Interagency Advisory Board

Meeting Agenda, Tuesday, November 1, 2011

1. **Opening Remarks** *(Mr. Tim Baldridge, IAB Chair)*

2. **FIPS 201-2 Update and Panel Discussion with NIST Experts in Q&A Session** *(Bill MacGregor and Hildy Ferraiolo, NIST)*

3. **Securing Mobile Devices for Government Specific Apps** *(Debb Blanchard, Verizon)*

4. **Enabling HSPD-12 and Biometrics to Secure the Pentagon and Mark Center** *(Derek Nagel and Roger Roehr, PFPA)*

5. **An Example of Enabling HSPD-12 in Multi-Tenant Building by Operating a PACS Platform as a Service** *(Tom Corder, Bridgepoint Systems)*

6. **DoD PIV-I Update** *(Paul Grant, DoD)*

7. **Closing Remarks** *(Mr. Tim Baldridge, IAB Chair)*

Personal Identity Verification (PIV) – Interoperable (PIV-I) Update
At
Industry Advisory Board

Paul D. Grant

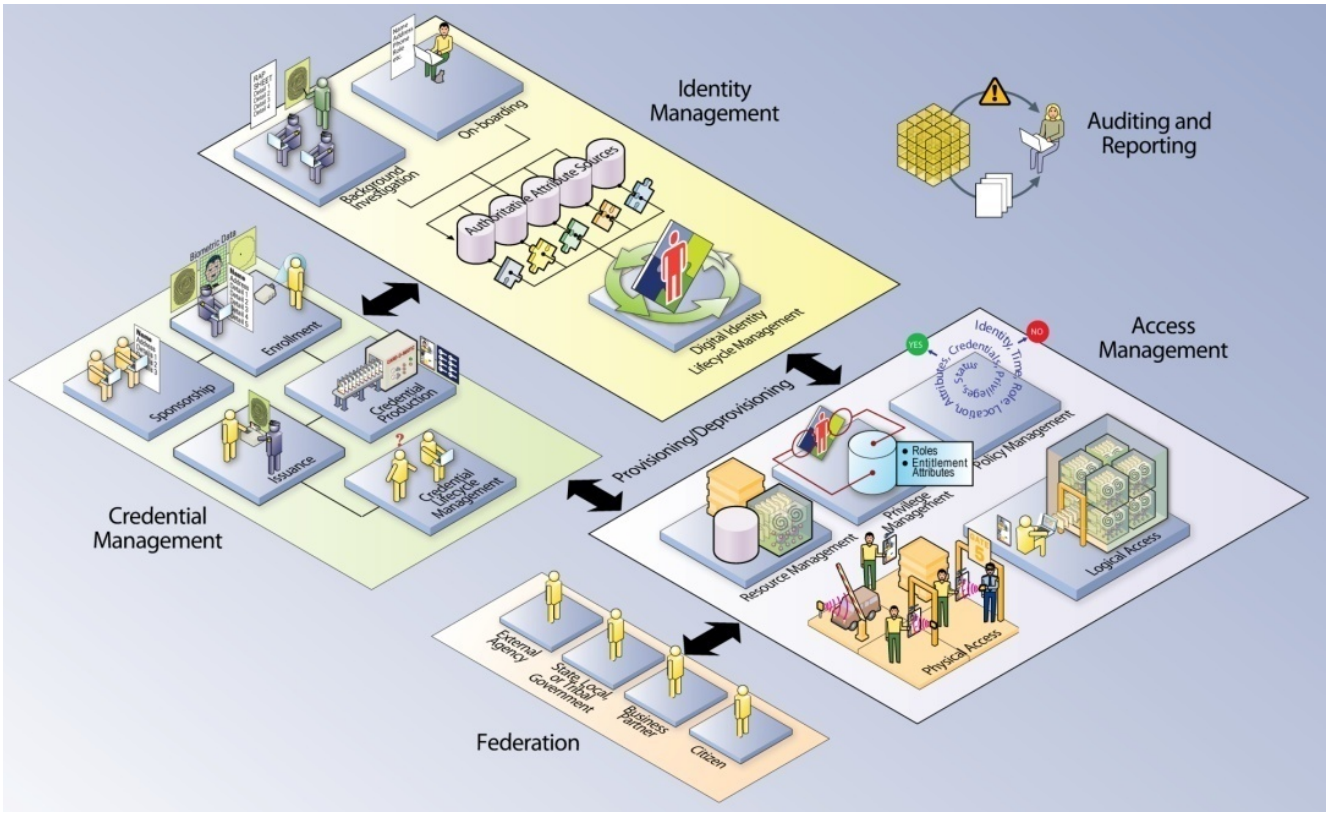
Special Assistant, Federated Identity Management and External Partnering
Office of the DoD CIO

