PIV and E-PACS: Using PKI for PIV and PIV-I Authentication in Access Control

Smart Card Alliance ***2014*** **Government** ***Conference***

October 29, 2014

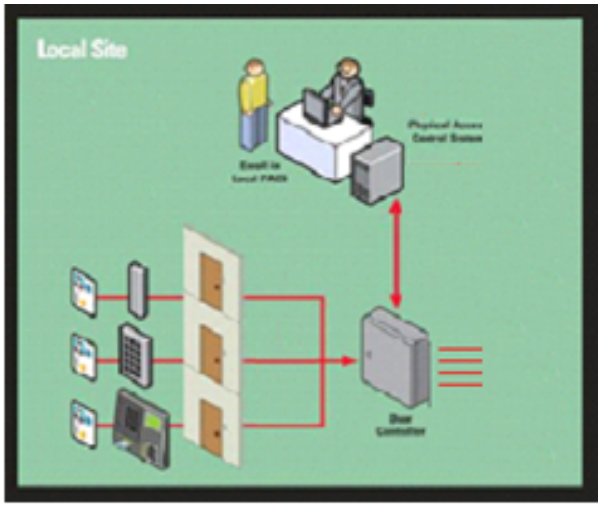
CertiPath

The Way It Was…

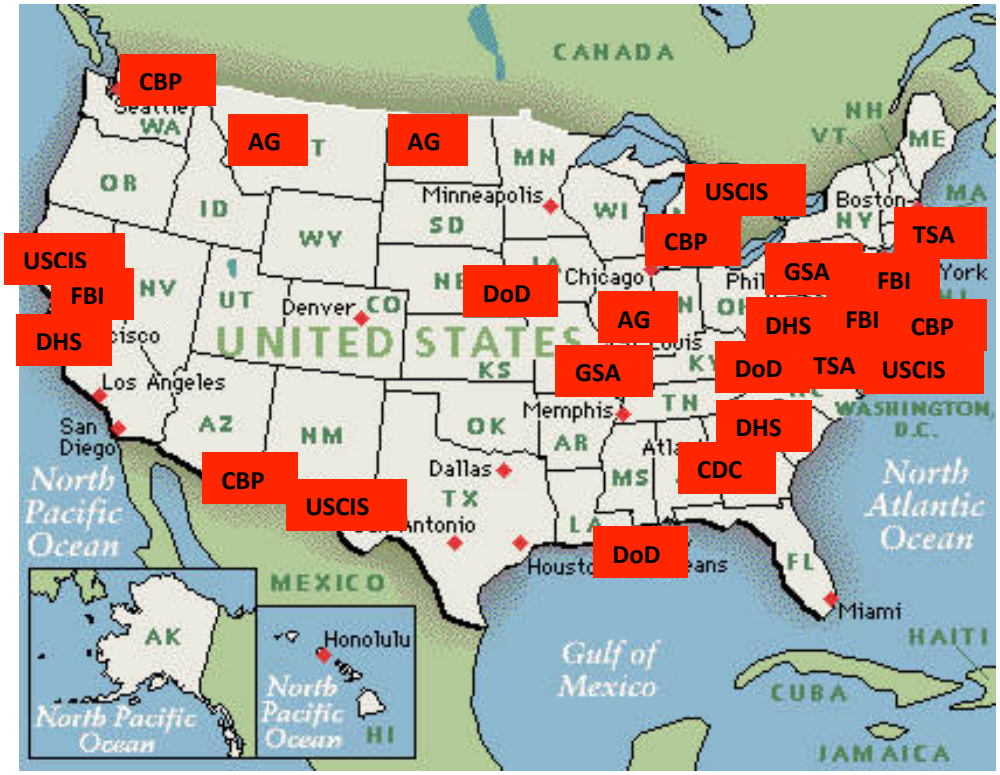
CertiPath

Traditional PACS: Site-centric

- Traditional identity credentialing process



Traditional PACS: The Silo Syndrome



- Proprietary PACS, card formats
- Duplication of operations
  - ID proofing
    - Low assurance!
  - Issuance
  - Registration to PACS
  - No guarantee of uniqueness

