

# Identity And Access Management

# Agenda

- **DoD PKI Operational Status**
- **DoD PKI SIPRNET Token**
- **Non Person Entity PKI**
- **Interoperability**
- **Public Key Enablement**
- **Directory Services**
- **Dynamic Access**

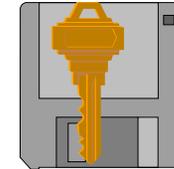
# DoD PKI Operational Metrics

- NIPRNet

- Over 80M NIPRNet Certificates issued
- Almost 28M Common Access Cards (CAC) issued
  - 3.8M active CACs, approximately 210K – 220K per month
  - More than 90% of target population now has a CAC
- 98% of DoD web servers have certificates

- SIPRNet

- Nearly 60K SIPRNet PKI Hardware tokens issued to date
- Delivered infrastructure, token, middleware, & readers
- Initial Operational Test and Evaluation ended 8 Sep 2011
- Tokens performed in geographically dispersed operational environments



DoD PKI is crucial for securing data flow across the GIG

# DoD PKI Program Context

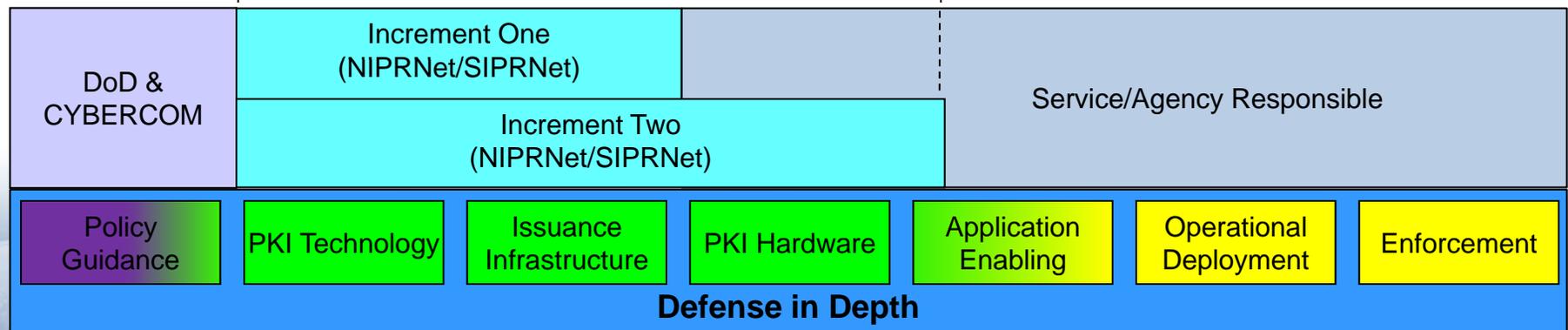
## Public Key Infrastructure

- Provides the mechanism to deliver a representation of a physical identity in a unique electronic/digital form
- Provides electronic credential for identifying and managing individual activities and access to resources over globally dispersed networks
- Includes Registration, Issuance and Life Cycle support



- PKI relies on Defense in Depth while enabling some Defense in Depth capability
- Services and Agencies are responsible for full operational deployment or enforcement of public key capability within their Service/Agency
- Increment Two expands acquisition to include PKI hardware and enhanced security on the SIPRNet

### DoD PKI Program (Part of larger context)



# SIPRNET Token Mission Imperatives



- To increase security of SECRET networks to address internal external threats
- Protection of critical DoD information in transit by providing data integrity and encryption capabilities
- DoD CIO's *DoD SIPRNet PKI Cryptographic Logon and Public Key Enablement of SIPRNet Applications and Web Servers* memo, dated 14 October 2011, mandated:
  - Issuance of SIPRNet tokens DoD-wide by 31 December 2012
  - Enablement of SIPRNet cryptographic logon using hardware tokens by 31 March 2013
  - Required SIPRNet cryptographic logon using hardware tokens by 1 April 2013
  - Enablement of all SIPRNet applications and web servers to support cryptographic authentication and complete Public Key enablement by 29 June 2013
  - Implementation of Public Key enablement of all SIPRNet application and web servers, with all access requiring PKI credentials no later than 30 June 2013