Co-Chair, Identity, Credential and Access Management Sub-Committee
Federal CIO Council

1 November 2011

FICAM
The Federal Bridge and PIV-I

FICAM Key Components

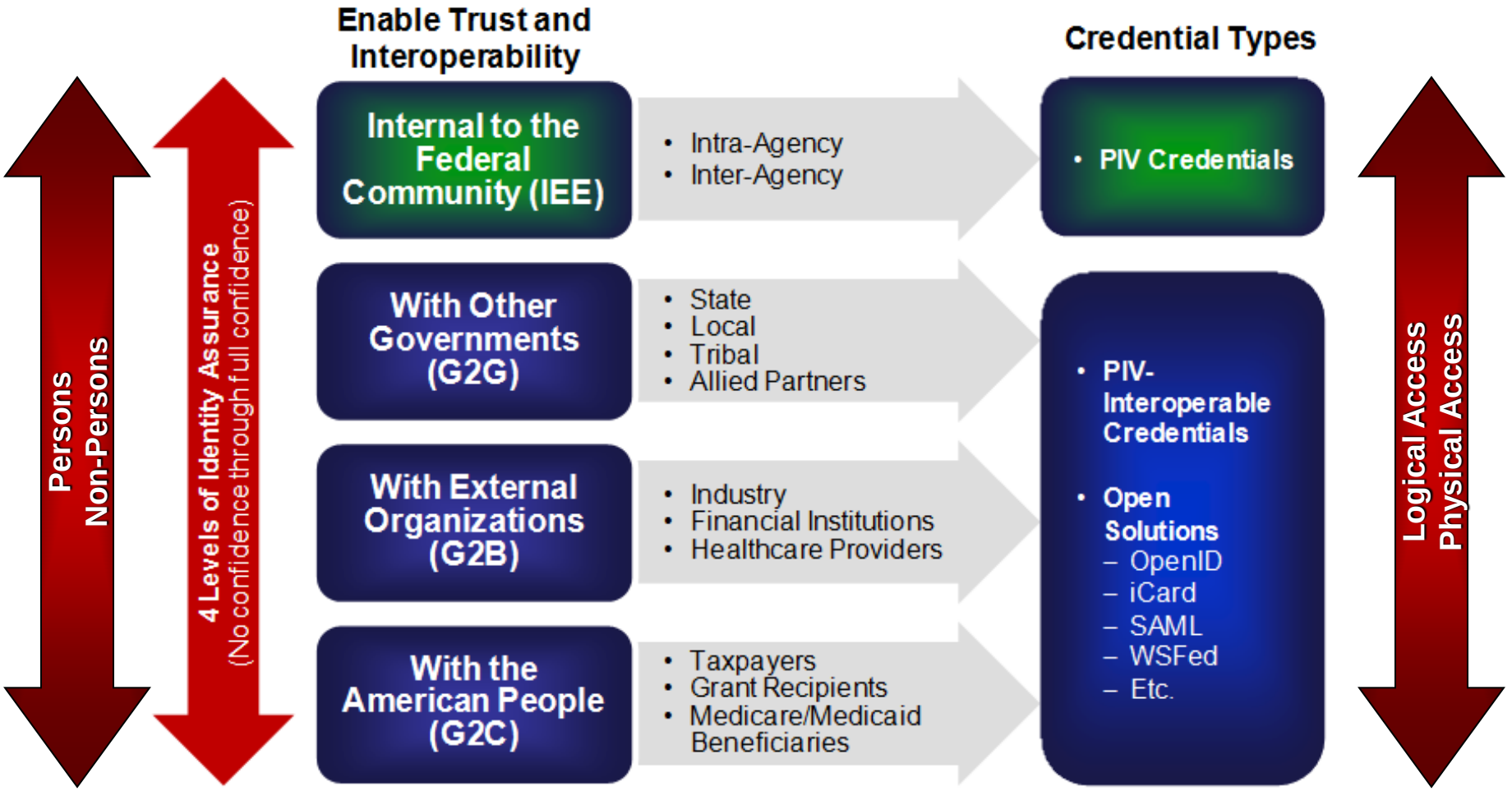


FICAM Service Areas

- Digital Identity
- Credentialing
- Privilege Management
- Authentication
- Authorization & Access
- Cryptography
- Auditing and Reporting