…Think of the expense
…and the Lock Down problem

CertiPath

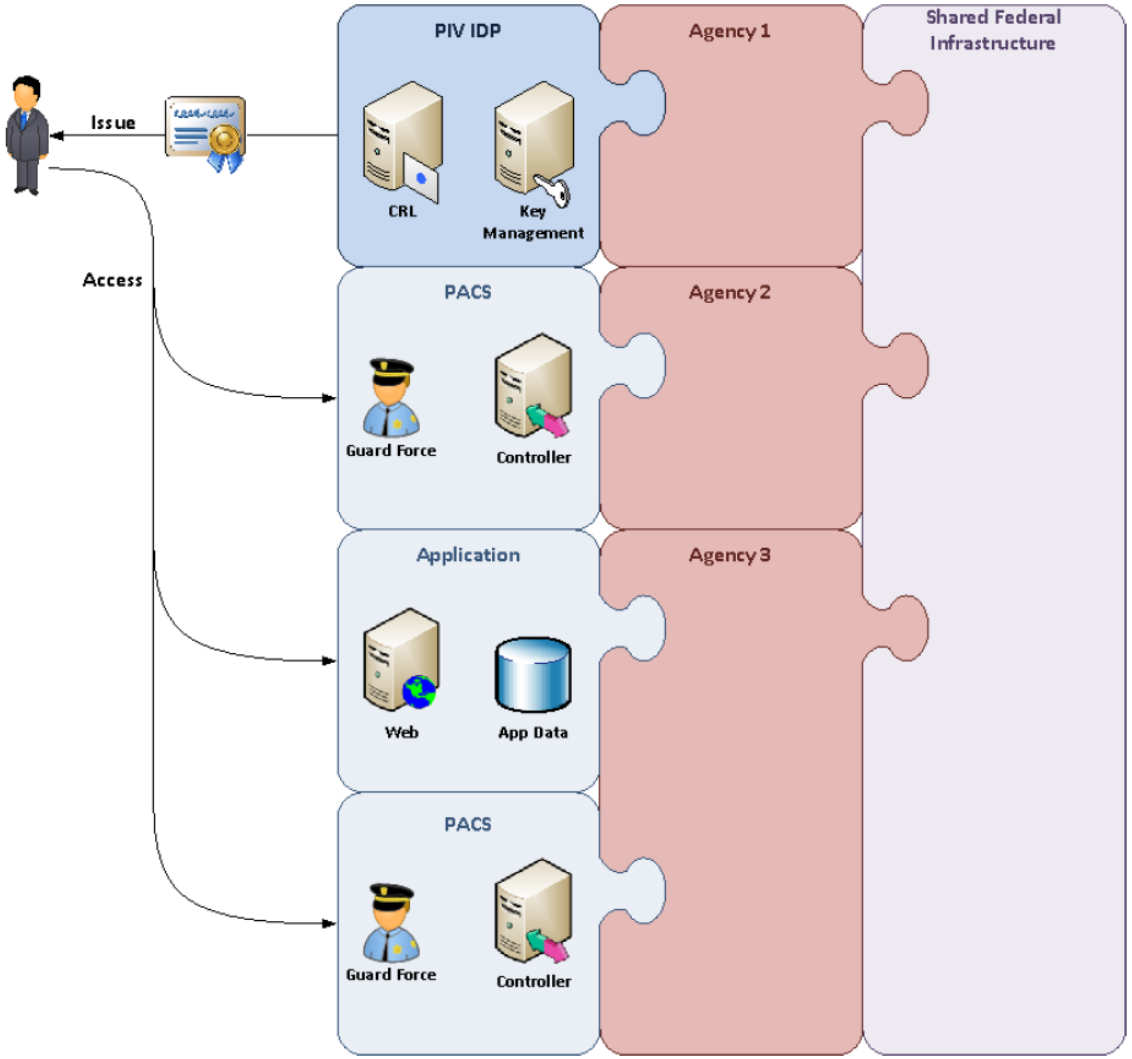
The Transformation…

Dependence on Cloud-Based

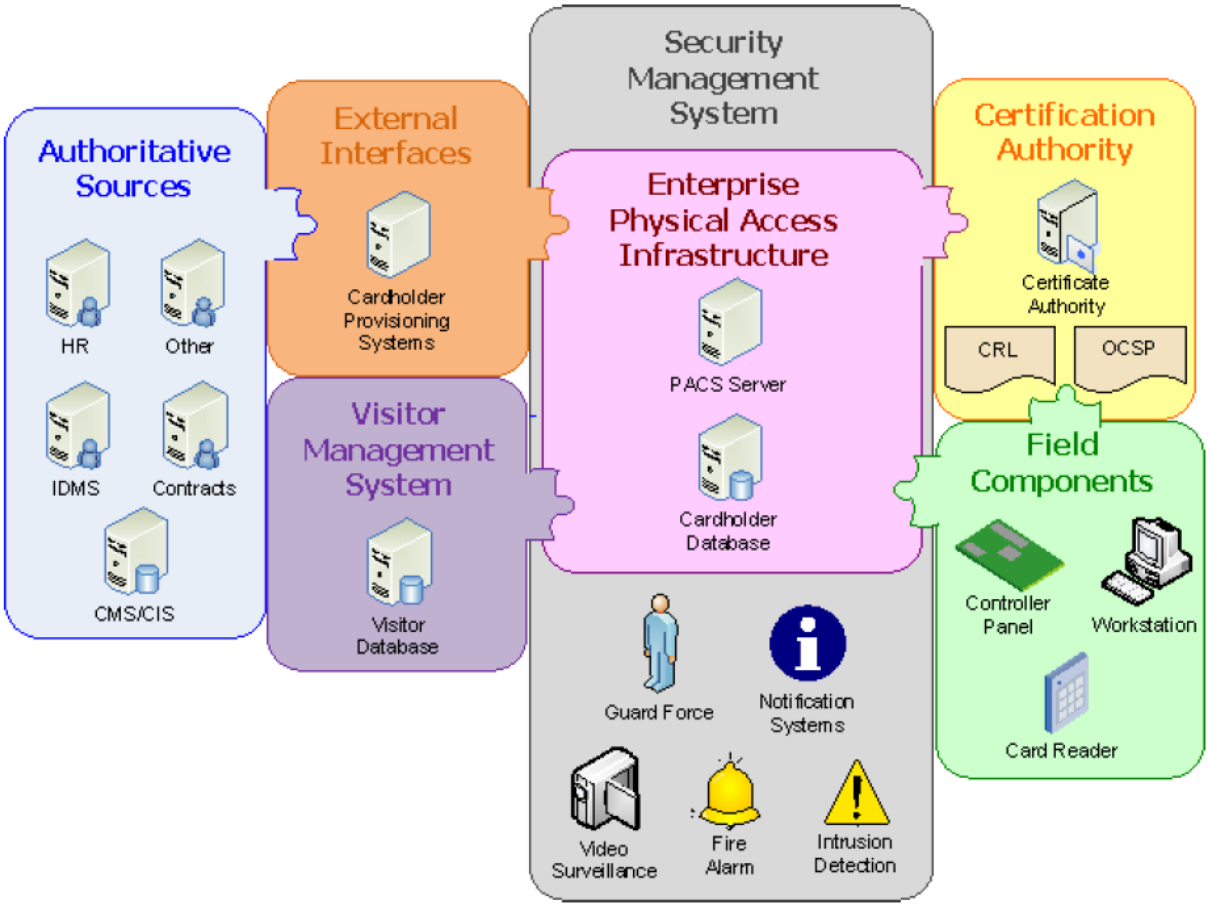
- Enterprise Identity Management
- Credential Issuance
- PKI Services

