American Association of Airport Executives

AAAE BASIC Committee
18 August 2011

Understanding Federal Credentialing Standards and Changes on the Horizon

Salvatore D'Agostino
IDmachines LLC

Identity is 21st Century Critical Infrastructure

- Identity infrastructure and services provide the tools and technology to deliver trust, privacy and security to everyday transactions.
- Identity is at the base of any critical infrastructure compliance regime.
- National Strategy for Trusted Identities in Cyberspace
  - EU Stork, other
  - Minister of Identity in India
- Registration and Authentication is required for individuals and devices

A Federal Identity Credential Timeline

- 1991 Department of Defense DoD ID card
- 1995 Murrah building bombing Oklahoma City, OK, creation of Federal Security Levels
- 1997 Secure networks with smart card on Navy "Smart Battleship"
- ~2000 Common Access Card (CAC)
- 2003 Executive Office of the President OMB M-04-04 E-Authentication Guidance for Federal Agencies
- 2004 Homeland Security Presidential Directive (HSPD) 12, one credential for Federal employees and contractors for logical and physical access.
- 2005 National Institute of Standards (NIST) Federal Information Processing Standard (FIPS 201), Personal Identity Verification (PIV), Security Industry Association Quarterly Technology Update (QTU)

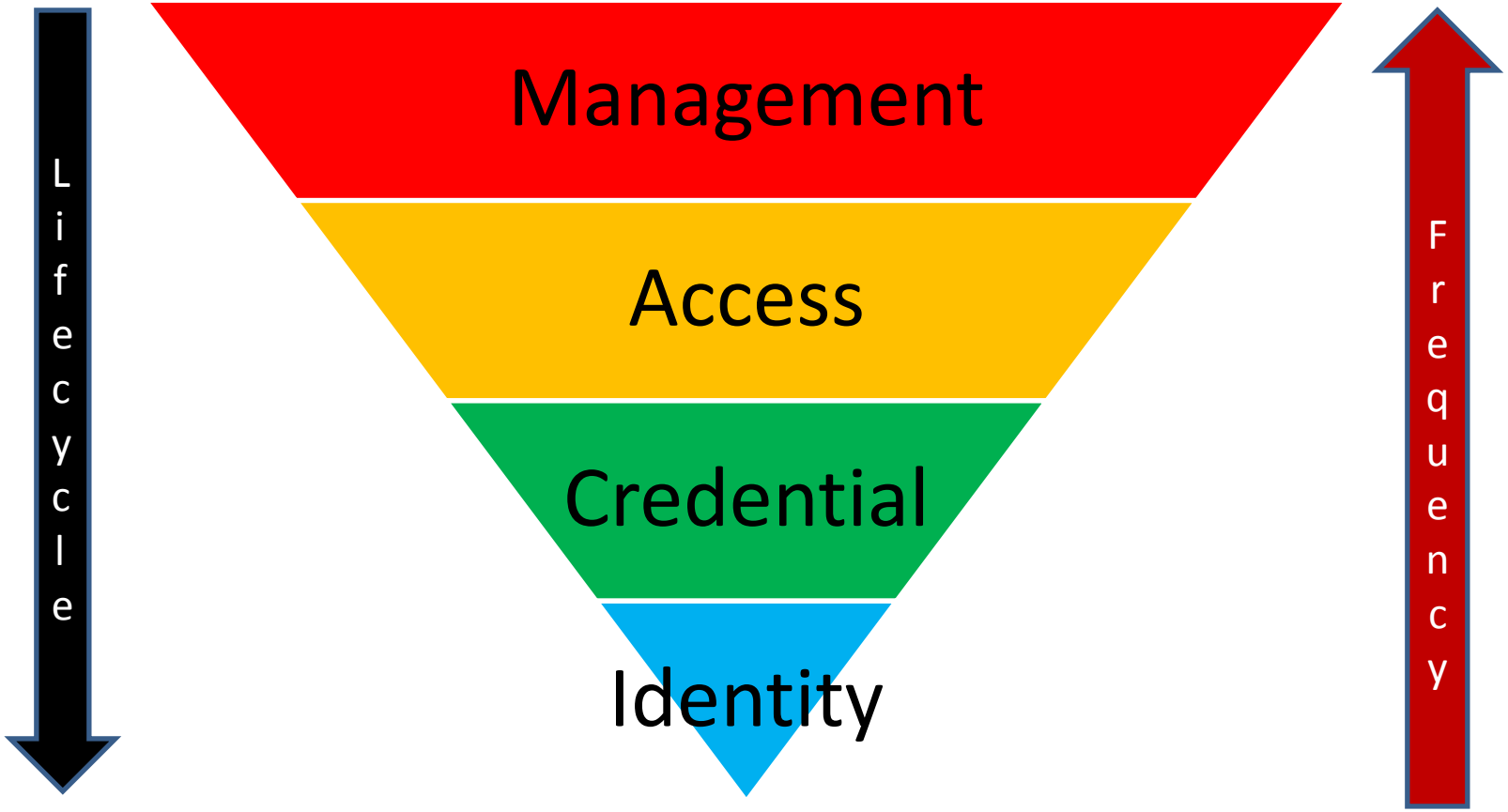
Copyright (c) IDmachines LLC 2011 all rights reserved