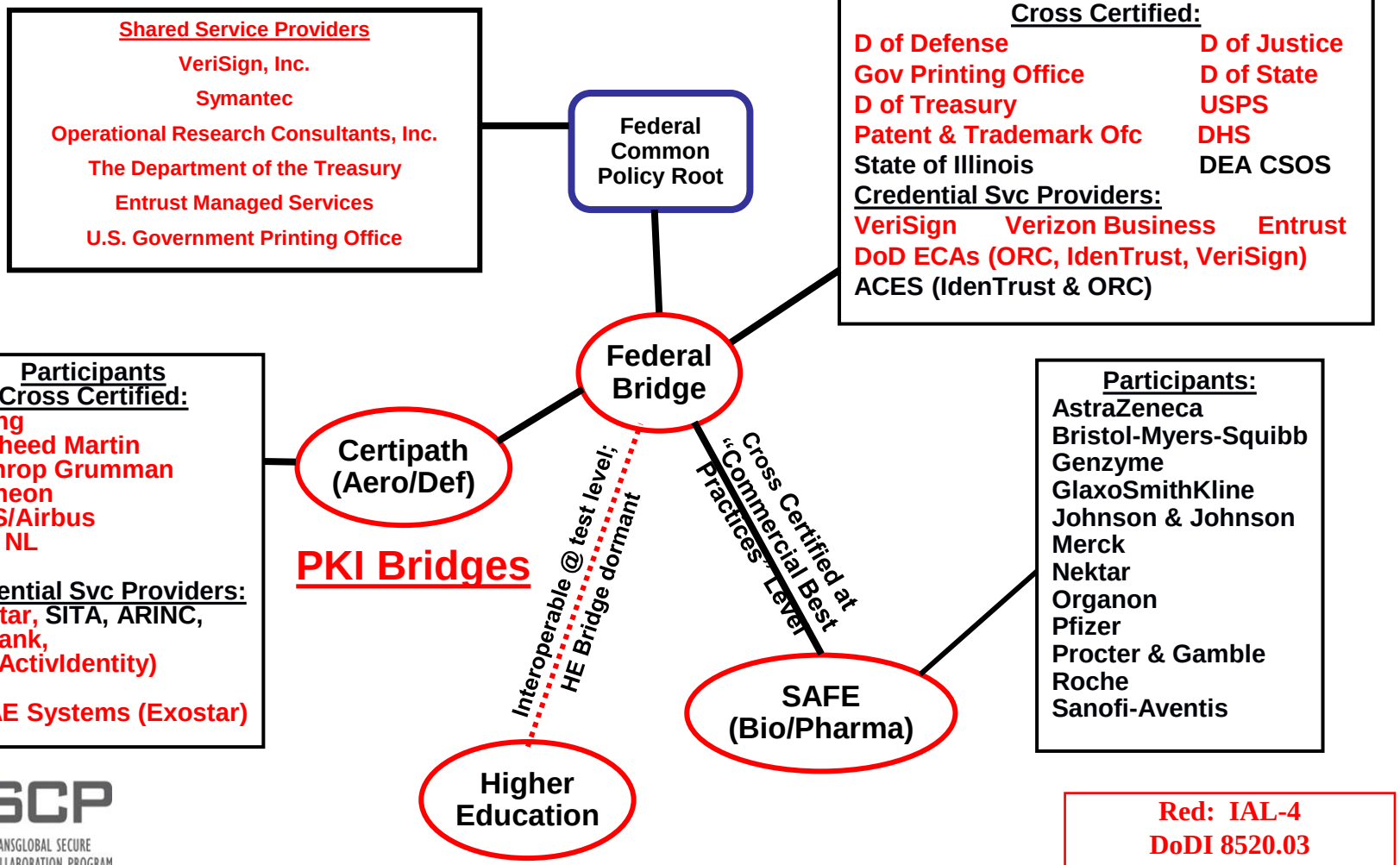
ICAM represents the intersection of digital identities, credentials, and access control into one comprehensive approach