CertiPath

FICAM Roadmap Federal Enterprise Target Conceptual Diagram

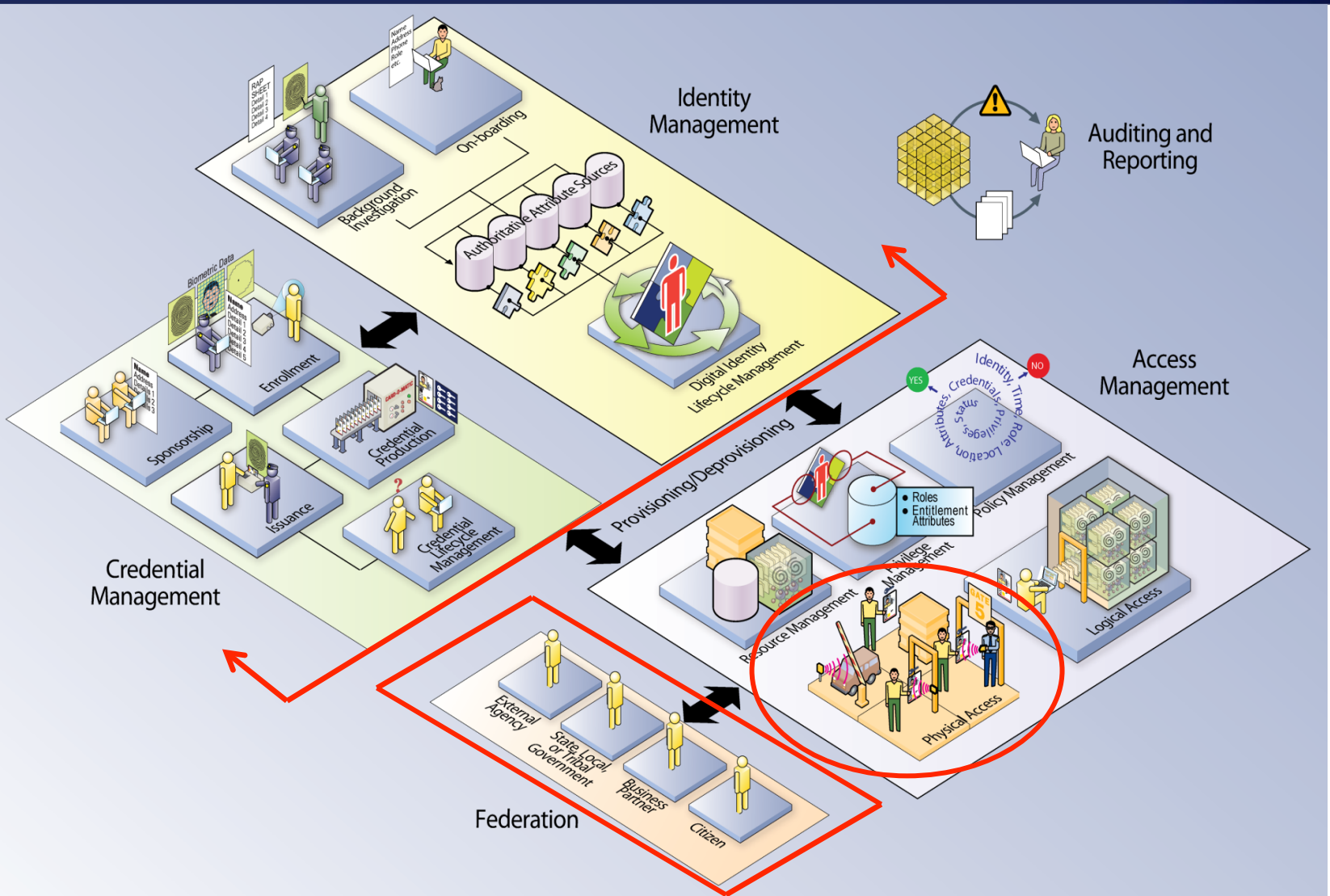


FICAM Roadmap Overview of PACS within the Overall Infrastructure

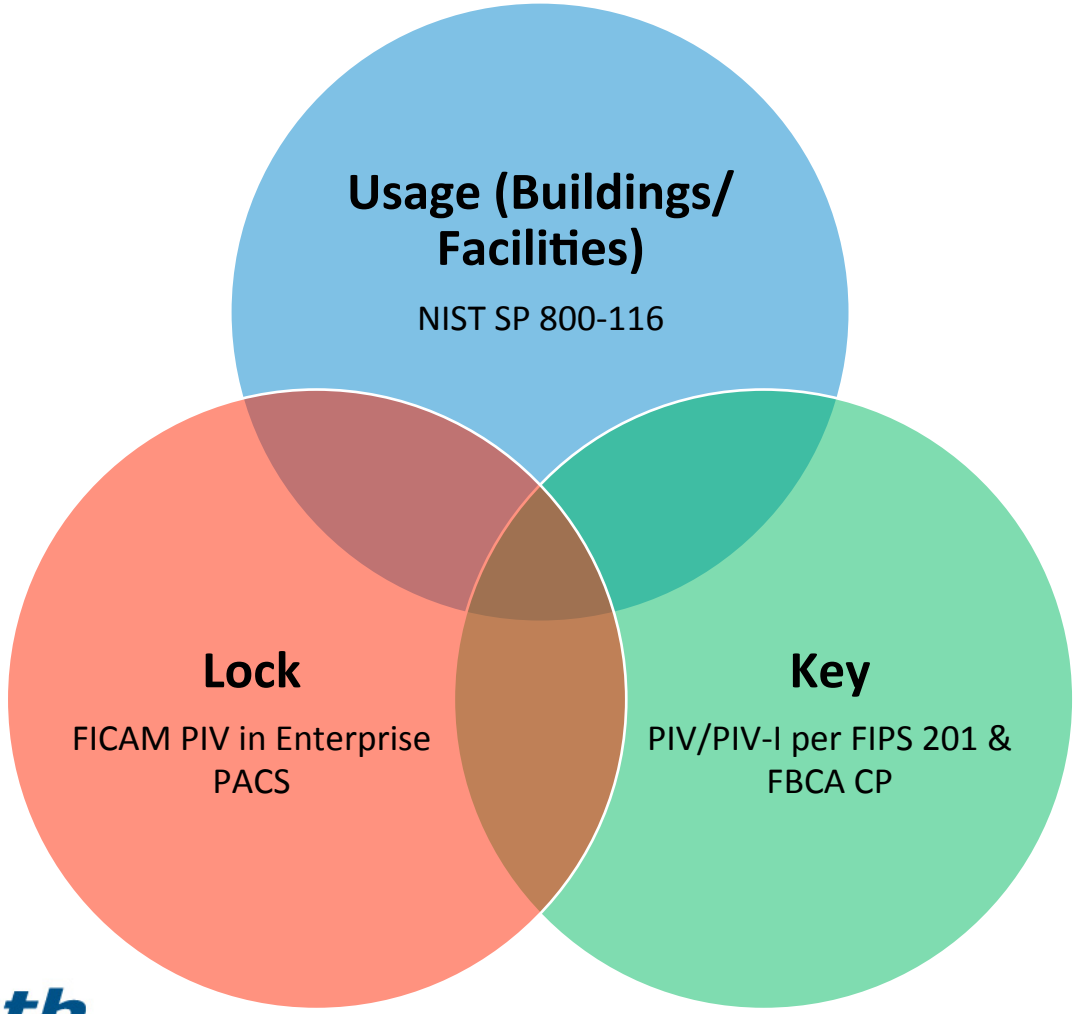


CertiPath

ICAM Foundational Architecture



How Policies Govern Implementations



CertiPath

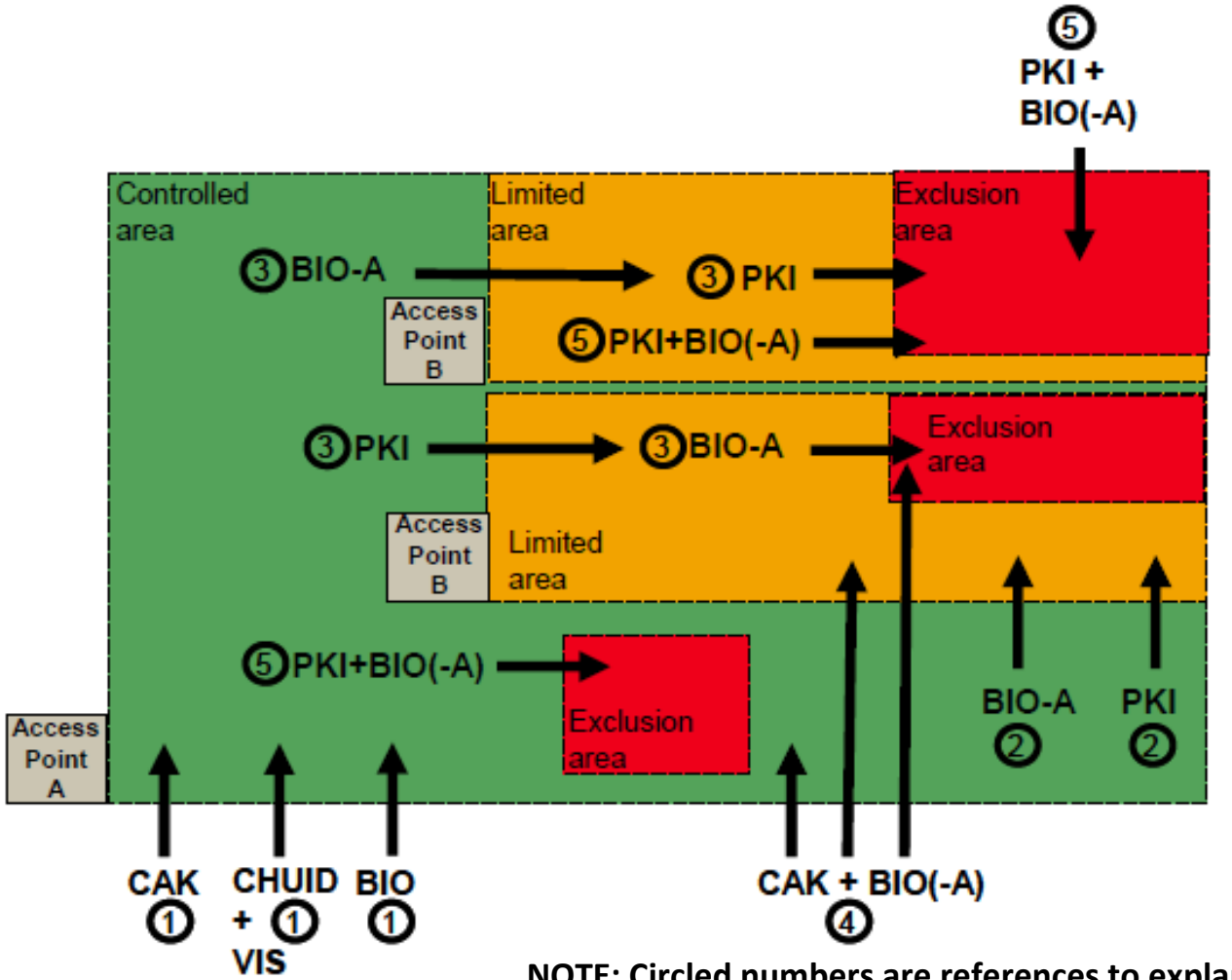
The Tools in my Arsenal…

	Secures against cards that are						
Auth Modes ↓	Revoked	Counterfeit or Altered	Copied or Cloned	Lost or Stolen	Shared	Auth Factors	SP 800-116 Security Area
Chip Serial #						None	Uncontrolled
FASC-N/UUID	✓					None	Uncontrolled
CHUID+VIS	✓	✓				1	Controlled
PKI-CAK	✓	✓	✓			1	Controlled
PKI-AUTH	✓	✓	✓	✓		2	Limited
PKI-AUTH+BIO	✓	✓	✓	✓	✓	3	Exclusion

- Performing signature checks and private key challenges at enrollment is not sufficient to achieve these levels of assurance. They must be done at the time-of-access.
- **CHUID** as an authentication method is ***deprecated***

CertiPath

Mapping Authentication Method to Controlled Areas



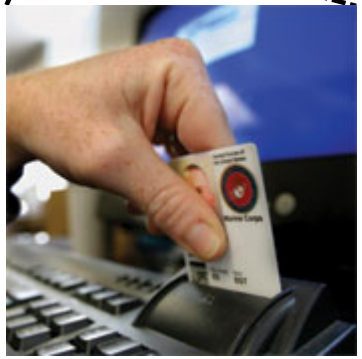
NOTE: Circled numbers are references to explanatory text in SP800-116, not the number of authentication factors

