

8th Annual

DIGITAL IDWORLD

“Driving Innovation with Identity”

PRODUCED BY **CSO**

8th Annual

DIGITAL ID WORLD

"Driving Innovation with Identity"

PRODUCED BY

CSO

Identity Governance Frameworks

Marc Lindsey

Partner

***Levine, Blaszak, Block &
Boothby, LLP (“LB3”)***

www.lb3law.com

8th Annual

DIGITAL ID WORLD

"Driving Innovation with Identity"

PRODUCED BY

CSO

Introduction

- Key IdM participants:
 - **Subjects:** Individuals whose identify must be authenticated to provide access to info assets
 - **Identity providers:** Entities that identify and authenticate subjects and provide appropriate credentials to relying parties to support assertions by subjects
 - **Relying parties:** Entities relying on the identification and authentication from identity providers to verify subjects for electronic transactions

- Key IdM task and responsibilities
 - Establishing and updating identity attributes of subjects
 - Protecting privacy of subjects' personal information
 - Applying identity attributes to authenticate subjects
 - Establishing the scope of assertion for transactions
 - Employing technical measures to limit access by subjects
 - Using the assertion appropriately
 - Monitoring to detect, report and resolve incidents in system
 - Apportioning liability
 - False authentication
 - Misuse of, or fraudulent, assertions
 - Improper use or disclosure of personal information
 - Failure to implement or comply with IdM rules and negligence

8th Annual

DIGITAL ID WORLD

"Driving Innovation with Identity"

PRODUCED BY

CSO

Framework Approaches

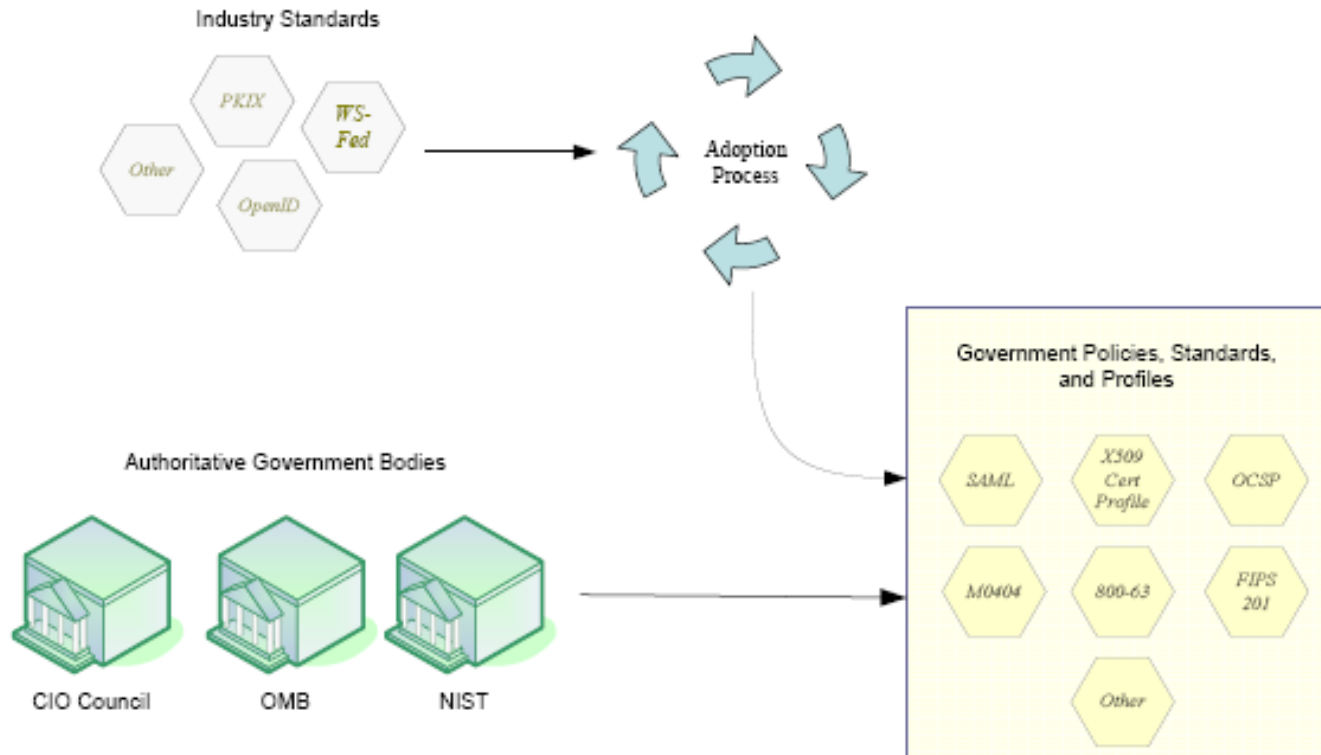
- Components of a comprehensive framework
 - Appropriate (open) technical standards
 - Clearly defined and fairly balanced rights, roles and liabilities
 - Written policies, rules and guidelines
 - Contracts between participants (with SLAs)
 - Compliance certification and audit process
 - Enforcement mechanisms with meaningful incentives to behave