# SIPRNET Token Facts

- SIPRNET Token is unclassified when removed from the workstation allowing token to be mobile
- Services and Agencies are responsible for token issuance to their SIPRNET users
- Token is not an ID card like the CAC so there is no personalization
  - There is no picture
  - Name is not printed on card
  - Card can be reused by service/agency
- DoD SIPRNET PKI operates under the CNSS Root
- CNSS Root stood up in 2011
  - All federal agencies will have PKI tokens issued under the CNSS Root
  - Supports interoperability with other federal agencies on classified networks
  - DoD will become the common service provider for classified PKI tokens for all agencies except Dept of State and FBI



# SIPRNet Token Issuance

- As of 23 March, 59,550 tokens have been enrolled/issued
- An additional 28,544 have been formatted

Organizations	SIPRNet Tokens Received	SIPRNet Tokens Enrolled/Issued
USA	109,105	27,583
USAF	16,500	4,467
USMC	10,887	5,794
USN	15,000	6,211
USCG	800	548
DISA	7,610	2,958
DLA	3,000	712
DODIG	50	46
DTRA	100	1
JOINT STAFF	900	356
NGA	500	0
NSA/CYBERCOM	705	19
WHS/OSD	5,470	3,504
Contractor*	--	6,897
Other*	--	484

\* Issuing organization not currently identified in the Token Management System



# CY12 Token Distribution Profile

	3 Feb	10 Feb	29 Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	FY12 Funded Subtotal	Dec*	Total CY12 Delivery
<b>Army</b>	Delivered 31500	Delivered 14500	Delivered 40000	40000	32500	15500	0	0	0	0	0	0	174000	0	174000
<b>Navy</b>	0	0	0	0	5000	10500	22500	22500	22500	22500	22500	22500	150500	22500	173000
<b>Air Force</b>	0	0	0	0	9000	20000	22500	22500	22500	22500	22500	22500	164000	22500	186500
<b>Marine Corps</b>	0	0	0	0	2500	2500	2500	2500	2500	2500	2500	2500	20000	2500	22500
<b>Agencies</b>	0	0	0	0	1000	1500	2500	2500	2500	2500	2500	2500	17500	2500	20000
<b>Total</b>	Delivered 31500	Delivered 14500	Delivered 40000	40000	50000	50000	50000	50000	50000	50000	50000	50000	526000	50000*	576000

\* December deliveries will be procured with FY13 Procurement funds.  
 After February 2012, token deliveries will be made on the last business day of the month.

# Non-Person Entity PKI

- Non-Person Entity (NPE) will provide PKI certificates to devices
  - Will remove anonymity for devices on DoD networks
  - Supports IPSEC
  - Allows DoD to manage devices on its networks
- Initial focus will be on workstations, domain controller and web servers
- Capability will provide:
  - A centralized trust on the SIPRNet and NIPRNet
  - Auto issuance/rekey of PKI certificates to workstation and domain controllers
  - Will support both Microsoft and non-Microsoft devices
  - Certificates will have 12 month validity periods
- Future plans to support VOIP, radios, and other devices
- Initial operation capability will be available by May 2013
- FOC is planned for June 2014

# DoD PKI Interoperability

- DoD CIO Memo of 22 July 2008
  - Expanded the number of external PKIs that qualify as potential candidates to be Approved for Use
  - Laid out requirements for approval
  - DoD ECA Certificates
- The DoD External Interoperability Plan (EIP) defines three categories of PKIs
  - **Category I:** U.S. Federal agency PKIs
  - **Category II:** Non-Federal Agency PKIs cross certified with the Federal Bridge Certification Authority (FBCA) or PKIs from other PKI Bridges that are cross certified with the FBCA
  - **Category III:** Foreign, Allied, or Coalition Partner PKIs or other PKIs
- Current list of approved PKIs can be found at:  
<http://iase.disa.mil/pki-pke/interoperability>