Last 5 Years

- 2006 First Responder Authentication Credential (FRAC), CertiPath Aerospace and Defense Industrial Base Bridge, initial Personal Identity Verification Interoperability (PIV-I) deployments
- 2007 Transportation Worker Identification Credential (TWIC)
- 2008 Special Publication 800-116, Guidance on Physical Access Control
- 2009 Federal Identity, Credentialing, and Access Management (FICAM) Roadmap, PIV-I baseline
- 2010 Draft National Strategy for Trusted Identities in Cyberspace (NSTIC), PIV-I 1.1, PIV-I FAQ, Department of Commerce; Cybersecurity, Innovation and the Internet Economy, Citizen and Commerce Class Common Certificate Policy.
- 2011 FIPS 201-2, FICAM part B, NSTIC, Federal PKI Policy Authority X.509 update …

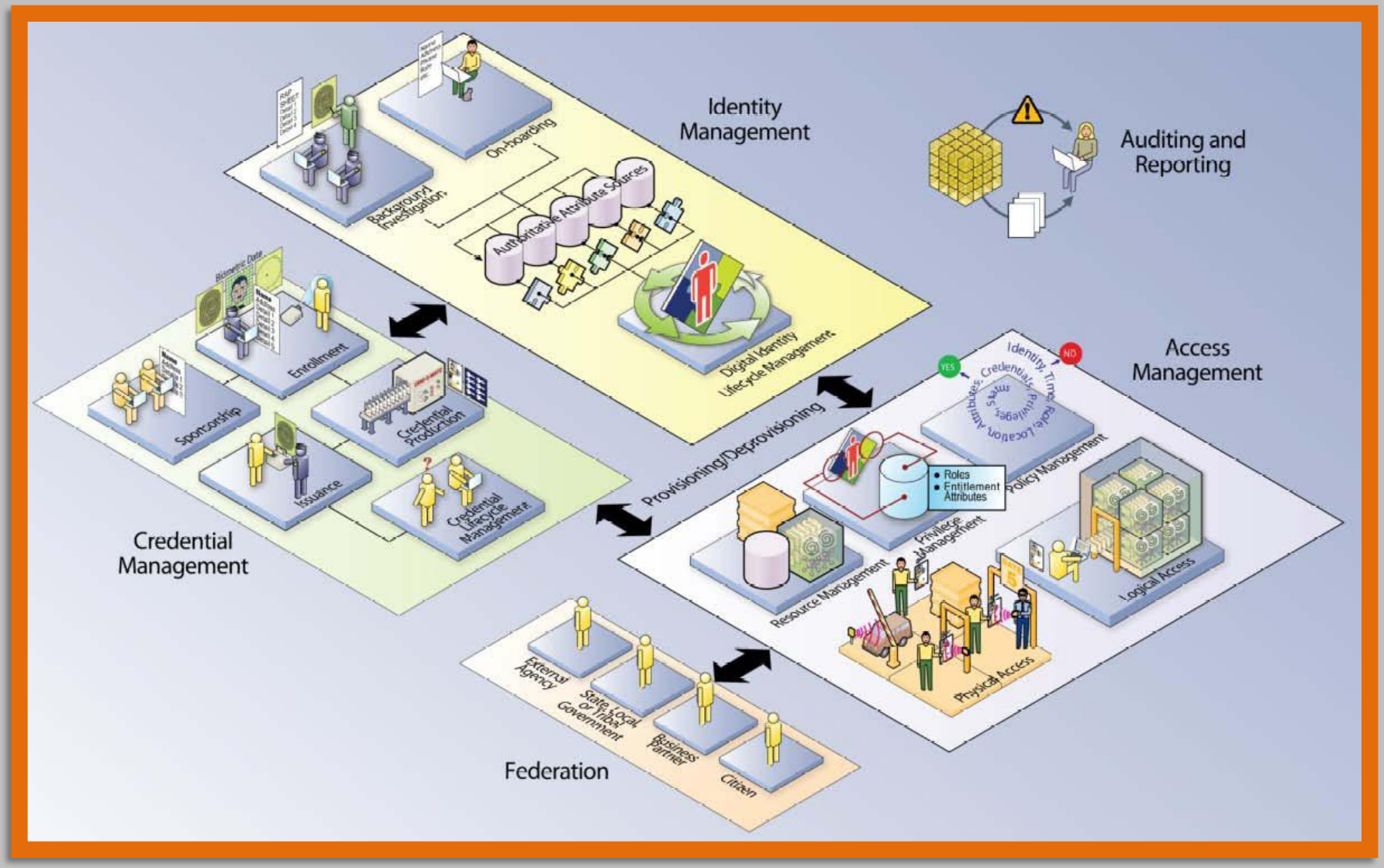
Copyright (c) IDmachines LLC 2011 all rights reserved