CertiPath

SO…
When Someone Shows Up at My Door…

PKI-Authentication

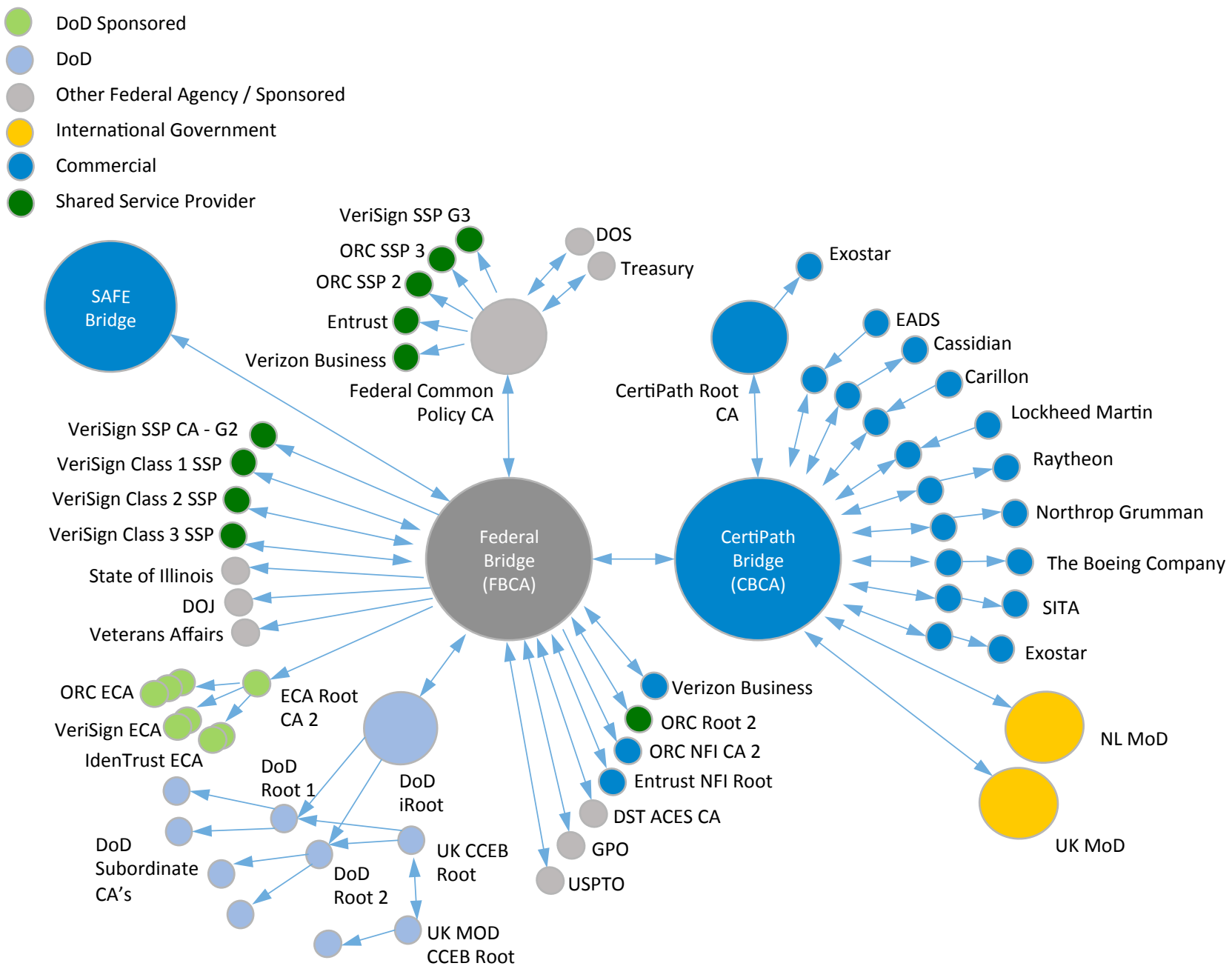
User Digitally Signs for Access



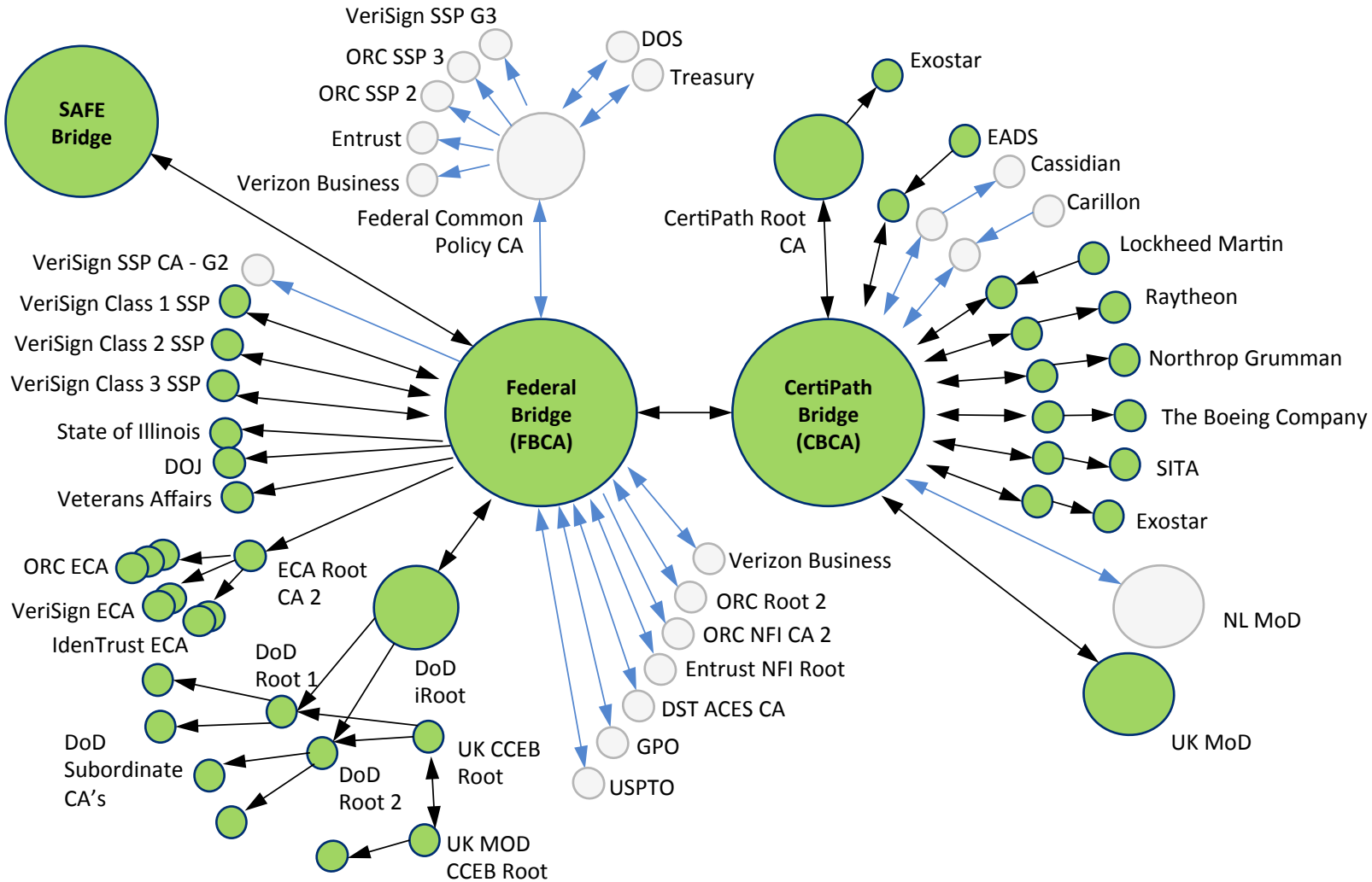
PKI-Digital Signature For Email or PC Login