# Coalition PKI

- Provides PKI capability between Coalition Partners and DoD using existing clients, systems, and network
- Flexible solution to provide a lower assurance S/MIME and Coalition specific applications
- Coalition PKI Systems will be co-located with DoD PKI systems, leveraging current facilities, infrastructure and personnel expertise
- No system development or hosting required outside of DoD
- Minimal operational change to DoD and Coalition personnel

	<b>DoD PKI</b>	<b>Coalition PKI</b>
<b>Certificate Assurance</b>	<p>Medium (software cert) Medium Hardware (CAC)</p>	<p>- Standard Token (Role Based) - Intermediate S/W Cert (Vetting Req'd) - Intermediate Token (Vetting Req'd)</p>
<b>Use Within the DoD</b>	<p>DoD Approved PKIs</p>	<p>CPKI should only be used for Coalition Specific Applications and Email</p>
<b>Key Recovery</b>	<p>Key Recovery Requires Two Collocated Key Recovery Agents (KRA)</p>	<p>Each RA is a KRA; KRAs Do Not Need to Be Collocated</p>

# DoD PKE - What We Do

- **PKI Integration across the DoD**
  - Interface between PKI operations and customer
  - Assist DoD community with integrating capabilities into their environments, to include external PKI use
  - Feed customer requirements and recommendations to PKI development
- **PKE Engineering**
  - Engineering Consultation
  - Product Evaluations
  - Reference Documentation
  - Tools
- **Community Collaboration**
  - Website - <http://iase.disa.mil/pki-pke/>
  - The Quarterly PKE Post
  - PKE Technical Interchange Meetings
  - Conference Support

Public Key Enablement – The Key to PKI

# PKE Tools Catalog

Product	Description
<b>InstallRoot</b>	<ul style="list-style-type: none"><li>■ Easy installation of DoD PKI CA certificates into trust stores</li></ul>
<b>CRLAutoCache</b>	<ul style="list-style-type: none"><li>■ Automates CRL caching for system administrators</li></ul>
<b>FBCA Cross-Certificate Remover</b>	<ul style="list-style-type: none"><li>■ Helps Microsoft products build the shortest certification path to the DoD Root</li></ul>
<b>TACT</b>	<ul style="list-style-type: none"><li>■ Allows web servers to enforce additional PKI constraints during authentication (e.g. key size, algorithms, assurance level)</li></ul>
<b>MailCrypt</b>	<ul style="list-style-type: none"><li>■ Allows bulk decryption and encryption of email with new certificates</li></ul>
<b>BlackBerry Expired OCSP Certificate Remover</b>	<ul style="list-style-type: none"><li>■ Removes expired OCSP signing certificates from device to prevent digital signature and encryption problems</li></ul>

The DoD PKE team develops tools to help DoD customers use PKI

# Thin Clients

Vendor	Model	Thin Client OS	Integrated Smart Card Reader	Ability to read SIPR Token Y/N	Remarks
Oracle SunRay	2FS	None	✓	✓	Production release available. Successfully tested with RDS; VMWare View testing in progress Citrix not supported.
	3+	None	✓	✓	Production release available. Successfully tested with RDS; VMWare View testing in progress Citrix not supported.
Wyse	C10	Wyse Thin OS	✗	✓	Successfully tested with RDS. Awaiting WTOS firmware upgrade to fix XenDesktop functionality with SIPR Token. VMWare View not supported.
	R90	Windows XPe	✗	✓	Successfully tested with RDS, Citrix XenDesktop and VMWare View.
ClearCube	I9424	None	*✓	✓	Successfully tested with VMWare View. RDS and Citrix not supported. Requires BETA firmware 3.5.1, *external card reader (internal reader does not support the SIPR token).
	I9424ST	None	✓	✓	Successfully tested with VMWare View. RDS and Citrix not supported. Requires BETA firmware 3.5.1. Internal and external readers support SIPR token.
HP (Teradici)	5740	Windows XPe	✗	✓	Successfully tested with RDS, Citrix XenDesktop and VMWare View.
	5740e	Windows 7e	✗	✓	Successfully tested with RDS, Citrix XenDesktop and VMWare View.
	gt7725	HP ThinPro	✗	✗	Awaiting firmware update to support SIPR token.
GD Tadpole	M1500	None	✓	✓	Successfully tested with RDS, VMWare View testing in progress.