FICAM Scope



Foundation for Trust and Interoperability in Conducting Electronic Transactions both within the Federal Government and with External Partners

Identity Federations (PKI Based)



Fed Bridge Status: http://www.idmanagement.gov/fpkia/crosscert.cfm
Certipath Status: http://www.certipath.com/certipath-bridge/piv-i-issuers

Approved PIV-I Providers

- **Federal Bridge Approved PIV-I Providers:**
  - VeriSign, Inc. (A Symantec Company)
  - Verizon Business
  - Entrust
- **Certipath Approved PIV-I Providers:**
  - Exostar
  - CitiBank
  - HID (ActivIdentity)

Goal: Large Number of Qualified Providers (NFI) for Partners to have Competitive Choices

Recent Purchases of PIV-I Credentials

- Booz Allen Hamilton
- California Prison Health Care Services
- Computer Sciences Corporation
- ICF international
- Millennium Challenge Corporation
- US Senate
- State of Colorado – purchasing PIV-I and trusts DoD CAC
- State of Kansas
- State of Illinois
- Commonwealth of Virginia – First Responders
- State of West Virginia – RFP
- Commonwealth of Pennsylvania – Chester Country issuing PIV-I

ICAM
Identity, Credential, & Access Management

PIV-I in DoD

DoD Acceptance and Use of PIV-I Credentials

ICAM Identity, Credential, & Access Management

- **DoD Instruction 8520.03, Identity Authentication for Information Systems**
  - Outlines steps for acceptance and use of PKIs external to DoD (to include PIV and PIV-I)
  - May 13, 2011
- **DoD CIO Memo, DoD Acceptance and Use of Personal Identity Verification-Interoperable Credentials, 5 Oct 2010**
  - Proper use of PIV-I credentials support DoD security goals
  - PIV-I credentials meet Federal interoperability requirements
  - Meets DoD criteria for approved PKI-based identity credentials
    - Cross certified with Federal PKI Bridge
    - An established need to interoperate w/ DoD relying parties
    - Proven (tested) to operate with DoD infrastructure
    - PIV-I provider has legal relationship w/ DoD (MOA)
  - "Approved for Use" by DoD CIO; Relying party decision required
    - Not used for authentication to DoD networks (NIPR and SIPR)
    - Must be electronically validated at physical access control points

Now Available to Public
Information Assurance Support Environment (IASE) PKI/PKE

ICAM Identity, Credential, & Access Management

- **Hosts the DoD PKI/PKE site:**
  - http://iase.disa.mil/pki-pke/interoperability/index.html
- **3 categories of PKIs**
  - Category I – U.S. Federal agency PKIs (i.e. PIV)
  - Category II – Non-Federal Agency PKIs cross certified with the FBCA or PKIs from other PKI Bridges that are cross certified with FBCA
  - Category III – Foreign, Allied, or Coalition Partner PKIs
- **There are currently 3 Category II PIV-I providers approved for use in DoD:**
  - HID - ActivIdentity Inc. NFI PKI (August 2011), and
  - VeriSign NFI PKI (April 2011)
  - CitiBank (Jul 2011)

Defense Industrial Base and Aerospace/Defense Community and PKI Use

- DIB and A/D partners are starting to use signed and encrypted email to move / share sensitive unclassified information.
- Several DIB Partners have native PKI approved for use and trusted by DoD (all are members of the Transglobal Secure Collaboration Program - www.TSCP.org)
- Other partners can/have acquire PKI credentials from approved credential service provides (including Non-Federal Issuers (NFI) of PIV-I)
- The TSCP Specification for Signed and Encrypted eMail is publically shared at:

  www.tscp.org/images/stories/library/sev1_tech_specs.pdf
- Federal ICAM documentation is shared at:

  www.IdManagement.Gov

Questions?

