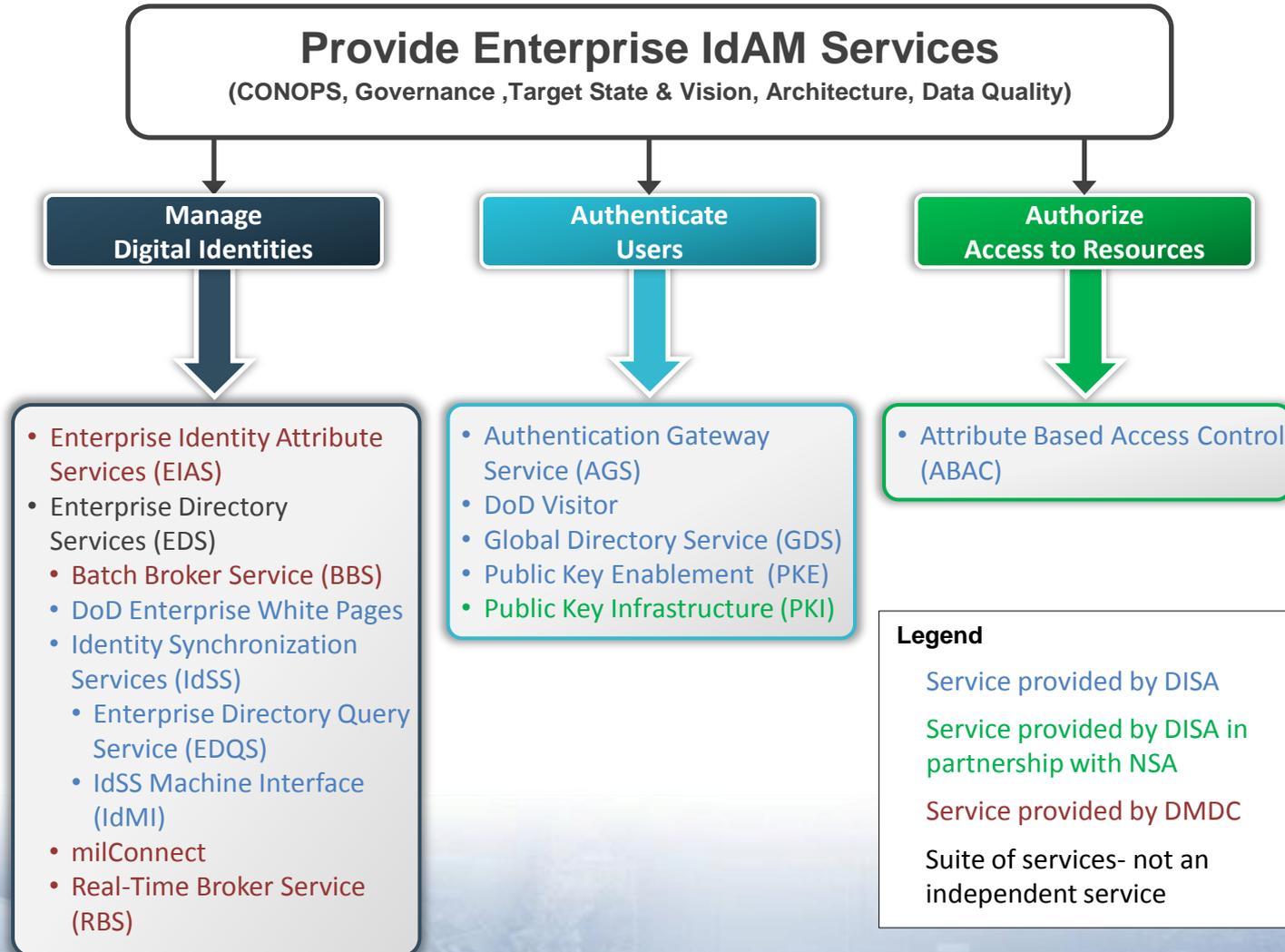
Source: Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, version 1.0, 10 Nov 2009

# IdAM Portfolio

- Joint Defense Information Systems Agency (DISA) /Defense Manpower Data Center (DMDC)/National Security Agency (NSA) organizational construct for managing an array of core material solutions to enable DoD enterprise-wide digital identity, authentication, and authorization capabilities
- Creates a foundation for building a secure and trusted computing environment
- Provides the capabilities for secure enterprise information sharing
- Utilizes account and attribute management services, assured digital identity capabilities, automated account provisioning, and attribute based access control