Enabling Thin Clients with the SIPR Hardware Token

# Mobile Devices

- Working to make PKI on mobile devices more user-friendly
  - Working with vendors and developing tools to address usability issues such as BlackBerry OCSP certificate handling
- New Mobile Devices page on IASE:
  - [https://powhatan.iie.disa.mil/pki-pke/landing\\_pages/mobile.html](https://powhatan.iie.disa.mil/pki-pke/landing_pages/mobile.html)
  - Contains general information on approved mobile devices in use in the DoD, their PKI capabilities and usage best practices



BlackBerry



Android



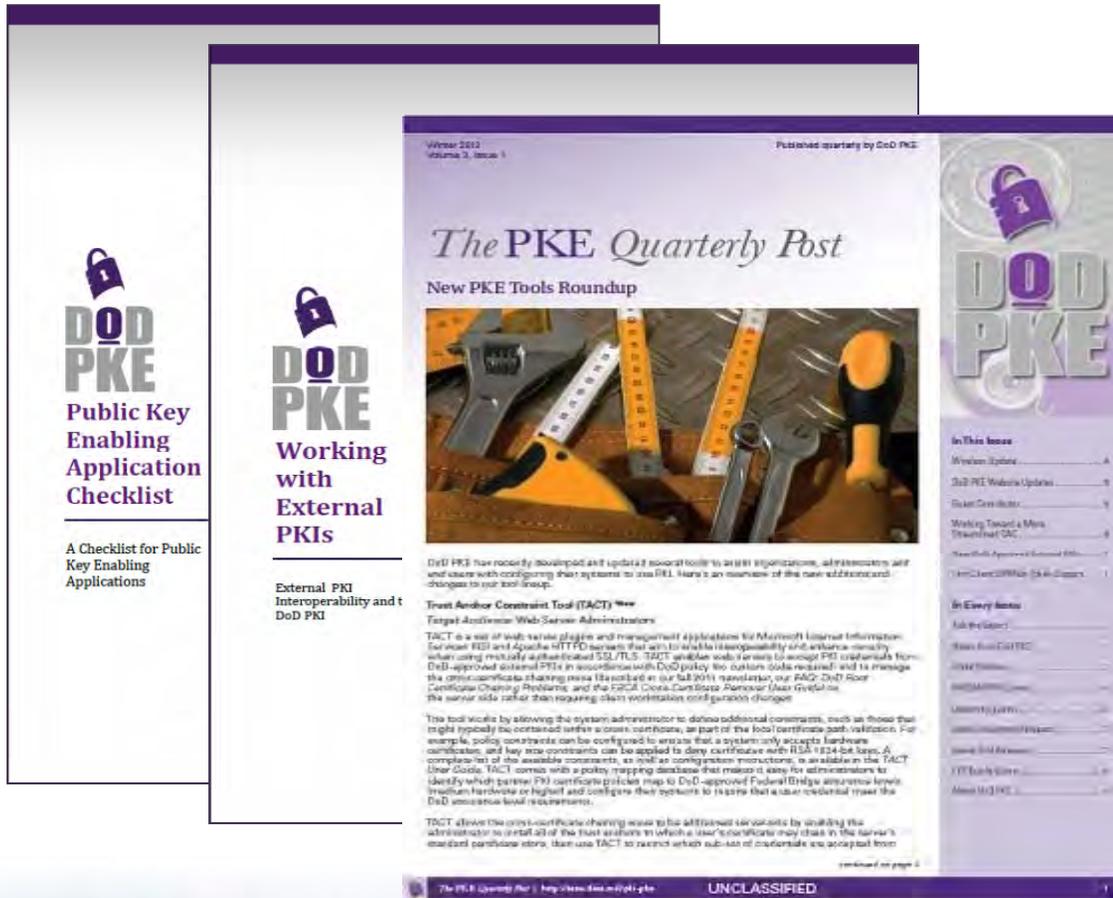
iOS