www.idmanagement.gov

http://iase.disa.mil/pki-pke/interoperability/index.html

Backup

Federal Bridge Approved PIV-I Bridges

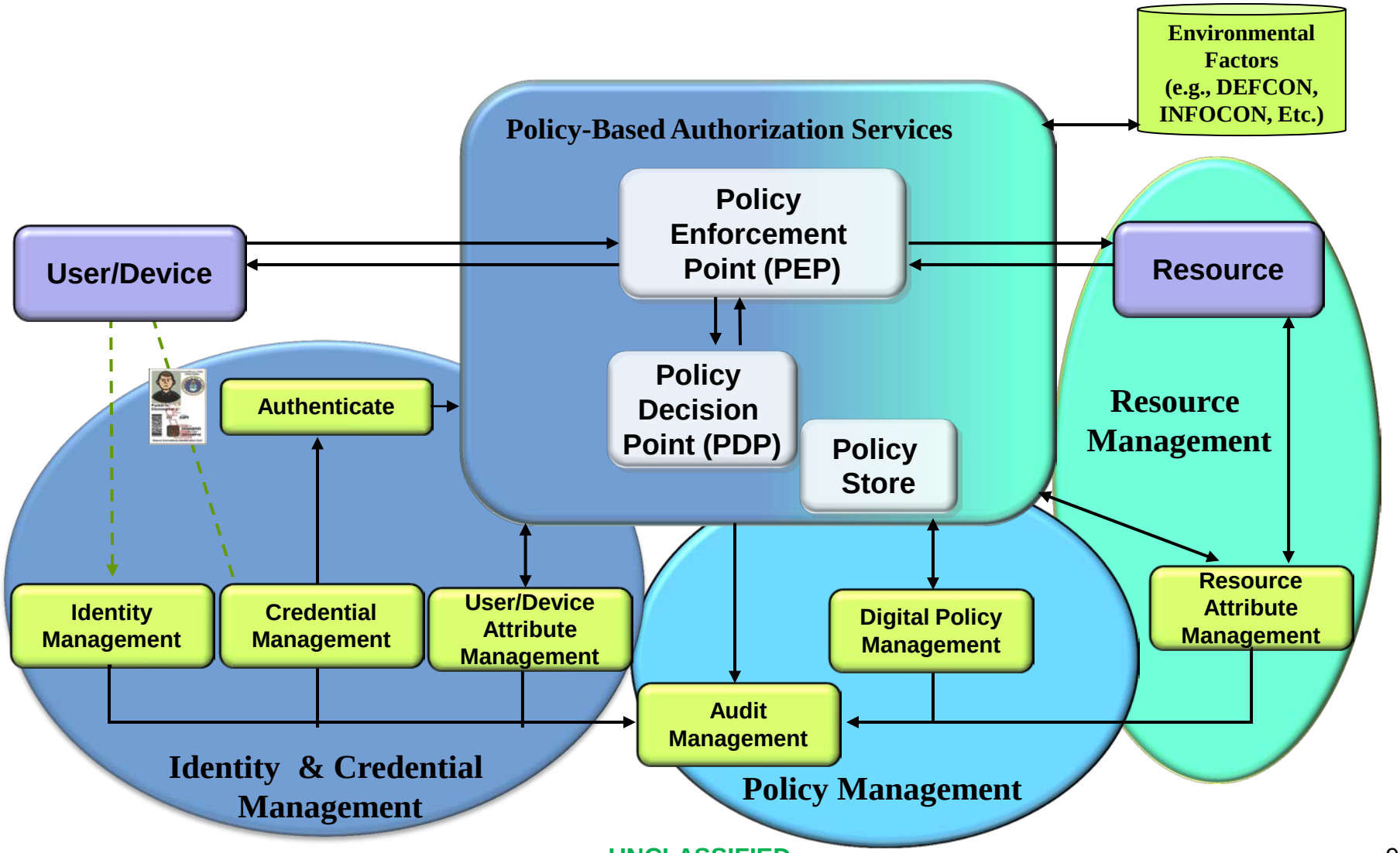
- **Approved PIV-I Bridges:**
  - CertiPath
    For more information, contact Sergio Smith (Senior Director of Corporate Development Operations) at # 703-793-7871 or via email at "sergio.smith@certipath.com"

DoD I 8520.03 Snapshot

ICAM Identity, Credential, & Access Management

		Entity Environment						
		Untrusted	User Managed	Partner Managed	DoD Managed	DoD Network	Classified Partner Network	Classified DoD Network
Sensitivity Level	Classified 7						H	H
	Classified 6						G	G
	Classified 5						F	F
	Admin Accounts			E	E	E	H	H
	Unclassified 4			E	E	E		
	Unclassified 3		D	C	C	B		
	Unclassified 2		D	B	B	A		
	Unclassified 1	A	A	A	A	A		

DoD ICAM Target State: Dynamic Access Control



Clause Overview

Defense Federal Acquisition Regulation Supplement; Safeguarding Unclassified Information (DFARS case 2011-D039)

