The Imperative for High Assurance Credentials: State Identity Credential and Access Management (SICAM) Guidance and Roadmap

AAMVA Region I Conference
E-ID, DLDV, and Privacy – Conducting Business Securely
July 15, 2013

Chad Grant, Senior Policy Analyst
National Association of State Chief Information Officers
About NASCIO

- National association representing state chief information officers and information technology executives from the states, territories and D.C.
- NASCIO's mission is to foster government excellence through quality business practices, information management, and technology policy.
- Founded in 1969 – we’re a legacy system
Fiscal recovery uneven, slow revenue growth, budgets are better, federal deficit reduction impact?

CIOs seeking IT operational cost savings and alternative IT sourcing strategies

Opportunities for change and innovation

Living with the past - modernizing the legacy

IT security and risk! Game has changed

IT workforce: retirement wave, skills, recruiting

State CIO transition – major churn
CIOs' view on IT budgets for 2013

- 80% of Federal grant money is going to states.
- In the past, many CIOs saw budget decreases as an opportunity to improve by breaking down barriers, strengthening IT governance, and developing creative solutions.
- Optimistic outlook by state CIOs on IT budgets - 47% anticipate an increase for 2013.

Source: NASCIO Midyear Conference, May 2012
View from the States: Priorities and Trends
State CIO Priorities for 2013

1. **Consolidation / Optimization**: centralizing, consolidating services, operations, resources, infrastructure, data centers, communications and marketing "enterprise" thinking, identifying and dealing with barriers

2. **Cloud Services**: scalable and elastic IT-enabled capabilities provided "as a service" using internet technologies, governance, service management, service catalogs, platform, infrastructure, security, privacy, data ownership, vendor management, indemnification, service portfolio management

3. **Security**: risk assessment, governance, budget and resource requirements, security frameworks, data protection, training and awareness, insider threats, third party security practices as outsourcing increases, determining what constitutes "due care" or "reasonable"

4. **Mobile Services / Mobility**: devices, applications, workforce, security, policy issues, support, ownership, communications, wireless infrastructure, BYOD

5. **Budget and Cost Control**: managing budget reduction, strategies for savings, reducing or avoiding costs, dealing with inadequate funding and budget constraints

6. **Shared Services**: business models, sharing resources, services, infrastructure, independent of organizational structure, service portfolio management, service catalog, marketing and communications related to organizational transformation, transparent charge back rates, utility based service on demand

7. **Health Care**: the Affordable Care Act, health information and insurance exchanges, health enterprise architecture, assessment, partnering, implementation, technology solutions, Medicaid Systems (planning, retiring, implementing, purchasing), eligibility determination

8. **Legacy modernization**: enhancing, renovating, replacing, legacy platforms and applications, business process improvement

9. **Interoperable Nationwide Public Safety Broadband Network**: planning, governance, collaboration, defining roles, asset determination

10. **Disaster Recovery / Business Continuity**: improving disaster recovery, business continuity planning and readiness, pandemic flu / epidemic and IT impact, testing

Source: NASCIO State CIO Survey, November 2012
IT Security Risks in the States

- Critical infrastructure protection
- More aggressive threats – organized crime, unorganized crime, hacktivism
- Spam, phishing, hacking, and network probes up
- Advanced persistent threats
- Data breaches – trust impact!
- Insider threats, third party
- Securing mobile solutions, BYOD
- Identity and Access Management
- Inadequate funding
Priority Technologies, Applications and Tools

1. Cloud computing: software as a service, infrastructure, platform, storage
2. Mobile workforce technologies
3. Virtualization: servers, desktop, storage, applications, data center
4. Legacy application modernization / renovation
5. Identity and access management
6. Enterprise Resource Planning (ERP)
7. Security enhancement tools
8. Networking: voice and data communications, unified
9. Business Intelligence (BI) and Business Analytics (BA) applications, Big Data
10. Document/Content/Records/E-mail management: active, repository, archiving, digital preservation

Source: NASCIO State CIO Survey, November 2012
Levels of Maturity and Adoption of Identity and Access Management

Source: 2012 Deloitte-NASCIO Cybersecurity Study
State CIOs Recognize Why Identity Management Needs to be a Top Priority

- Support for a national framework that provides interoperability and trust across multiple jurisdictions.
- Promotes state enterprise approach: avoids silos, avoids proprietary solutions. Adoption of the standards will reduce redundant credentialing efforts and expenditures.
- Follows the great work the states have led in improving drivers license issuance. Provides strong proof of cardholder identity.
- Supports multiple applications & legacy infrastructure: issue once, use many times.
- Enables standards-based provisioning of access management and auditing.
State Government Challenges

- Attacks on identity services
- Real-time provisioning and de-provisioning of user accounts (life cycle management)
- Insider threats
- Least privilege/need to know (privacy preservation)
- Password management
- User-centric access control
- Dynamically scale up and down
- Interoperability with existing IT systems and solutions
- Multi-jurisdictional compliance
Business Drivers

Enabling Services and Workflow
- Improve trust in the digital identity
- Streamline and re-engineer business processes
- Improve fraud detection

Enterprise Data Sharing and Management
- Support data sharing and interoperability
- Permits cross-departmental data analysis and forecasting
- Promotes evidence-based policy making

Protecting Critical Assets
- Supports multiple risk and access levels
- Access auditing
- Security, privacy, compliance
- Secure authentication

Operational Efficiencies
- Standards-based approach
- Simplified sign-on
- Automatic provisioning
- Password resets

Critical Service Capabilities

SICAM Guidance and Roadmap Business Drivers
If Digital Identity is a Priority…

What we should not do

- each state work independently
- use proprietary solutions
- disregard interoperability and a federated approach

What we should do

- Document and benchmark ROI elements and share business drivers and solutions
- Incorporate identity and access management into the existing enterprise architecture
- Harmonize public and private efforts through adoption of the NSTIC guiding principles
SICAM Document Background

- **Who participated**
  - NASCIO Digital Identity Working Group participants were from both public and private sector

- **Purpose**
  - Provide a standard, unified framework for all states to utilize and adopt
  - Provide definitions, architectural guidance, and describe processes
  - Develop a baseline for further discussion and improvement by NASCIO community

- **Scope**
  - Evangelize the business drivers of SICAM
  - Break down identity silos and streamline services
  - Compliance with existing law, regulations, standards, and state policies
  - Improve interoperability
  - Enhanced privacy and customer service (protect PII)
SICAM Document Overview

- Goals and Objectives
  - Trust
  - Interoperability
  - Security
  - Process Improvements
- SICAM Model for Assurance Levels
- Principles, Processes, and Concepts
- Architecture Framework
- Implementation Strategy
  - Risk Assessment
  - Assurance Levels
  - Identity Proofing Requirements
  - Attribute Management
  - Governance
  - Architecture Compliance
Looking Ahead

- Call-to-Action for state leaders to include IdM as a domain within existing EA Frameworks
- Take an active role in the identity ecosystem
- Evangelize the business drivers and highlight ROI
- Identity implications for reforming social programs?
- Demand for secure identities by citizens
- Reduce cyber risks!
Connect with...

nascio.org
facebook.com
linkedin.com
youtube.com/nasciomedial
twitter.com/nascio