Windows Mobile

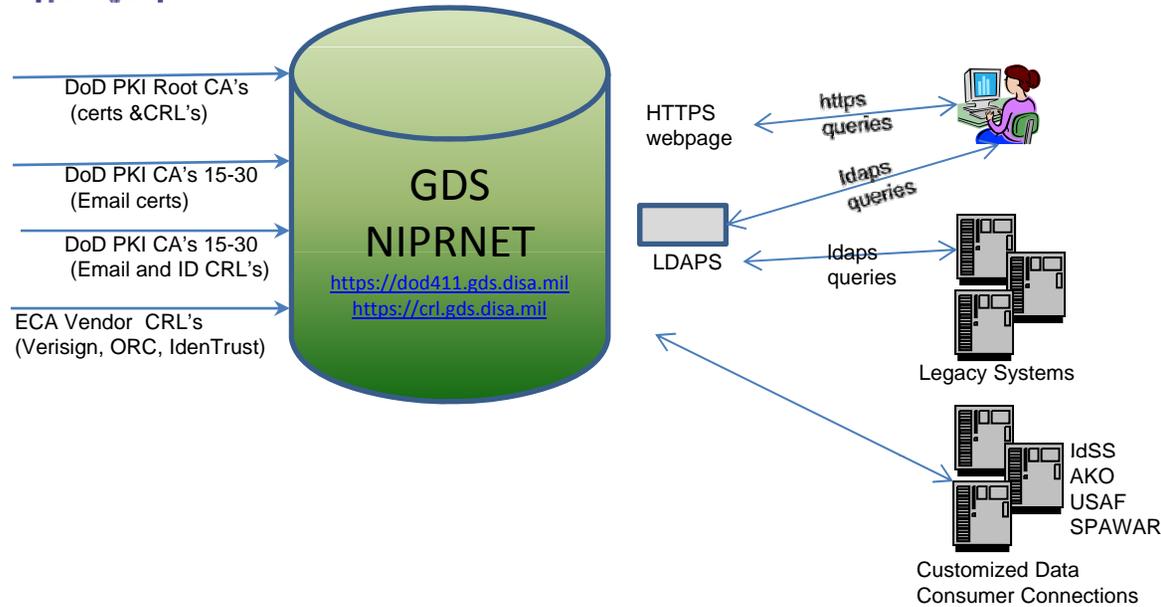
# Community Collaboration

- Website
  - <http://iase.disa.mil/pki-pke/>
- Quarterly Newsletter
  - The PKE Quarterly Post
- Slick Sheets
- PKE Technical Interchange Meetings
- Conference Support



How DoD PKE communicates capabilities to the DoD Community

# GDS



## 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

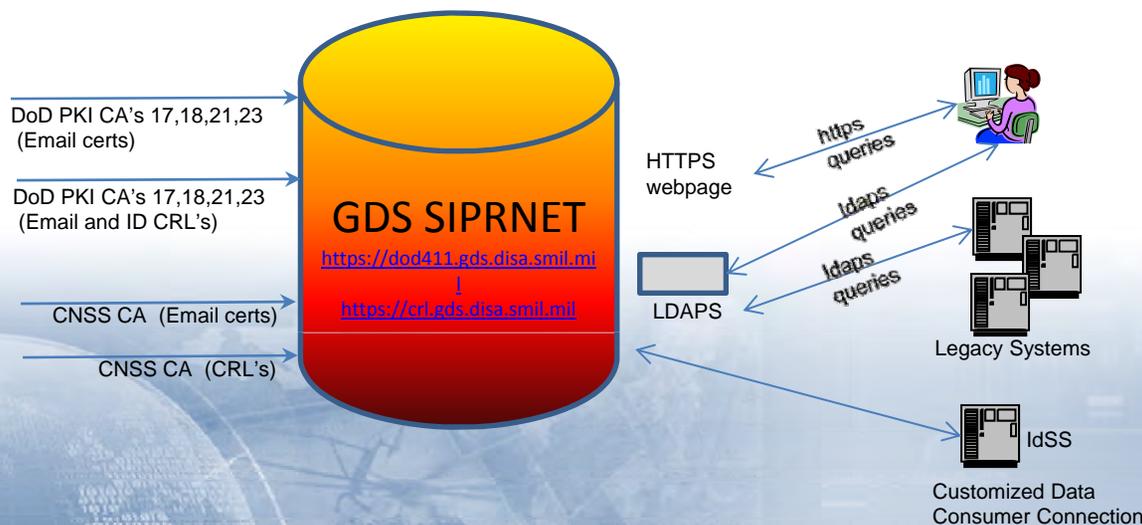
- Distribution point for DoD PKI Test and preproduction Root CRLs, Certificates, and cross certificates

- Distribution to GCDS for NIPR users, directly for Internet users and to PKI RCVS servers.