# IdAM Portfolio

## High-Level Capability Model





Overview

# IdAM Portfolio Activities

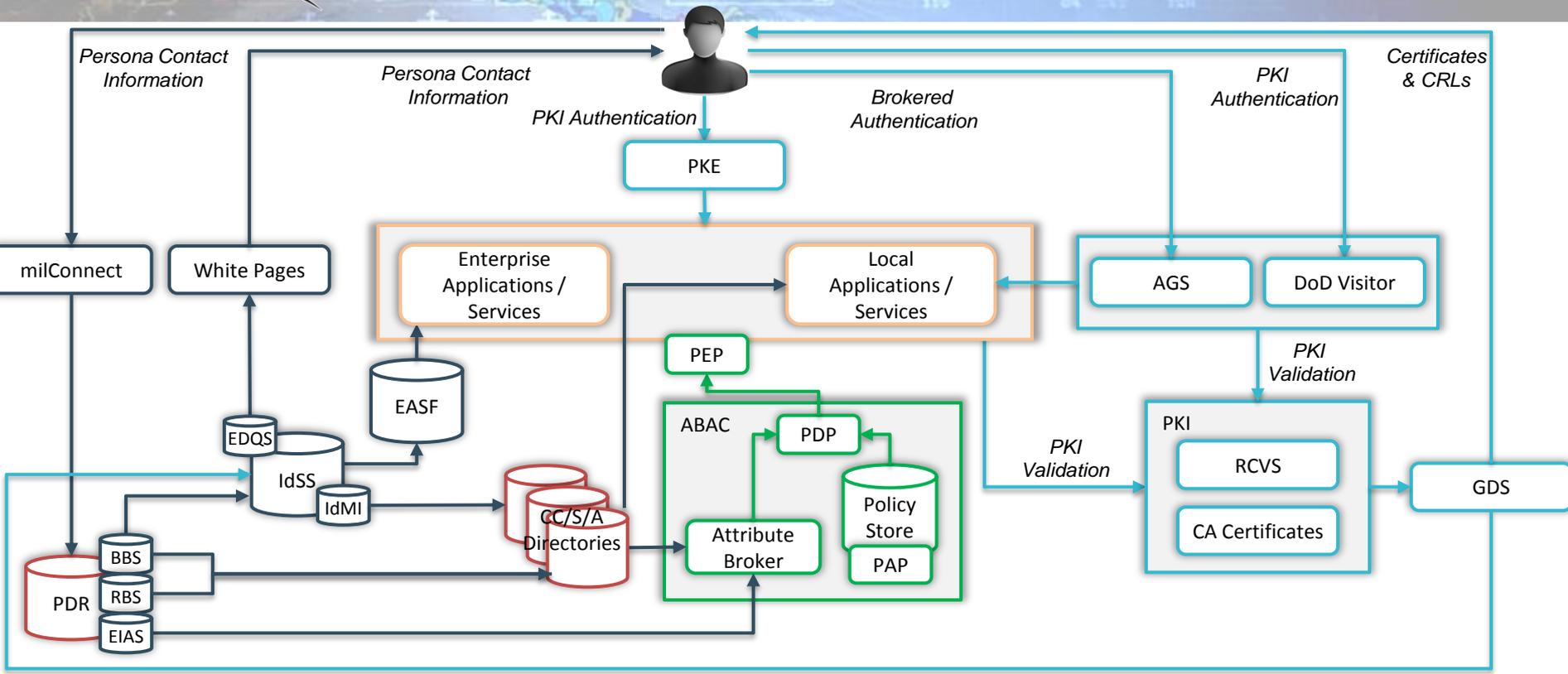


- IdAM Policy and Guidance
  - Developed by DoD CIO in coordination with DISA and DMDC
    - Combatant Commands, Services, and Agencies (CC/S/As) included in review and adjudication
    - Ensures alignment to existing DoD policy and guidance
  - Mandates usage of enterprise IdAM services and defines relevant processes and procedures
- IdAM Services
  - Developed, deployed, and maintained by DISA and DMDC
    - Other entities such as NSA may be included in the fielding process where appropriate
    - Coordination with CC/S/As for requirements development and pilots
  - Services primarily deployed at enterprise level within Defense Enterprise Computing Centers (DECCs)
    - Specific services deployed locally at CC/S/A level (DoD Visitor, AGS)
  - DISA and DMDC coordinate with CC/S/As to integrate IdAM services into local CC/S/A infrastructures

# IdAM Target State & Vision

- IdAM Goals
  - Mission-enabling capabilities: Enterprise User capability “I can go anywhere in the DoD, login, and be productive” – automatic and data driven
  - Security: IT resources protected from inappropriate modification or disclosure and users are able to be held accountable for their actions – automatic and data driven
  - Efficiency: reduce required resources – automatic and data driven
- IdAM Target State Capabilities – used by all DoD IT devices, systems, applications & services on NIPRNET, SIPRNET, and commercial enclaves
  - Same user identifiers, attributes, and credentials used everywhere, managed automatically from accountable data source to consumer
    - Persona-based from DMDC’s Person Data Repository (PDR) and DISA’s Global Directory Service (GDS) for users with DoD PKI credentials
    - Accountable source-based for other users (other federal, coalition, state & local, etc.)
  - Dynamic authentication, authorization and access control
    - Automatic and user data driven (all use cases)
    - Directly or through gateway services
  - DoD-wide people and organization discovery services

# IdAM Portfolio Architecture



**Legend**

- ➔ Identity Information Flow
- ➔ Authentication Information Flow
- ➔ Authorization Information Flow
- ☐ Identity Service
- ☐ Authentication Service
- ☐ Authorization Service
- ☐ Service External to IdAM
- ☐ IdAM Services Consumer

ABAC: Attribute Based Access Control  
 AGS: Authentication Gateway Service  
 BBS: Batch Broker Service  
 CA: Certificate Authority  
 CC/S/A: Combatant Commands/Services/Agencies  
 CRL: Certificate Revocation List  
 EASF: Enterprise Applications Services Forest  
 EDQS: Enterprise Directory Query Service  
 EIAS: Enterprise Identity Attribute Service  
 GDS: Global Directory Service