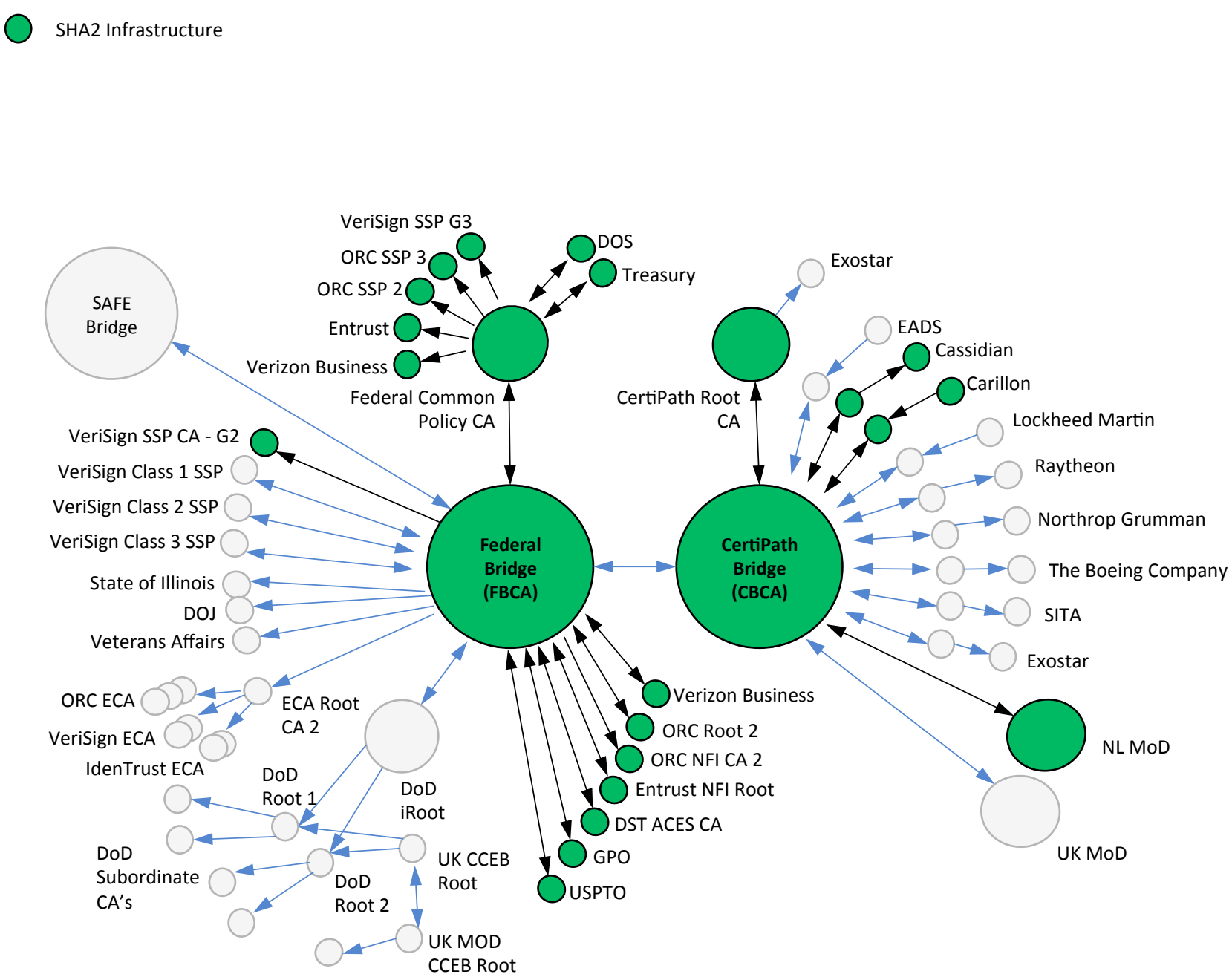
CertiPath

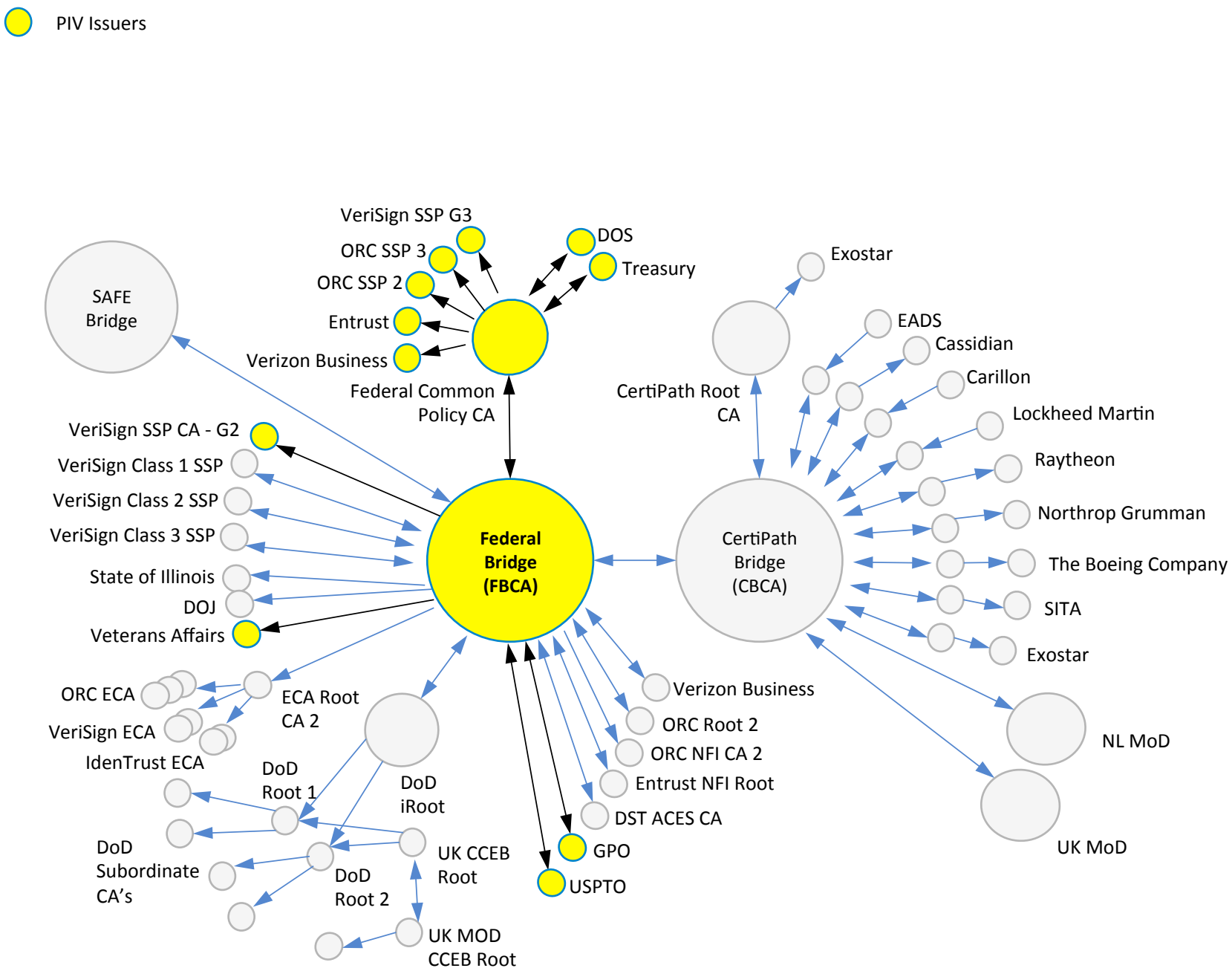
How LONG is the PKI Cloud Dog's tail?