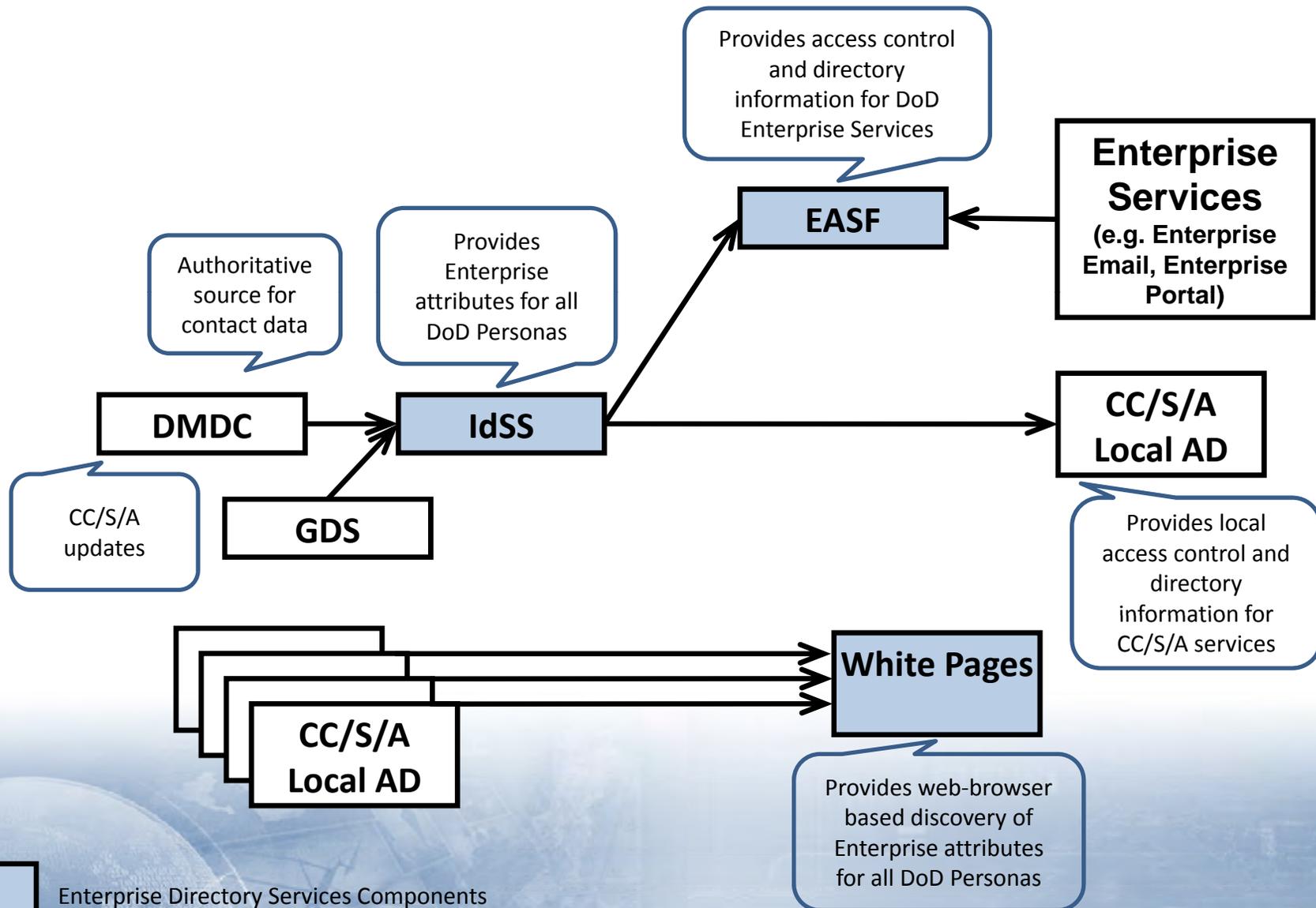
## GDS OUTPUTS

- 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



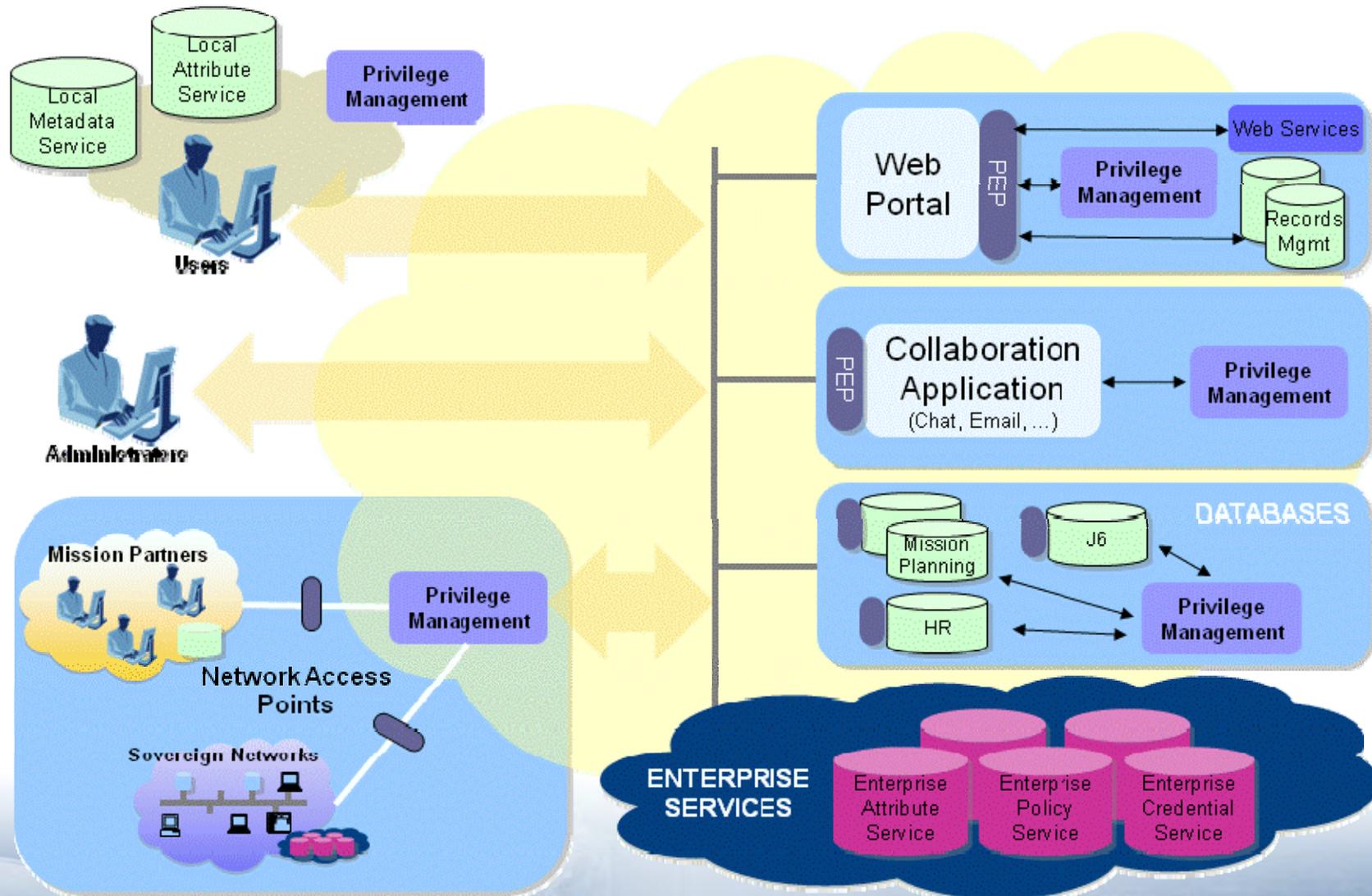
# Enterprise Directory Services



# Dynamic Access Overview

- Access Management uses authenticated identity to enforce policies regarding the access to information, services, or recourses
- Enterprise Solutions require available DoD services to include:
  - Defense Manpower Data Center (DMDC) Enterprise Identity Attribute Service (EIAS) for persona attributes
  - Enterprise Access Policy
  - Service and Resource Metadata
  - Provisioned Account Services
- DISA and NSA are working together to develop a suite of solutions to address DoD Enterprise Requirements
  - Enterprise Service
  - Reference Implementations
  - Reviewing Open Source and COTS solutions
- DISA has been involved in Piloting efforts to prove out technology and applicability in the DoD

# Dynamic Access



# Enterprise Service

- NSA and DISA (PEO-MA and ESD) are developing a pilot for a Enterprise Service Center (ESC) to provide an Access Control Service for ESC located DoD resources
  - DoD resources could implement access control without the need to stand up individual solutions or buy licenses
    - Takes advantage of economies of scale
    - Reduces cost impact to CC/S/A
    - Reduces stove pipe or proprietary solutions