ICAM

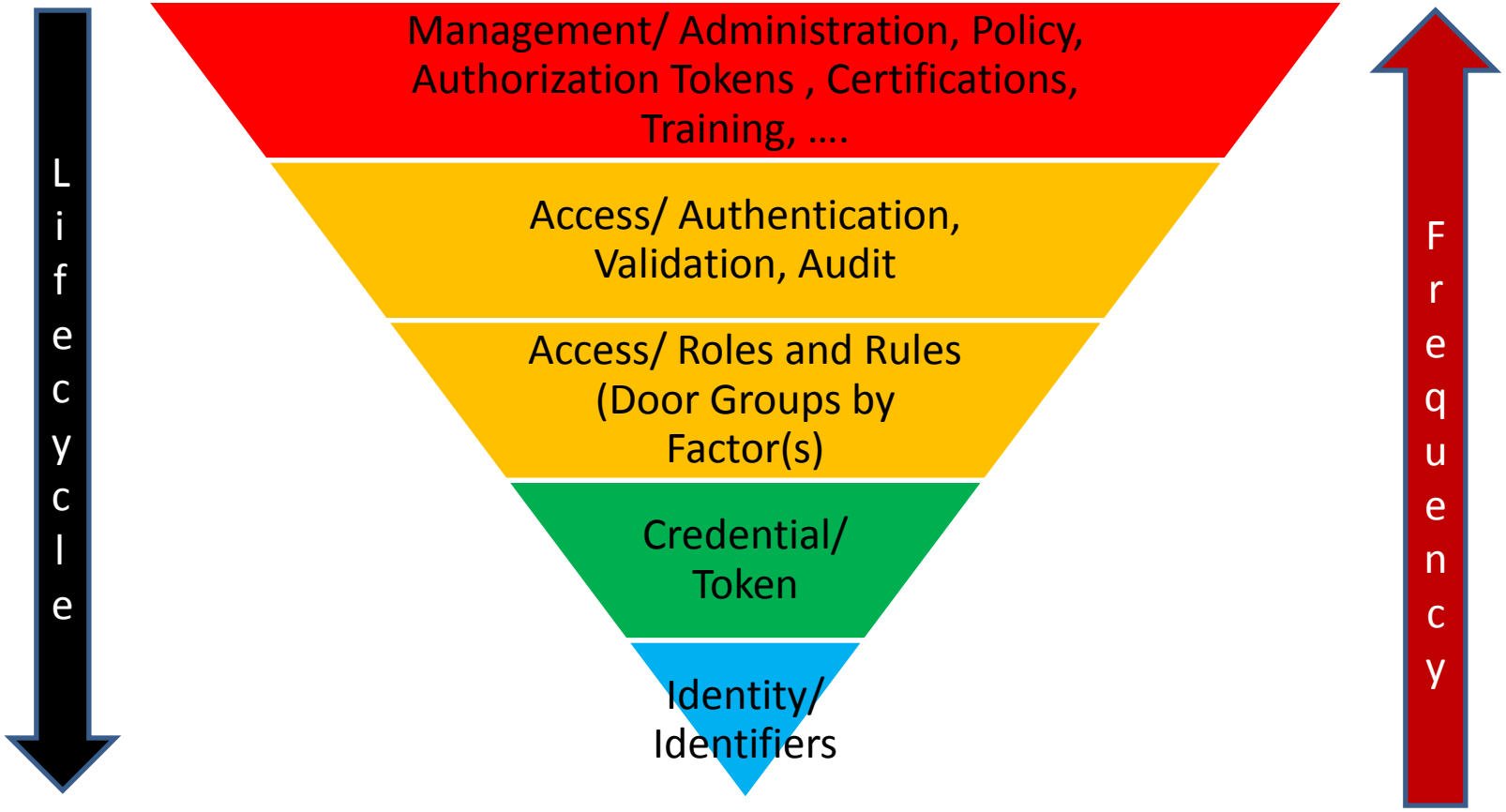


Copyright (c) IDmachines LLC 2011 all rights reserved