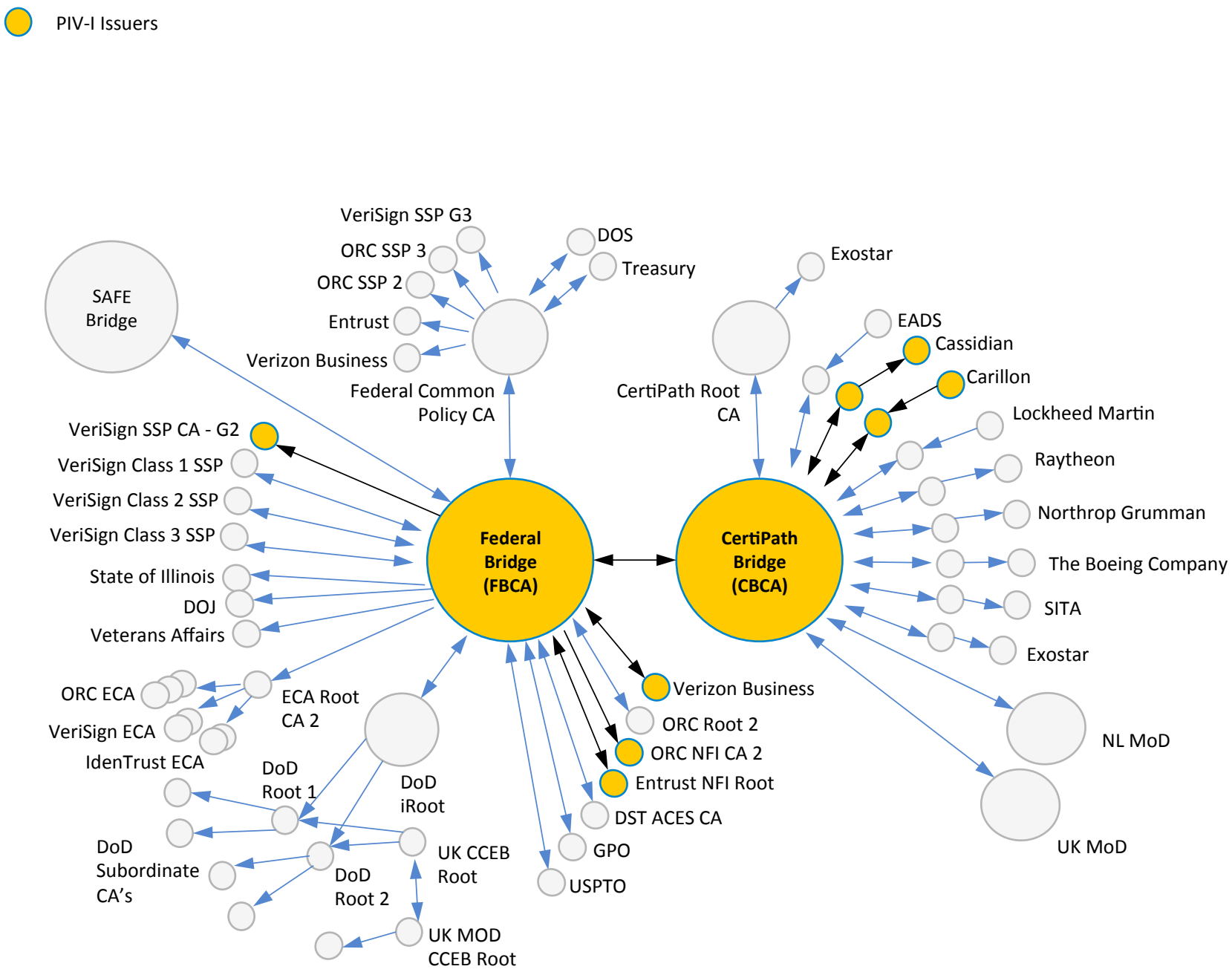

DoD Sponsored
DoD
Other Federal Agency / Sponsored
International Government
Commercial
Shared Service Provider
SAFE Bridge
VeriSign SSP G3
ORC SSP 3
ORC SSP 2
Entrust
Verizon Business
Federal Common Policy CA
DOS
Treasury
VeriSign SSP CA - G2
VeriSign Class 1 SSP
VeriSign Class 2 SSP
VeriSign Class 3 SSP
State of Illinois
DOJ
Veterans Affairs
Federal Bridge (FBCA)
ORC ECA
VeriSign ECA
IdenTrust ECA
ECA Root CA 2
DoD Root 1
DoD iRoot
DoD Subordinate CA's
DoD Root 2
UK CCEB Root
UK MOD CCEB Root
Verizon Business
ORC Root 2
ORC NFI CA 2
Entrust NFI Root
DST ACES CA
GPO
USPTO
CertiPath Root CA
Exostar
CertiPath Bridge (CBCA)
EADS
Cassidian
Carillon
Lockheed Martin
Raytheon
Northrop Grumman
The Boeing Company
SITA
Exostar
NL MoD
UK MoD

SHA1 Infrastructure




SHA2 Infrastructure
SAFE Bridge
VeriSign SSP G3
ORC SSP 3
ORC SSP 2
Entrust
Verizon Business
DOS
Treasury
Federal Common Policy CA
Exostar
CertiPath Root CA
EADS
Cassidian
Carillon
Lockheed Martin
Raytheon
Northrop Grumman
The Boeing Company
SITA
Exostar
VeriSign SSP CA - G2
VeriSign Class 1 SSP
VeriSign Class 2 SSP
VeriSign Class 3 SSP
State of Illinois
DOJ
Veterans Affairs
Federal Bridge (FBCA)
CertiPath Bridge (CBCA)
ORC ECA
VeriSign ECA
IdenTrust ECA
ECA Root CA 2
DoD Root 1
DoD iRoot
DoD Subordinate CA's
DoD Root 2
UK CCEB Root
UK MOD CCEB Root
Verizon Business
ORC Root 2
ORC NFI CA 2
Entrust NFI Root
DST ACES CA
GPO
USPTO
NL MoD
UK MoD


PIV Issuers
VeriSign SSP G3
ORC SSP 3
ORC SSP 2
Entrust
Verizon Business
DOS
Treasury
SAFE Bridge
Federal Common Policy CA
VeriSign SSP CA - G2
VeriSign Class 1 SSP
VeriSign Class 2 SSP
VeriSign Class 3 SSP
State of Illinois
DOJ
Veterans Affairs
Federal Bridge (FBCA)
Exostar
CertiPath Root CA
EADS
Cassidian
Carillon
Lockheed Martin
Raytheon
Northrop Grumman
The Boeing Company
SITA
Exostar
CertiPath Bridge (CBCA)
NL MoD
UK MoD
ORC ECA
VeriSign ECA
IdenTrust ECA
ECA Root CA 2
DoD Root 1
DoD iRoot
DoD Subordinate CA's
DoD Root 2
UK CCEB Root
UK MOD CCEB Root
Verizon Business
ORC Root 2
ORC NFI CA 2
Entrust NFI Root
DST ACES CA
GPO
USPTO