    - Enterprise solution based on standards and industry best practices to ensure interoperability
    - DoD policy enforced as base requirement ensuring system is compliant at the highest level
  - Targeting FY13Q4 IOC
  - Develop capability within DISA Rapid Access Computing Environments (RACE)
    - Access Control Service will become part of the RACE suite to allow for programs to develop and ensure it is part of their ESC deployed solution

# Reference Implementation Overview

Documentation and configuration guidance of technical solutions for applying access control within the DoD, required for tactical or disconnected resources



- Provides solution for CC/S/As that need a locally deployed access control capability
- Documentation and guides will ensure that implementations are standardized and interoperable with DoD services
- DISA provided engineering support and for Open Source or COTS licenses

- NSA & DISA Phase II Pilot
  - DISA PEO-MA/IA43 supporting NSA PvM Phase II Pilot at USNORTHCOM
  - Addressing two (2) problem spaces in support of USNORTHCOM's mission for Defense Support of Civil Authority (DSCA) Events
    - Provide a federated integrated information and imagery sharing SharePoint portal that authorized DHS users can access
    - Provide an ability to extend the current DoD XMPP chat capability to allow authorized DHS users access to authorized DoD chat rooms while restricting all other unwanted activities
- DISA PEO-MA and ESD SharePoint Pilot
  - Reviewing Intelligence Community agency's SharePoint Attribute Based Access Control Solutions to determine if it can be used to support DoD Enterprise Portal
  - Potentially targeting Defense Enterprise Portal Service SIPR deployment

- Additional information available at:
  - DKO Privilege Management  
<https://www.us.army.mil/suite/page/595023>
  - DISA Privilege Management Branch  
[https://www.intelink.gov/wiki/Privilege\\_Management\\_Branch](https://www.intelink.gov/wiki/Privilege_Management_Branch)
  - Privilege Management References  
[https://www.intelink.gov/wiki/Privilege\\_Management\\_References](https://www.intelink.gov/wiki/Privilege_Management_References)
  - Privilege Management Implementation Outline  
[https://www.intelink.gov/wiki/Privilege\\_Management\\_Implementation\\_Outline](https://www.intelink.gov/wiki/Privilege_Management_Implementation_Outline)
  - DISA Global Information Grid Convergence Master Plan Outline: Privilege Management  
[https://www.intelink.gov/wiki/DISA\\_Global\\_Information\\_Grid\\_Convergence\\_Master\\_Plan\\_Outline/Privilege\\_Management](https://www.intelink.gov/wiki/DISA_Global_Information_Grid_Convergence_Master_Plan_Outline/Privilege_Management)
  - Email:  
[PvM\\_Support@disa.mil](mailto:PvM_Support@disa.mil)

# QUESTIONS