ICAM Roadmap Snapshot



ICAM outcomes



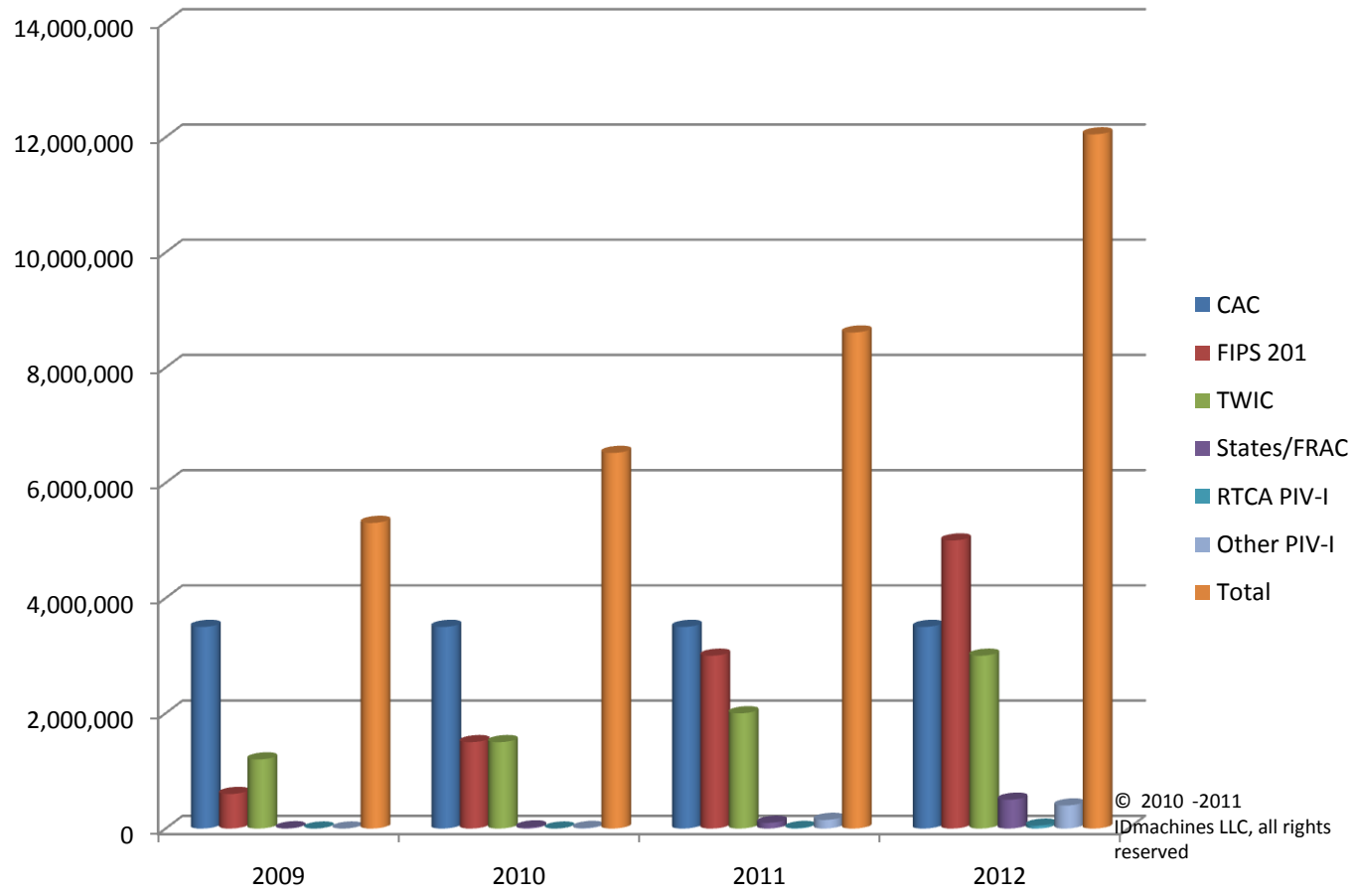
IDmachines
"Maximizing Identity"