PIV-I Issuers
SAFE Bridge
VeriSign SSP G3
ORC SSP 3
ORC SSP 2
Entrust
Verizon Business
DOS
Treasury
Federal Common Policy CA
Exostar
CertiPath Root CA
EADS
Cassidian
Carillon
Lockheed Martin
Raytheon
Northrop Grumman
The Boeing Company
SITA
Exostar
VeriSign SSP CA - G2
VeriSign Class 1 SSP
VeriSign Class 2 SSP
VeriSign Class 3 SSP
State of Illinois
DOJ
Veterans Affairs
Federal Bridge (FBCA)
CertiPath Bridge (CBCA)
ORC ECA
VeriSign ECA
IdenTrust ECA
ECA Root CA 2
DoD Root 1
DoD iRoot
DoD Subordinate CA's
DoD Root 2
UK CCEB Root
UK MOD CCEB Root
Verizon Business
ORC Root 2
ORC NFI CA 2
Entrust NFI Root
DST ACES CA
GPO
USPTO
NL MoD
UK MoD

High Assurance Transactions – have many opportunities to fail

Server SSL Cert has expired

Issuing CA was tampered wit

Cross-certificate

Issuing CA's CRL has expired

SSL Cert has been re-keyed

Server SSL has been revoked

ate has a new Policy Constraint

Server SSL Cert was tampered with

ation

Issuing CA's CRL was tampered with

Server SSL Cert's CRL has expired

An OCSP Resp

's Cer

has been

Issuir

been re-keyed

SCA Re-key has occurred

Server SSL Cert's CRL was tampered with

Cross-certificate has a new Nam

Cross-certificate mpered with

Cross-certificate's CRL was tampered with

Unable to build path – AiA location offline

OCSP Responder Cert has expired

OCSP Responder Cert was tampered with

Server SSL Cert's CRL is offline

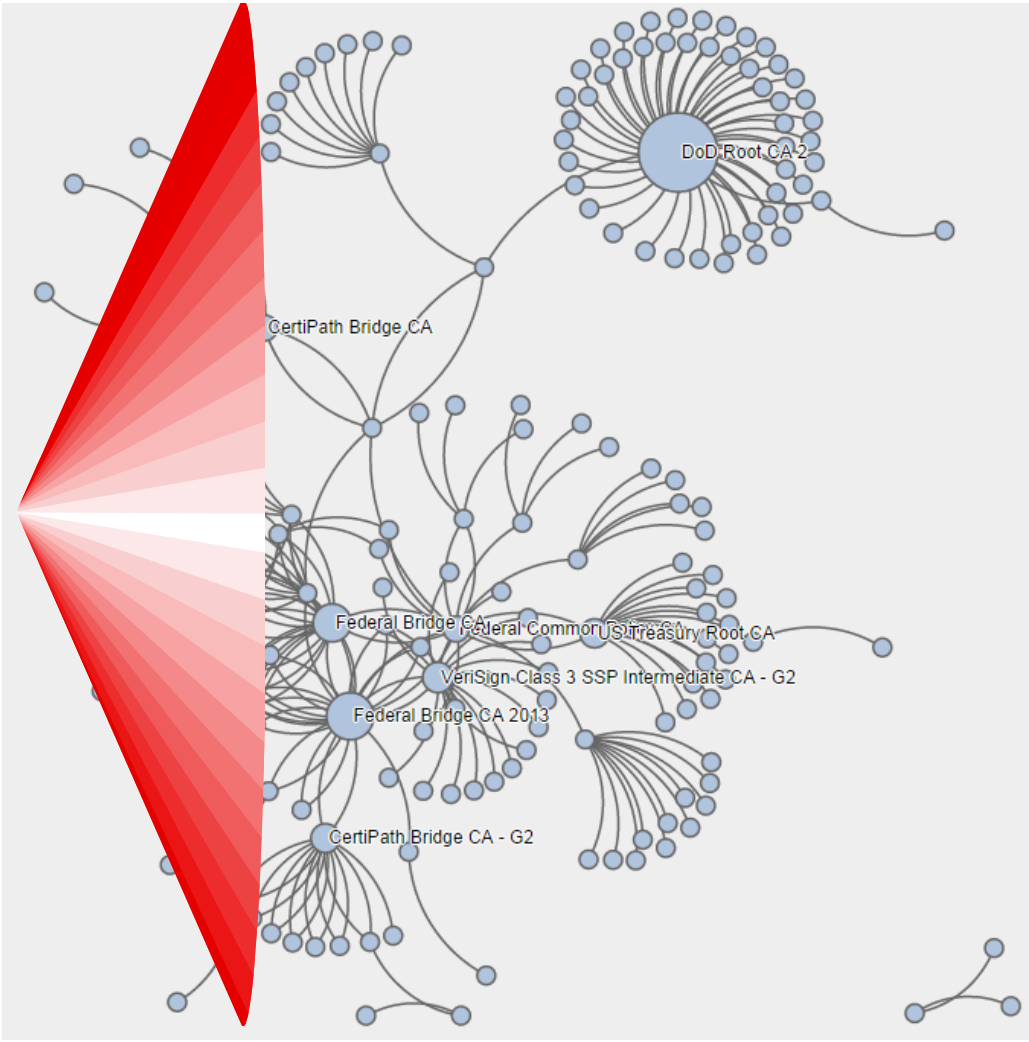
CertiPath

Oh By the Way…

- My E-PACS is NOT an island bounded by the Executive Branch
  - Regular access
    - Individuals having a trusted credential
    - Normal daily access to the facility
  - Visitors (***industry, legislative, judicial*** and ***state&local***)
    - Individuals having a trusted credential
      - PIV or PIV-I
    - Individuals *without* a trusted credential
      - Must issue facility access card
- Enterprise just took on a whole new meaning in scale
  - Prior to PIV and PIV-I, not feasible

Ultimately:
Continuous Monitoring is Required

Relying Parties need to know now what will happen in the next few days across a large portion of the trust fabric.



CertiPath

Summary

- ICAM is a good thing
  - Saves a lot of money avoiding redundant, silo'd processes
  - One credential, one human, one identity
    - And is it still valid!
- Nothing is perfect
  - Trust but verify…
  - Use the PKI!
  - Challenge the Card!
  - And be prepared for "issues" with cards from various issuers
- I wonder how mobile and derived credentials will change all this?