IdMI: IdSS Machine Interface  
 IdSS: Identity Synchronization Service  
 PAP: Policy Administration Point  
 PDP: Policy Decision Point  
 PDR: Person Data Repository  
 PEP: Policy Enforcement Point  
 PKE: Public Key Enablement  
 PKI: Public Key Infrastructure  
 RBS: Real-time Broker Service  
 RCVS: Robust Certificate Validation Service

# Data Quality Initiative

- The **Data Quality Initiative** is an initiative to improve and maintain the accuracy of enterprise identity and organizational contact information
- Leverages milConnect to provide users with a self-service portal to manage their contact data in DMDC for access via RBS, BBS, and IdSS
- Currently coordinating with CC/S/As to provide DMDC with initial authoritative data
- Currently developing enterprise data specifications, including DoD IdAM Data Dictionary



Overview

# Manage Digital Identities

# Enterprise Identity Attribute Service (EIAS)

- The **Enterprise Identity Attribute Service (EIAS)** distributes DoD person, persona, and personnel attributes to applications and services in a controlled, consistent, and secure manner for making authorization decisions
- Provides ability for relying party to confirm an individual's identity and affiliation to the DoD for the purpose of enabling Attribute Based Access Control (ABAC)
- Provides the capability to cross-reference, share, and distribute the DoD Electronic Data Interchange Person Identifier (EDI-PI) and the DoD Enterprise Username
- Leverages real-time, signed SAML Request/Response
- Available on NIPRNet and SIPRNet

- Suite of services providing authoritative DoD Enterprise organizational and contact attributes
- Consists of:
  - Real-Time Broker Service (RBS)
  - Batch Broker Service (BBS)
  - Identity Synchronization Services (IdSS)
  - Enterprise Directory Query Service (EDQS)
  - Enterprise White Pages
  - milConnect
- Local directories must leverage the provisioning and sync services
- Applications requiring people discovery functions must use EDS as the source for their enterprise directory information

# Real-time Broker Service (RBS)

- The **Real-time Broker Service (RBS)** is a synchronous web service that provides DoD identity and contact data to CC/S/As
- Delivers one record per transaction, customized to the requester
- Useful for integration into applications in lieu of local data store / directory server
- Target response < 2 seconds
- Recommended persona population under 1 million records

# Batch Broker Service (BBS)

- The **Batch Broker Service (BBS)** is an asynchronous web service that provides DoD identity and contact data to CC/S/As
- Can deliver tens of thousands of records per transaction, customized to the requester, for populations in the millions
- Supports local directory provisioning and updating
- Useful for periodically updating large populations
- Provides the largest set of authentication attributes of any EDS service
- Provides DoD dependent and retiree data
- Feeds the Identity Synchronization Service (IdSS)

# Identity Synchronization Service (IdSS)

- The **Identity Synchronization Service (IdSS)** is a DoD Enterprise directory service forest synchronization service
- Connects to accountable identity sources to collect and groom identity information for all CAC holders
  - DMDC Person Data Repository (PDR) for identity data
  - DISA Global Directory Service (GDS) for encryption certificates
- Controls all account creation, deletion, and updates into DISA's Enterprise Application Services Forest (EASF) which is used for DISA-hosted DoD enterprise services (DEE, DEPS, etc)
- Data available for consumption via the IdSS Machine Interface (IdMI) and the Enterprise Directory Query Service (EDQS)

# IdSS Machine Interface (IdMI)

- The **IdSS Machine Interface (IdMI)** provides DoD identity and contact data to CC/S/As from IdSS
- Supports local directory provisioning and updating
- Supports populating Global Address List (GAL)
- Active Directory, LDAP v3, CSV, other formats available
- Available on both NIPRNet and SIPRNet
- No cost for initial connection (both NIPR and SIPR)

# Enterprise Directory Query Service (EDQS)

- The **Enterprise Directory Query Service (EDQS)** provides an LDAP interface to query IdSS data
- Provides flexible integration for applications for identity/authentication in lieu of local directory store
- Currently utilized as data service for DoD Enterprise White Pages
- Fee for service (cost model TBD)

- **DoD Enterprise White Pages** is a website to search for identity and organizational contact information for members of the DoD Enterprise
- Leverages persona-based authoritative data provided by IdSS
- Enables search by an individual's full name, rank, e-mail addresses, and other relevant information
- NIPRNet deployment occurred in April 2013 – <https://www.whitepages.mil>
- SIPRNet deployment planned FY13; Legacy capability provided by JEDS
- No cost enterprise service

- For the purposes of EDS, **milConnect** is a website that allows members of the DoD to access and update their persona contact data
- Designated interface for maintaining DoD person and persona information such as Duty Organization, Job Title, Installation, Address, and Phone Number
- milConnect populates DMDC systems, and, in turn, supports all EDS capabilities
- Keeping persona contact data updated is integral to ensuring local directories, Global Address Lists (GALs), and enterprise applications such as DoD Enterprise White Pages have up-to-date information
- DoD personnel, including DoD contractors, may access milConnect at <https://www.dmdc.osd.mil/milconnect/>
- No cost enterprise service



Overview

# Authenticate Users

- **DoD Public Key Infrastructure (PKI)** is a framework established to issue, maintain, and revoke public key certificates, including systems, processes, and people
- Provides certificates for NIPRNet (DoD Root CA) and SIPRNet (NSS PKI CA) as software certificates or on hardware (e.g., Common Access Card PKI certificates)
- Interoperates with DoD External Certificate Authorities (ECA), federal PIV certificate issuers, selected approved commercial PKI CAs, and selected approved Combined Communications Electronics Board (CCEB) PKI CAs
- No cost enterprise service