- Results in the addition of new subpart and associated contract clauses for safeguarding, proper handling, and cyber intrusion reporting of unclassified DoD information contained on contractor owned / operated information systems

Basic Safeguarding

- Apply to **any** DoD information
- Requires some form of Access Control (i.e. user ID/PW)
- At least one physical or electronic barrier in place when not under direct control
- Proper media sanitization
- Intrusion protection (i.e. anti-virus, anti-spyware, etc)
- Limit distribution to need to know personnel
- Applicable to all sub-contracts

Enhanced Safeguarding

- Applies to: Critical Program Information (DoDI 5200.39), DoD OPSEC Program (DoDD 5205.02) information subject to export controls, information designated for withholding (non-FOIA), information bearing current or prior designations (FOUO, SBU, etc), technical information, PII
- In addition to Basic Safeguarding, it also requires Cyber Intrusion Reporting specifics

Minimum Security Controls for Enhanced Safeguarding (cond.)

ICAM Identity, Credential, & Access Management

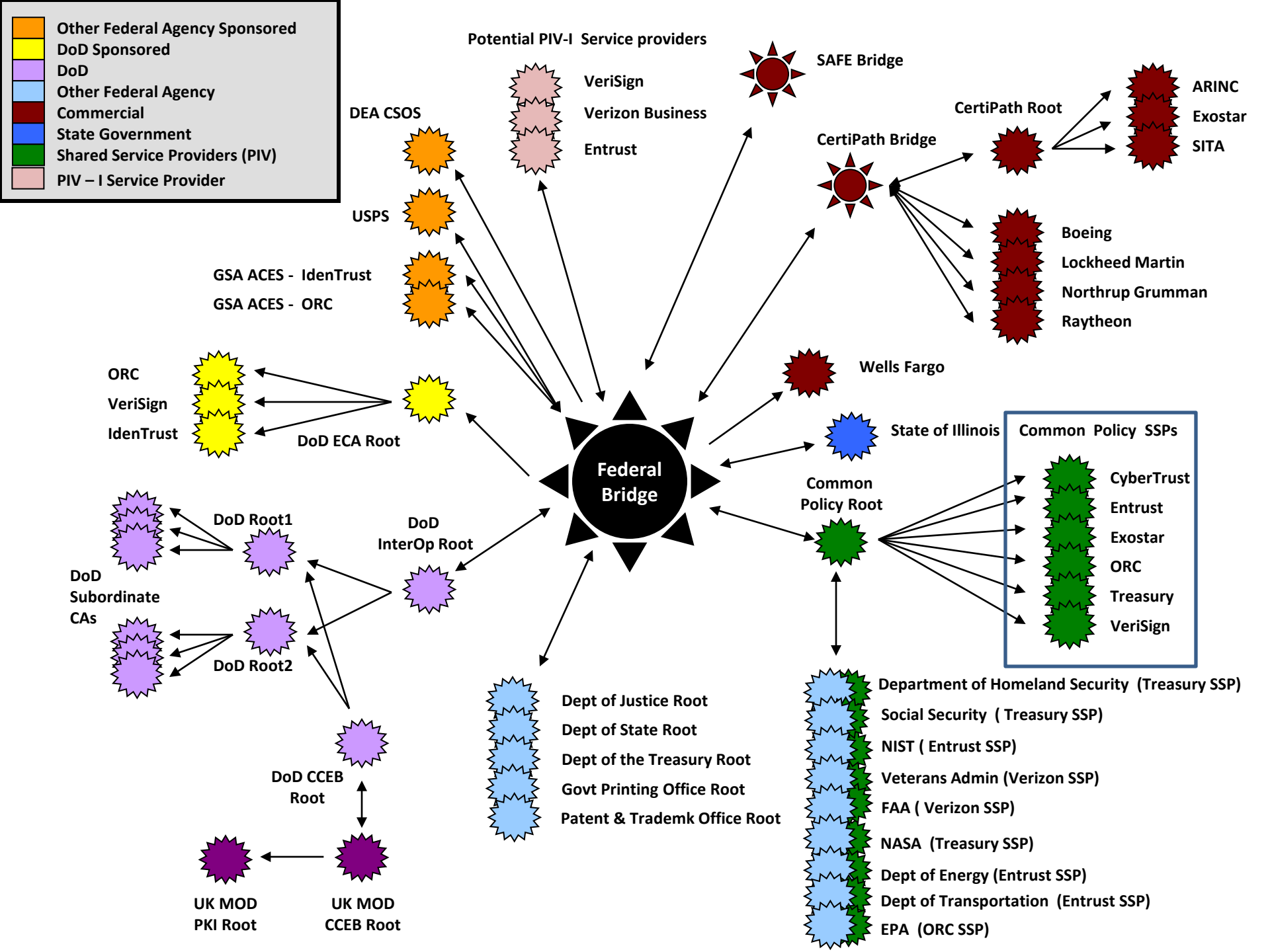
Access control	Awareness & training	Contingency planning	Maintenance	System & comm protection
AC–2	AT–2	CP–9	MA–4	SC–2.
AC–3			MA–4(6)	SC–4.
AC–3(4)	Audit & Accountability	Identification and Authentication.	MA–5	SC–7.
AC–4	AU–2		MA–6	SC–7(2).
AC–6	AU–3	IA–2		SC–9.
AC–7	AU–6	IA–4	Media Protection	SC–9(1).
AC–11	AU–6(1)	IA–5	MP–4	SC–13.
AC–11(1)	AU–7	IA–5(1)	MP–6	SC–13(1).
AC–17	AU–8			SC–13(4).
AC–17(2)	AU–9	Incident Response	Physical and Environmental Protection.	SC–15.
AC–18	AU–10			SC–28.
AC–18(1)	AU–10(5)	IR–2	.	
AC–19		IR–4	PE–5	System & Information Integrity.
	Configuration Management	IR–5	PE–7	SI–2.
		IR–6		SI–3.
	CM–2		Program Management	SI–4.
	CM–6			
	CM–7		PM–10	
	CM–8			