Copyright (c) IDmachines LLC 2011 all rights reserved

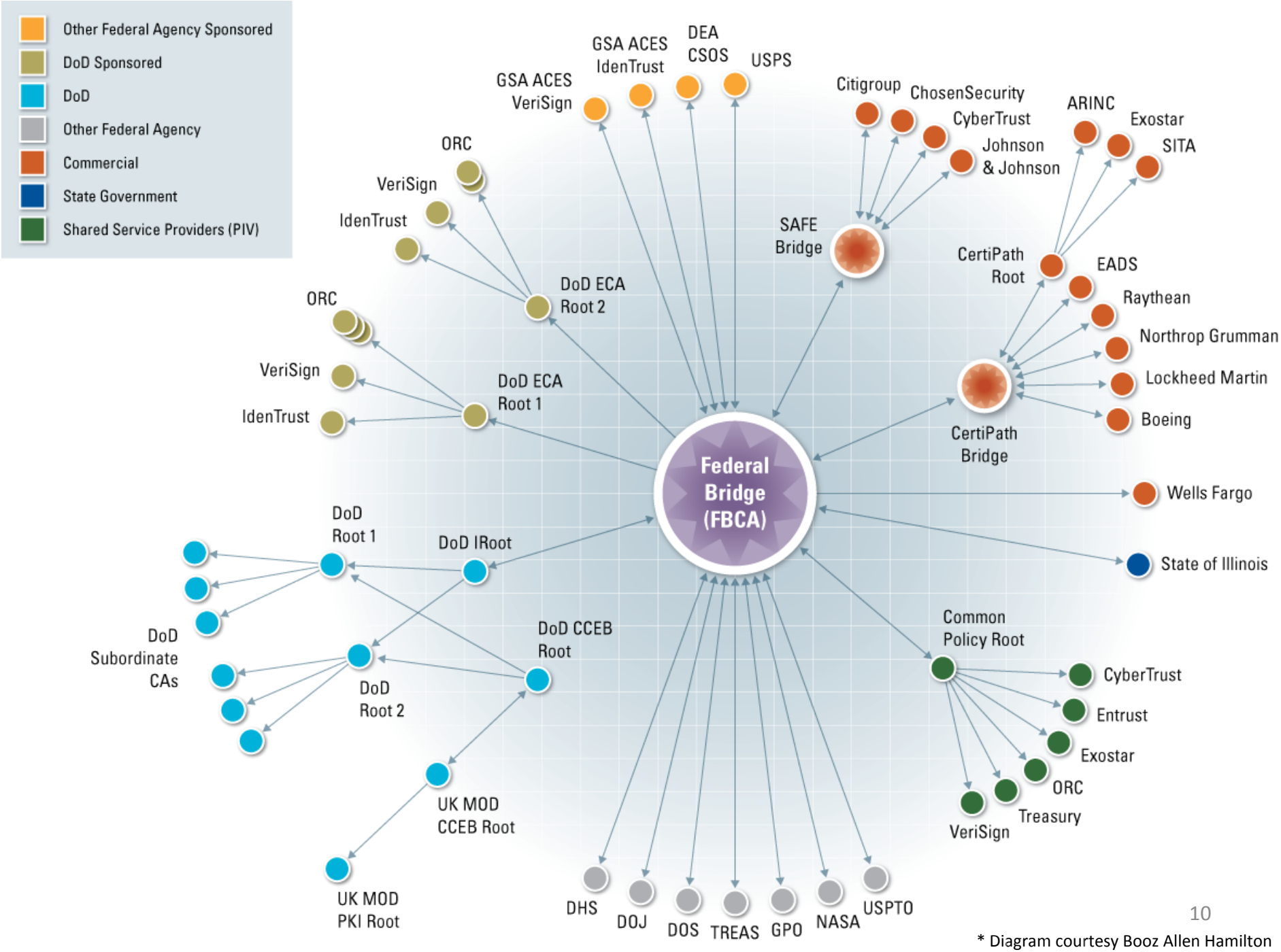
Personal Identity Verification Interoperability (PIV-I)

- Expanding the Federal Information Processing Standard 201 (FIPS 201) Personal Identity Verification (PIV) to Interoperability (PIV-I) to commercial enterprises, state and local governments, and other organizations.
- Initially with First Responders in the Washington, DC area (prior to PIV-I), e.g. Virginia
- Other industries and organizations adopting PIV-I framework
  - SAFE/Bio-pharma
  - CertiPath/Aerospace
  - Educause/InCommon/Education
  - Citibank, Other PIV-I issuers (even smaller firms)
  - UK Public Safety (e.g. Midlands Gateway Programme)
  - Other critical infrastructure starting; e.g. utility, transportation, etc.