# Public Key Enablement (PKE)

- **DoD Public Key Enablement (PKE)** is the process of ensuring that applications can use certificates issued by the DoD PKI, NSS PKI, or DoD-approved external PKIs to support identification and authentication, data integrity, confidentiality, and/or technical non-repudiation
- Common uses include enabling:
  - Smart card logon to DoD networks and certificate-based authentication to systems
  - Secure connections (SSL/TLS) to DoD servers
  - Digital signature and encryption of emails from desktop, web, and mobile clients
  - Digital signature of forms
- No cost enterprise service

- The **Global Directory Service (GDS)** is a DISA-provided enterprise-wide directory service that supports the DOD PKI Program
- GDS is the DoD PKI distribution point for its Certificate Revocation Lists (CRLs) and individual public key email encipherment certificates
- Currently provides a DoD-wide search capability for information (names, e-mail addresses, and public key email encipherment certificates) regarding DoD personnel with a DoD PKI certificate on the NIPRNet and SIPRNet
- No cost enterprise service

- **DoD Visitor** is GOTS software deployed to CC/S/A user-facing MS domain controllers allowing CAC-holding employees temporary access to basic productivity tools while on travel
- Provisions temporary access accounts allowing access to a web browser, Microsoft Office, and local print services at a non-home location
- Files are stored temporarily on the workstation and automatically removed when the user logs off the system
- NIPRNet: CTO 10-116 was released FY12 directing local components to upgrade to latest version of DoD Visitor
- SIPRNet : CTO J3-13-0628 was released in FY13 mandating initial installation of DoD Visitor on SIPRNet
- No cost GOTS software

# Authentication Gateway Service (AGS)

- The **Authentication Gateway Service (AGS)** is an authentication middleware that performs PKI authentication for applications and systems that cannot be directly PK-enabled
- Where possible, DoD components are directed to perform direct PKI authentication using approved PKI certificates; When not possible, AGS provides an alternative for CAC users only
- May be locally deployed or deployed at DECC; any instance must be placed in same logical security boundary as the applications associated with it
- All DoD applications must either become compliant via direct PKI authentication or migrate to the DISA provided service until such time as they are able to become compliant
- Will be deployed into DECC OKC in August for applications located in the same logical security boundary
- AGS is participating in the Google Applications for Government Pilot
- Fee for service GOTS middleware (cost model TBD)



Overview

# Authorize Access to Resources

# Enterprise Attribute Based Access Control (ABAC)

- **Enterprise Attribute Based Access Control (ABAC)** provides authorization decision support for web services, Enterprise Messaging, and internal applications
- Allows Programs of Record to develop custom code for application use
- Open source software available at <https://project.forge.mil/sf/projects/nces>
  - Click on “Documents” at top of page
  - Expand “Open Source Attribute Based Access Control (OS ABAC)” folder
  - Identify most recent version and expand that folder (e.g. “ABAC V1.4”)
  - Expand “UserGuide/Installation/Training” folder and download “OS ABAC Install Guide”
- CC/S/As may deploy locally or utilize DISA-managed service (currently deployed at Columbus and Oklahoma City DECCs)
- No cost GOTS software; Fee for service if utilizing DISA-managed service (cost model TBD)
- DISA also evaluating COTS software for enterprise service