- Four basic governance framework approaches
 - Statutory or regulatory mandates
 - Dominant participant dictated standards
 - Private party agreements
 - Voluntary standards

- In the U.S., there are no regulatory or statutory regimes specific to IdM but:
 - FFIEC authentication guidelines for banks
 - Federal Identity, Credential and Access Management committee (ICAM) approval process launched July 9, 2009
 - ICAM agencies are evaluating standards frameworks *and* vetting identity providers

- ICAM’s evaluation criteria depend on level of assurance required
 - Level 1: Little or no confidence in the asserted identity’s validity
 - Level 2: Some confidence in the asserted identity’s validity
 - Level 3: High confidence in the asserted identity’s validity
 - Level 4: Very high confidence in the asserted identity’s validity
- No standard above level 1 has been approved by ICAM

ICAM Scheme Adoption Process



- **ICAM identity provider (TFPs) criteria**
 - **Registration and Issuance** – How well does the identity provider register and proof the identity of the credential applicant and issue the credential to the approved applicant?
 - **Tokens** – What is the identity provider's token technology and how well does the technology intrinsically resist fraud, tampering, hacking, and other attacks?
 - **Token and Credential Management** – How well does the identity provider manage and protect tokens / credentials for the life cycle?
 - **Authentication Process** – How well does the identity provider secure its authentication protocols?
 - **Assertions** – How well does the identity provider secure assertions, if used, and how much information is provided in the assertion?
- Yahoo, Google and PayPal under review

- Key points regarding ICAM's approval processes
 - May embrace specific technologies
 - Determinations are not applicable to private party transactions, but could form *de facto* standards for private industry
 - Courts often give considerable deference to standards adopted by/for the federal government, which could provide safe harbors for private parties
 - Can the federal government's approach to liability as a relying party translate to the private sector?

- **Single-Party Dictate**
 - Entity with market power establishes IdM rules it will employ and requires participants to comply with those rules
 - Key points
 - Legal protections for any participant other than the dictator are likely to be insufficient
 - Serious judicial scrutiny is likely, and raises serious questions as to the reliability of this sort of unilateral framework – particularly when consumers are involved
 - It is unlikely that this approach will support any serious financial transactions between commercial parties
 - Utility limited to technical standards

- Private Party Agreements
 - Identity provider and relying parties enter into contracts allocating responsibility and liability
 - Key points
 - Protections for subjects may not be covered adequately in provider-relying party negotiations
 - Protections are as good as the negotiated outcome
 - Not easily extensible because every framework is negotiable
 - Works well for large enterprise subjects or relying parties
 - Use leverage to obtain high standards and service levels (SLAs)
 - Allocate risk consistent with corporate policies and risk tolerance
 - Build-in compliance program with audit rights
 - Contract Ts&Cs may not withstand judicial scrutiny if not sufficiently protective

- Voluntary standards
 - Industry standards model
 - Single entity (either existing or created by industry players) drafts, adopts and enforces standard rules
 - Participants agree by contract to be bound by the standards
 - Not typically open – members may contribute proprietary specifications, and public comments non-existent or limited
 - Examples: InfoCard, SAML, and WS-Federation but these are technical in nature; SAFE BioPharma; CertiPath (Aerospace)

- Voluntary standards (cont'd)
 - Open guidelines / standards model
 - Standards body drafts and/or adopts standards using “open” process (public notice, comment, and subsequent revisions)
 - Providers agree to comply voluntarily
 - Standards are then incorporated into each transaction facilitated by complying providers
 - Enforcement occurs typically through private causes of action between parties – not through the standards body
 - Examples: OpenID, Kantara Initiative?

- Voluntary standards (cont'd)
 - Key points
 - Protections for subjects may not be covered adequately unless consumer advocacy groups participate in standards setting process
 - Historically, service levels are missing
 - Unclear whether courts will accept rules as adequate but certain features will improve the likelihood
 - Meaningful initial certification process
 - Periodic independent audits of compliance
 - Sanctions for non-compliance
 - Standards should be updated to keep pace with gaps identified and other reasonable safeguards as they emerge

Conclusion

- Some industry-specific comprehensive frameworks are under development but most generally applicable frameworks have focused on technical standards
- SSO across entity domains in the U.S. are handicapped by immature / incomplete approaches to legal liability apportionment and stable laws
- For now, participants in “trust circles” protect themselves by combining approaches
 - Forming industry-specific groups to set standards
 - Vetting thoroughly their trusted partners’ approach to IdM
 - Negotiating effective custom agreements with SLAs
 - Relying on judicial interpretations of negotiated protections

Contact Information

Marc Lindsey

Levine, Blaszak, Block & Boothby, LLP

MLindsey@LB3Law.com

202.857.2550