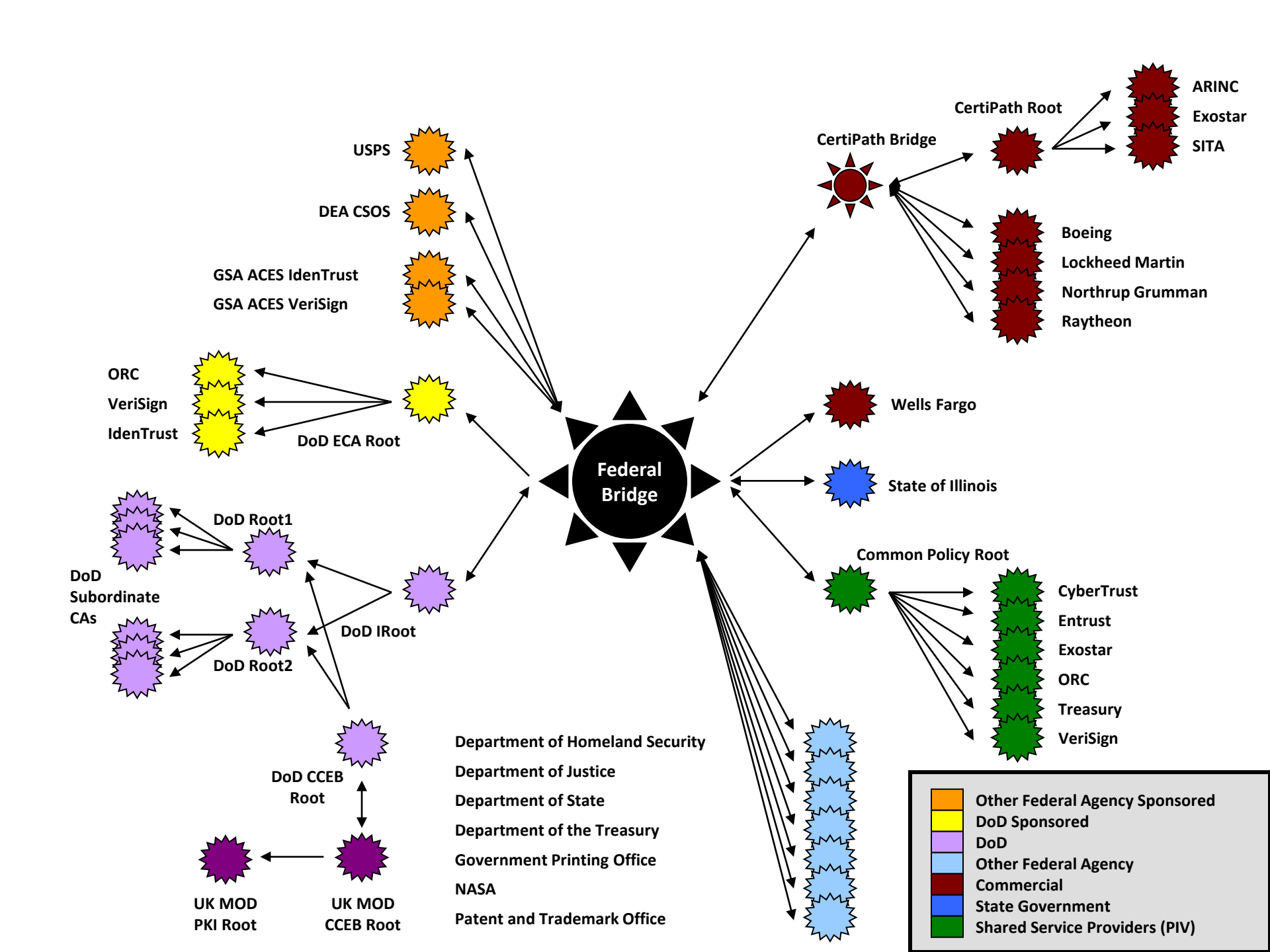
Legend: AC: Access Control, AT: Awareness and Training, AU: Auditing and Accountability Protection, CM: Configuration Management, CP: Contingency Planning Acquisition, IA: Identification and Authentication Communications Protection, IR: Incident Response Integrity, MA: Maintenance, MP: Media Protection, PE: Physical & Environmental, PM: Program Management, SA: System and Services, SC: System, & SI: System & Information.