IDmachines' PIV-I market estimate

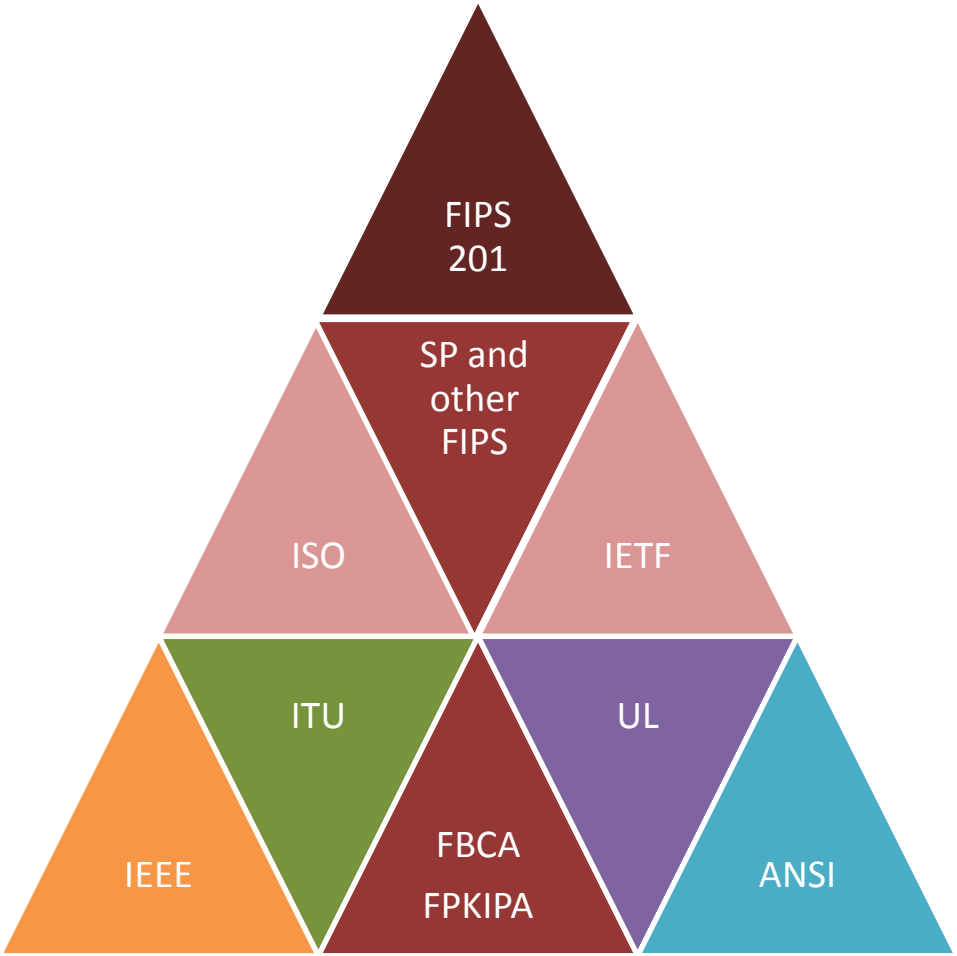


© 2010 -2011 IDmachines LLC, all rights reserved



* Diagram courtesy Booz Allen Hamilton

Standards Based Approach



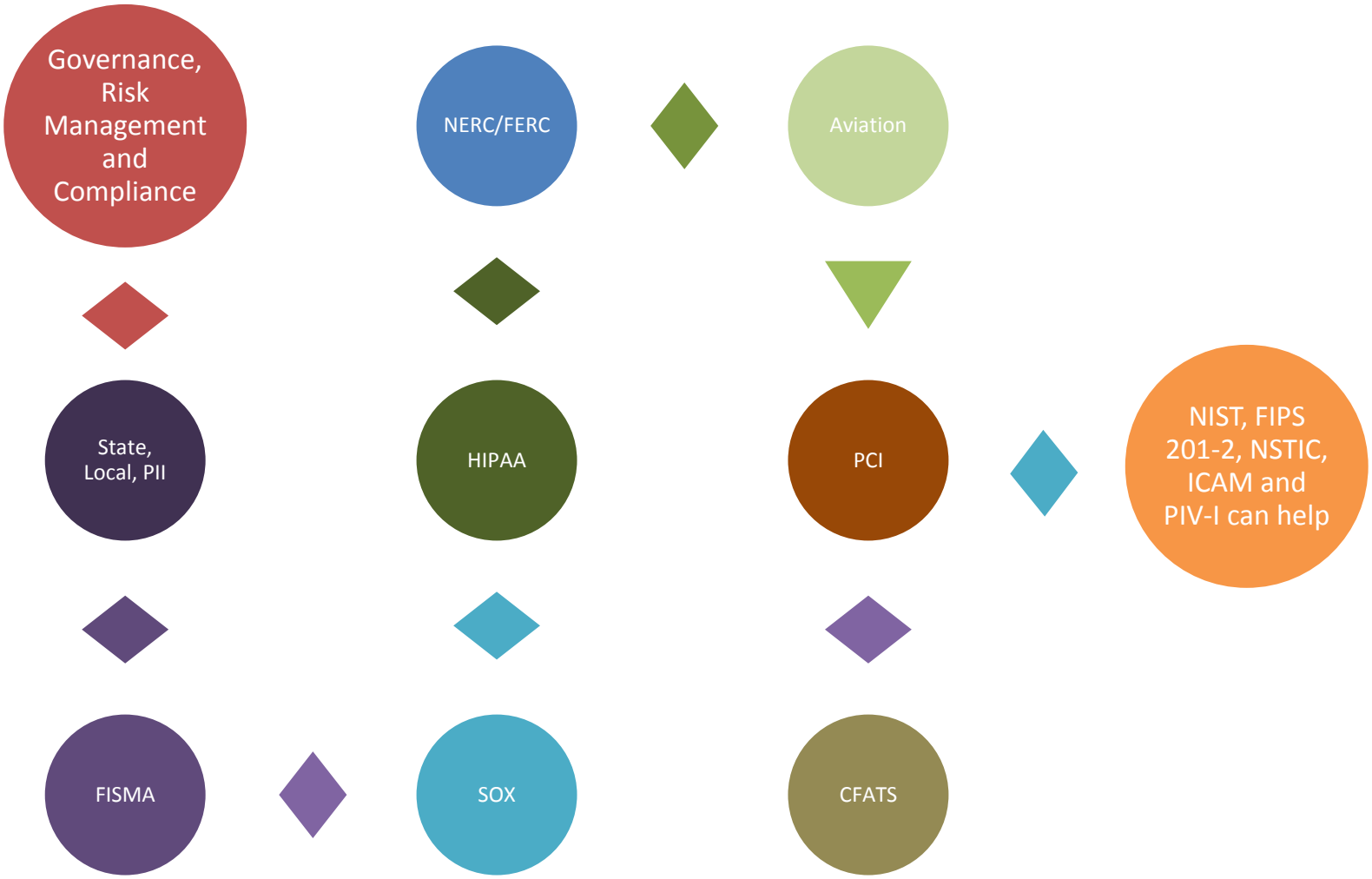
Copyright (c) IDmachines LLC 2011 all rights reserved