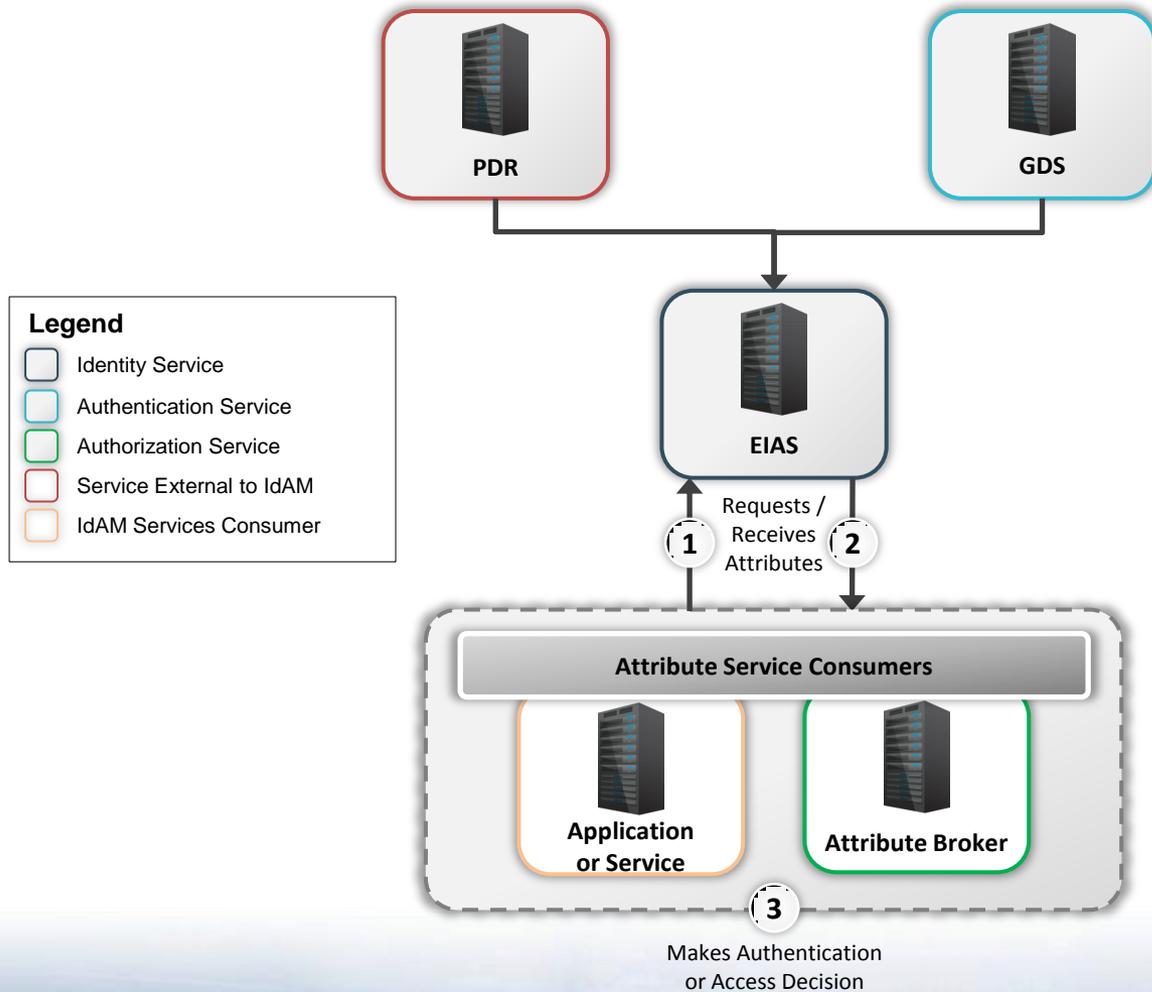
# IdAM Contact Information

- **IdAM Division Chief:** Jackie Huff
  - **IdAM Engineering Chief:** Amanda Cunningham
  - **Enterprise Directory Services Chief:** Lee Taylor