* Note that those numbers in parentheses signify security control enhancements that are specified in Appendix F of NIST SP 800-53

NIST SP 800-53 Extract

Identification and Authentication (Organizational Users)		
IA-2	Control	The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).
	Guidance	Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof.


Other Federal Agency Sponsored
DoD Sponsored
DoD
Other Federal Agency
Commercial
State Government
Shared Service Providers (PIV)
PIV – I Service Provider
Potential PIV-I Service providers
VeriSign
Verizon Business
Entrust
SAFE Bridge
DEA CSOS
USPS
GSA ACES - IdenTrust
GSA ACES - ORC
CertiPath Root
CertiPath Bridge
ARINC
Exostar
SITA
Boeing
Lockheed Martin
Northrup Grumman
Raytheon
ORC
VeriSign
IdenTrust
DoD ECA Root
Wells Fargo
State of Illinois
Federal Bridge
Common Policy SSPs
Common Policy Root
CyberTrust
Entrust
Exostar
ORC
Treasury
VeriSign
DoD Root1
DoD InterOp Root
DoD Subordinate CAs
DoD Root2
DoD CCEB Root
Dept of Justice Root
Dept of State Root
Dept of the Treasury Root
Govt Printing Office Root
Patent & Trademk Office Root
Department of Homeland Security (Treasury SSP)
Social Security (Treasury SSP)
NIST (Entrust SSP)
Veterans Admin (Verizon SSP)
FAA (Verizon SSP)
NASA (Treasury SSP)
Dept of Energy (Entrust SSP)
Dept of Transportation (Entrust SSP)
EPA (ORC SSP)
UK MOD PKI Root
UK MOD CCEB Root


Federal Bridge
USPS
DEA CSOS
GSA ACES IdenTrust
GSA ACES VeriSign
ORC
VeriSign
IdenTrust
DoD ECA Root
DoD Root1
DoD Subordinate CAs
DoD Root2
DoD IRoot
DoD CCEB Root
UK MOD PKI Root
UK MOD CCEB Root
CertiPath Bridge
CertiPath Root
ARINC
Exostar
SITA
Boeing
Lockheed Martin
Northrup Grumman
Raytheon
Wells Fargo
State of Illinois
Common Policy Root
CyberTrust
Entrust
Exostar
ORC
Treasury
VeriSign
Department of Homeland Security
Department of Justice
Department of State
Department of the Treasury
Government Printing Office
NASA
Patent and Trademark Office
Other Federal Agency Sponsored
DoD Sponsored
DoD
Other Federal Agency
Commercial
State Government
Shared Service Providers (PIV)