PIV-I Value

- Administration
  - Password reset (in exchange for PKI?)
  - Provisioning
  - De-provisioning
  - Identity lifecycle vs. Identity management
- Authentication
  - X.509 multi-factor
- Audit and Compliance
  - Privileged accountability
  - Common identity workflow
  - Enabling signatures
- Trust and Interoperability
  - PIV-I assurance level will meet most interoperability requirements
  - Identity registration

Copyright (c) IDmachines LLC 2011 all rights reserved

GRC ≡ Identity



Copyright (c) IDmachines LLC 2011 all rights reserved

FIPS 201-2 Top Ten

1. Asymmetric Card Authentication Key (CAK) is mandatory The Asymmetric CAK provides interoperability over the contactless interface. Previously optional, the CAK now provides a mandatory contactless Public Key Infrastructure (PKI) component. A symmetric CAK is also available as an option in addition to and in combination with the asymmetric key. This allows a practical approach to key management in a federated environment while providing options for speed and enterprise specific keys.
2. Introduction of enrollment record or chain of trust as maintained by the issuer. The document puts an emphasis on chain of trust with good reason particularly given the interoperability goals of FIPS 201. There are a number of reasons where the chain of trust helps to improve the economics and reduce the effort when you take lifecycle considerations into account. Some of these benefits of this include:
    1. Eliminates complete re-enrollment
    2. Eliminates recapturing biometrics
    3. Background Investigation (BI) may not need to be repeated
3. Iris recognition as an additional biometric modality is introduced. The draft proposes using a standard image (which then requires (non-standard) template/model creation and matching). Further testing and recognition rates were discussed and will likely be forthcoming and build on existing Iris Exchange (IREX) work at NIST. Iris biometrics bring benefits that include:
    1. Iris provides alternative in the case where fingerprints cannot be obtained as a basis of biometric binding of the individual to the credential.
    2. Iris can be used as an authentication method. There are an increasing number of vendors and applications use cases around iris matching and the draft now allows these to be part of an organizations identity toolkit.
4. Optional On Card Biometric Comparison (OCC) coincidentally called match on card. (Question here is should optional should be mandatory?) OCC use cases include enrollment, authentication, and PIN reset. Raising an interesting point on degrading the number of authentication factors if you combine PIN and BIO in the reset transaction.
5. ISO 24727 as a means of providing interoperability for smart card identification, authentication and digital signatures. It is a 6 part standard with the 6th part including a registration authority procedure. NIST also is active in committees to push the Generic ID-Card Command Set (GICS)
    1. NIST discussed registering a PIV authentication profile.
    2. Also provides secure channel features
        1. NIST also discussed a forthcoming Special Publication 800-xx on secure contactless communications.
6. Optional feature for card authentication to address issues related to the Rehabilitation Act and Section 508 and access to electronic and information technology procured by Federal agencies.
7. Maximum length of printed name (real issue is the length of the digital identifier - 128 bits for PACS)
8. Replace indicator for National Agency Check with Investigations (NAC-I) with a background investigation (BI) indicator. This addresses PIV-I where certain populations of cardholders are not applicable for a NAC-I. Indicates that a national BI indicator service would be put in place.
9. Allow post issuance updates to PIV card. This aligns with the desire to have the card live through two 3 year certificate cycles and have a 6 year life. This also ties to #2 chain of trust to enable the update.
10. Put employment eligibility verification background documents (I-9) into the FIPS 201 specification. This helped clarify some of the background document requirements as it represents the specific items accepted. Interesting not to have included a TWIC.