  - **Authentication and Authorization Chief:** Rich Abram
- **IdAM Website:** <http://iase.disa.mil/idam/>
- **Email:** [disa.meade.esd.mbx.idam@mail.mil](mailto:disa.meade.esd.mbx.idam@mail.mil)

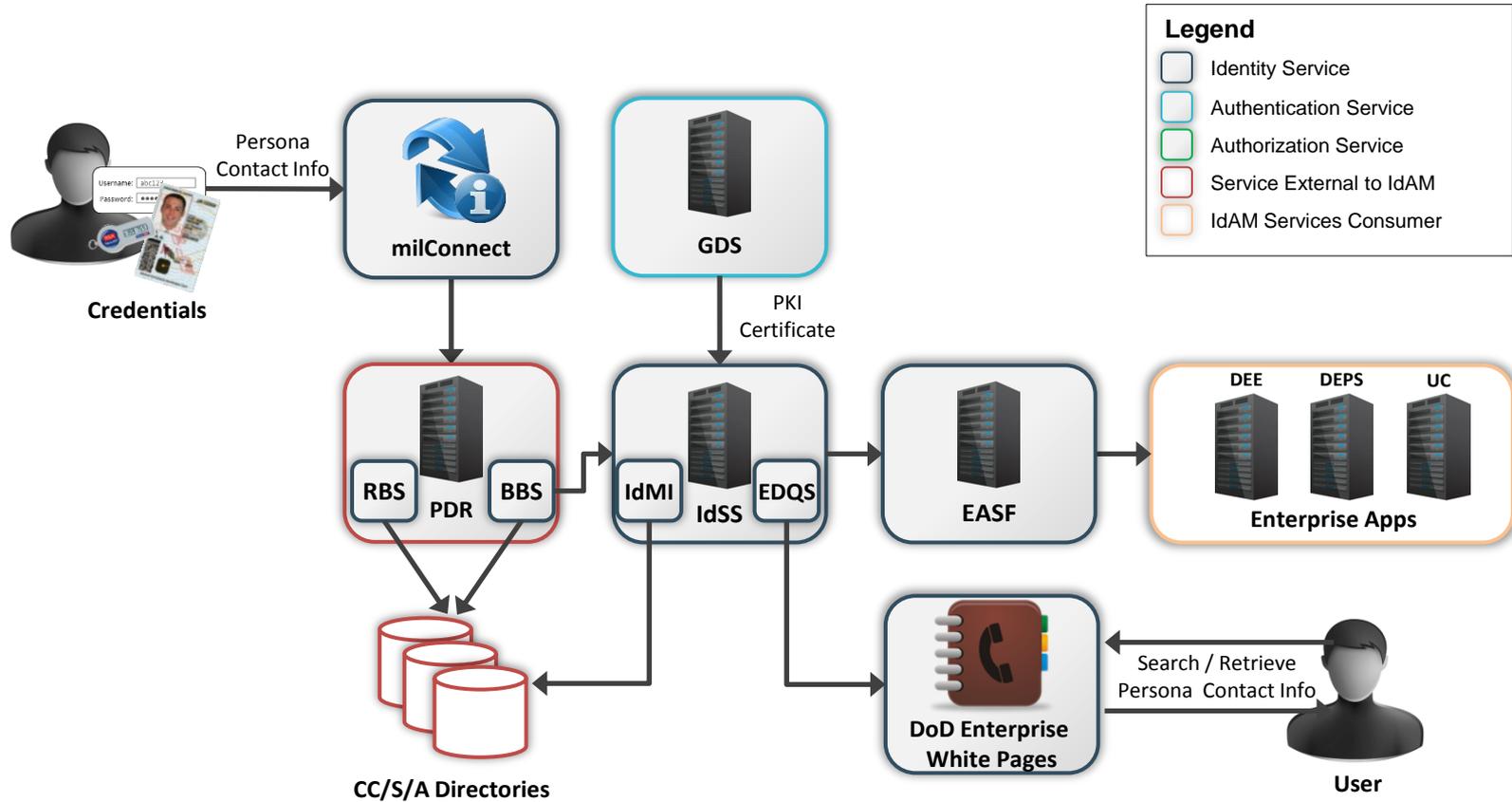
# Questions?