Copyright (c) IDmachines LLC 2011 all rights reserved

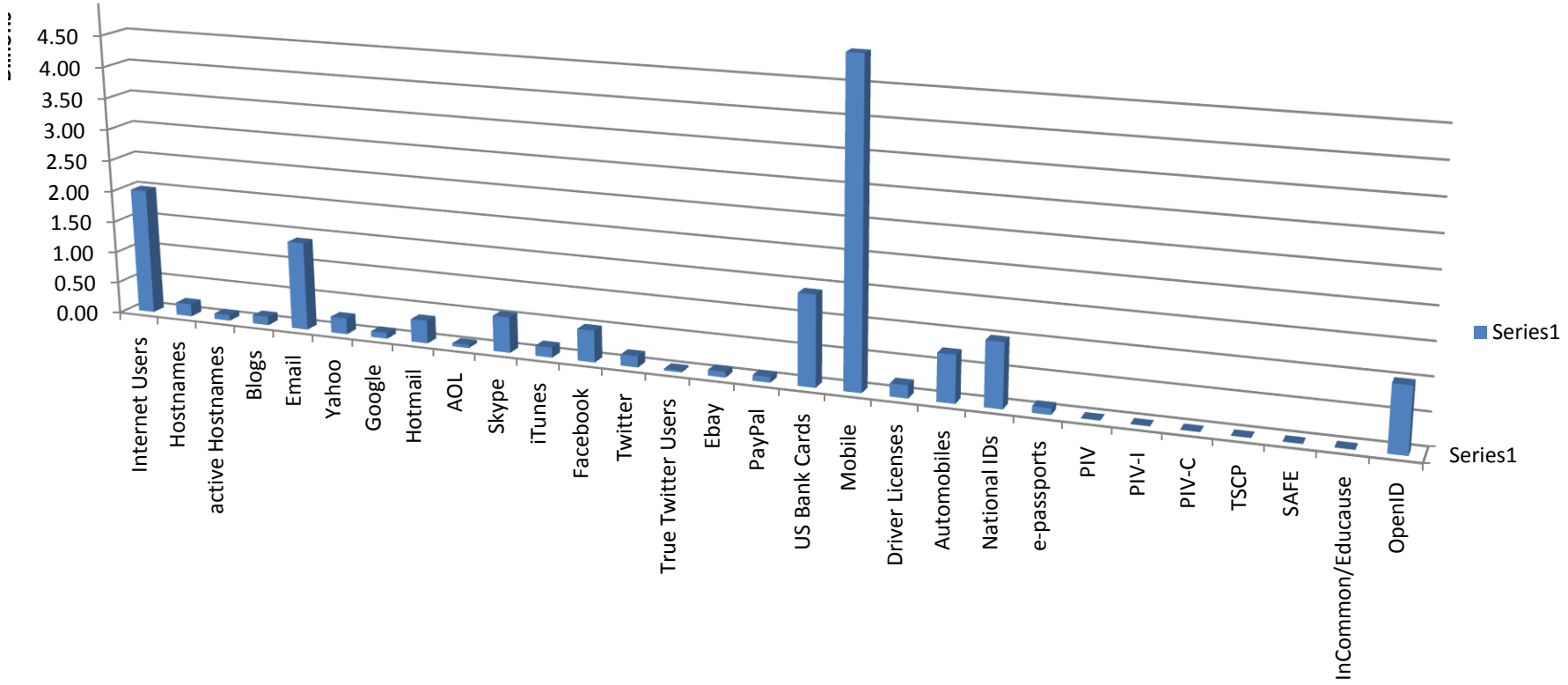
Beyond PIV-I other Levels of Identity

Assurance	Process Strength	Tokens
Level 1	Self-assertion minimum standards No liability with Identity Service Provider	Username and Password Open ID Foundation, Open Identity Exchange, Kantara Initiative CardSpace/InfoCard, and more (e.g. Mozilla, MyOneLogIn)
Level 2	On-line instant qualification, out-of band follow-up after transaction Mutually accepted liability.	Known (trusted?) identifier provider, e.g. Educause/Shiboleth/InCommon Shared secrets (pet's name), SAML, OAuth, JSON Web Tokens
Level 3	On-line out-of-band verification with transaction Limited personal liability some network liability.	Cryptographic solution One time password Soft certificates JWT Sign, Encrypt Machine identity
Level 4	In person proofing, separation of roles Biometrics Mixed service level liability	Cryptographic solution Hardware token **PIV, PIV-I**

IDmachines
"Maximizing Identity"

Copyright (c) IDmachines LLC 2011 all rights reserved

Identity and credential landscape



IDmachines

"Maximizing Identity"

Copyright (c) IDmachines LLC 2011 all rights reserved

Thanks, Questions

Sal D'Agostino
IDmachines LLC
1264 Beacon Street, #5
Brookline, MA 02446
sal@idmachines.com
http://idmachines.com
http://idmachines.blogspot.com
https://twitter.com/#!/IDmachines
http://www.facebook.com/IDmachines

IDmachines
"Maximizing Identity"

Copyright (c) IDmachines LLC 2011 all rights reserved