# Backup Slides

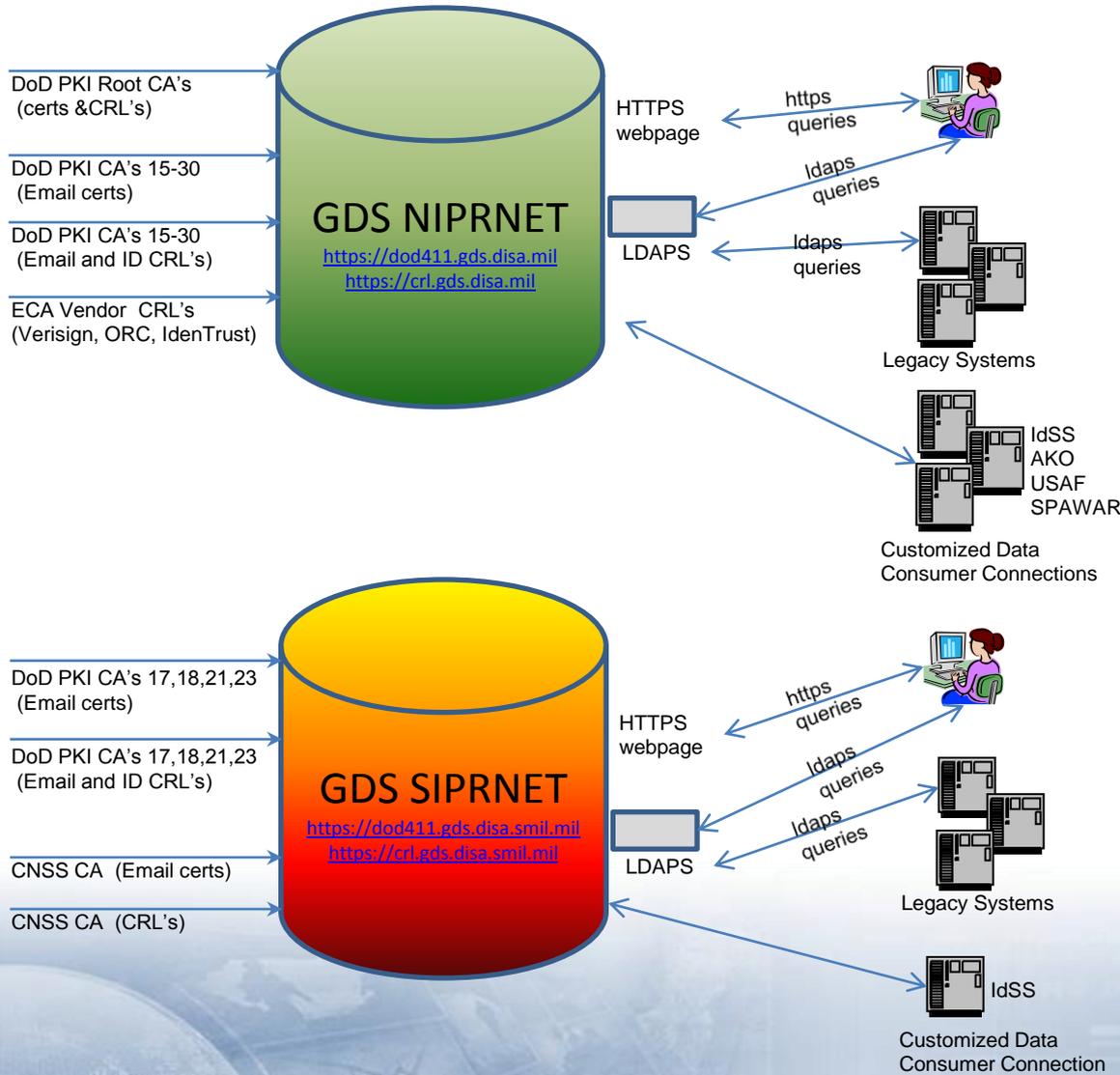
# EIAS Architecture



# EDS Architecture



# Global Directory Service (GDS) Architecture



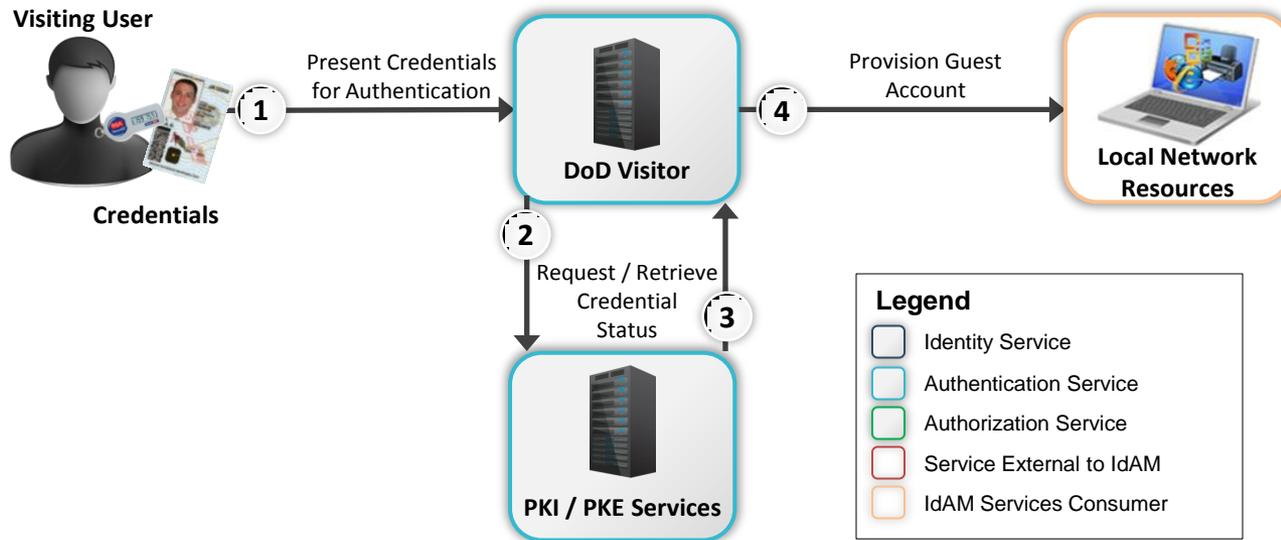
## GDS OUTPUTS

- Distribution point for DoD PKI Email Encryption Certificates to individual DoD and ECA Users
- DoD replication partners (AKO, AFDS, IdSS, SPAWAR) for delivery of DoD PKI Email Encryption Certificates
- Informally, a part of the local site account provisioning process.
- Distribution point worldwide for DoD PKI CA and ECA CRL(s)
- Distribution point for DoD PKI Root CRLs, Certificates, and cross certificates
- Servicing of AIA and CDP extensions for all DOD PKI issued certificates
- Servicing of AIA and CDP extensions for all DOD PKI Test certificates
- Distribution point for DoD PKI Test and preproduction Root CRLs, Certificates, and cross certificates
- Distribution to GCDS for NIPR users, directly for Internet users and to PKI RCVS servers.

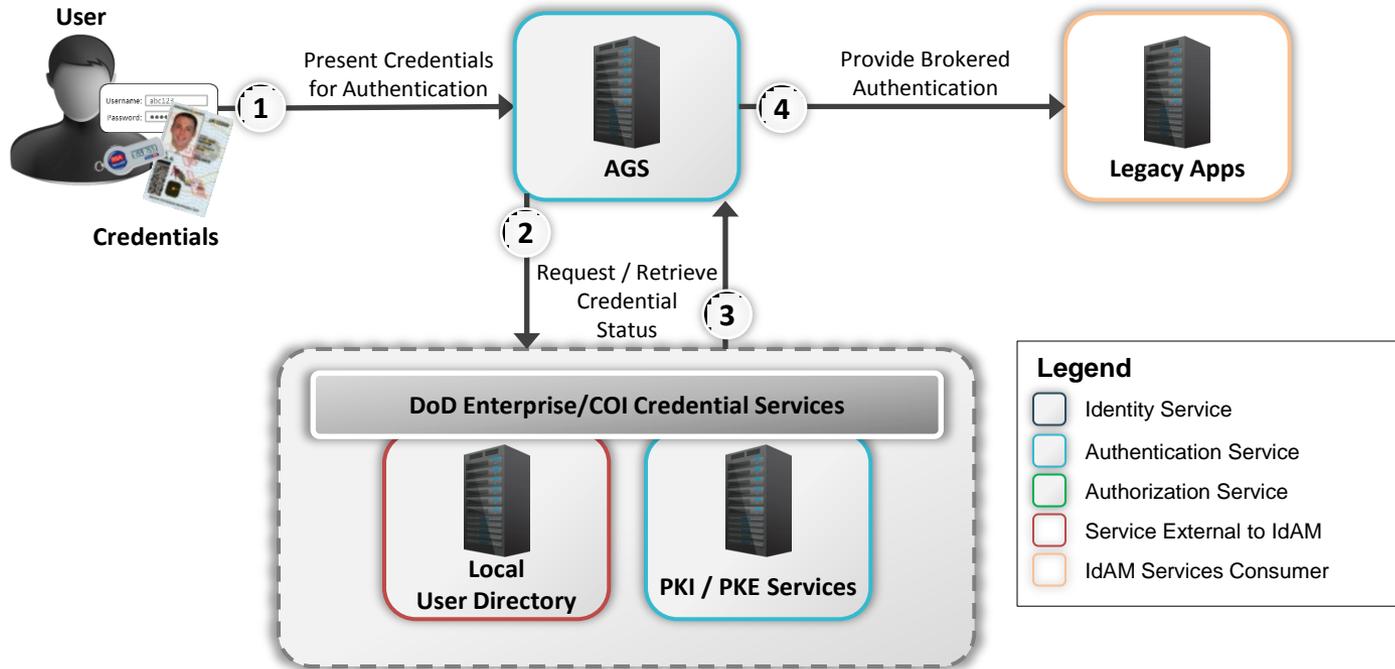
## GDS OUTPUTS

- Distribution point for Email Encryption Certificates for individual DoD users
- DoD replication partners ( IdSS) for delivery of DoD PKI Email Encryption Certificates
- Distribution point for DoD PKI CA CRL(s)
- Distribution point for DoD PKI Root CRLs
- Servicing of AIA and CDP extensions for all CNSS DOD PKI issued certificates
- Servicing of AIA and CDP extensions for all CNSS DOD PKI Test certificates
- Distribution point for CNSS DoD PKI Root CRLs, Certificates, and cross certificates
- Distribution point for CNSS DoD PKI Test and preproduction Root CRLs, Certificates, and cross certificates

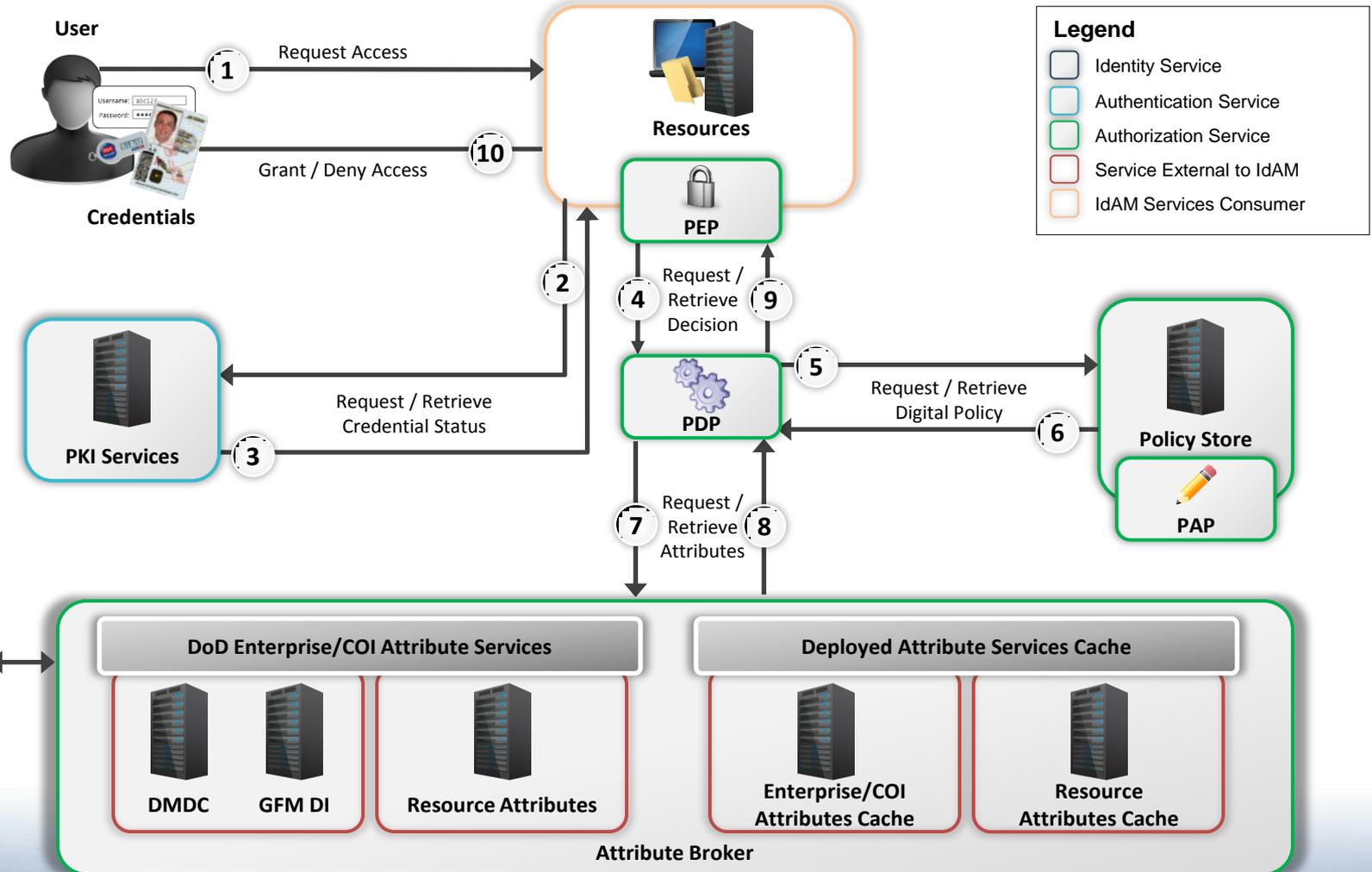
# DoD Visitor Architecture



# AGS Architecture



# Enterprise ABAC Architecture



- Identity Web Services (IWS) are capabilities developed by DMDC to provide identity verification services to government agencies for DoD military personnel, their dependents, retirees, DoD civilians, and contractors
- Data is fed from DMDC Person Data Repository (PDR)
- Includes:
  - Enterprise Identity Attribute Service (EIAS)
  - Real-Time Broker Service (RBS)
  - Batch Broker Service (BBS)