Trust and Interoperability with PIV-I: Recommendations from the NASCIO State Digital Identity Working Group

Achieving the benefits of an integrated enterprise strategy for digital identity is a focus and challenge for State CIOs. Currently, states maintain a variety of duplicative identity records for their residents as well as a plethora of credentials associated with those identity records —including driver's licenses, benefits cards, emergency response official badges, systems passwords and many others. As a result, a single person carries multiple credentials for a single common purpose: to prove that person's identity as the basis for granting a privilege. Maintaining these redundant systems is costly, inefficient, and rife with security risks—both for the state as well as the resident.

If states were able to consolidate their many identity records—and the credentials associated with those identity records—they could save time, money and improve service delivery. They could also improve customer convenience, access to services, and personal information security.

Following a standardized approach to digital identity, states could issue credentials that are trusted and interoperable not only at state agencies, but at county and city agencies as well. Reliance on that single credential need not stop at the state border, however; other states and even commercial entities, trusting that the credential was issued in the defined standardized process, could also accept and rely upon that credential. With the appropriate technology and coordination, states could help residents greatly increase the security of their online transactions, whether the relying entity is a governmental or commercial enterprise.

In this document, the NASCIO State Digital Identity Working Group offers information and recommendations for state CIOs as they contemplate their own digital identity initiatives.

1. Focus on Four Key Principles

In order for states to realize the benefits of consolidated, interoperable credentials, they will need to focus on four very important principles:

1. ***Trust*** - so that entities that wish to accept the credential (called "relying parties") can be sure that the entity that issued the credential (called the "issuing party") followed a defined process to make sure that the person holding the credential is in fact the person identified by the credential. This can take the form of a standardized and audited enrollment (sometimes called "identity proofing") process.

2. ***Interoperability*** - so that the credential is readable by those relying parties. This is primarily a technical matter, ensuring use of compatible hardware and software through adherence to a broadly accepted technical standard.

3. ***Security*** - so that personal information as well as issuing party and relying party systems are protected.

4. ***Process Improvements*** - that are enabled when relying parties take advantage of the trusted, interoperable and secure identity and associated credential. It is through this progression that the cost and efficiency benefits may be achieved.

2. Use An Existing, Non-proprietary Standard

Without broad adoption of a single standard, relying parties will not be able consistently to trust or read credentials issued by others. Thus, as a first step toward developing their digital identity initiative, states must select a standard to which they can adhere both as an issuer and as a relying party.

There are few options for states looking for a comprehensive, non-proprietary trust and interoperability standard for smart chip credentials. The federal government has issued defined standards for this purpose – *Federal Information Processing Standard (FIPS) 201, Personal Identity Verification (PIV) of Federal Employees and Contractors,* and the non-federal version of PIV, *Personal Identity Verification Interoperability for Non-Federal Issuers (PIV-I).* The Federal CIO Council distinguishes between the two as follows:

- **PIV** – an identity that is fully conformant with federal PIV standards (i.e., Federal Information Processing Standard (FIPS) 201 and related documentation). Only issued by federal entities can be fully conformant. Federal standards ensure that PIV is interoperable with and trusted by all Federal government relying parties.

- **PIV Interoperable** – an identity that meets the PIV technical specifications to work with PIV infrastructure elements such as readers, and is issued in a manner that allows Federal government relying parties to trust the identity.[1]

In the case of interoperability standards in general, adoption makes further adoption more attractive. PIV-I is no exception, and as states elect to issue PIV-I credentials, other states have been more inclined to adhere to that same standard in order to enable interoperability and trust across jurisdictions, including the federal government, which issues PIV credentials and accepts PIV-I credentials. For credentials based on smart chips, PIV and PIV-I are the leading standards in the public sector. Currently, more than 16 states—including Colorado, Illinois and the Commonwealth of Virginia— are pursuing some form of PIV-I strategy, driving toward trust and interoperability both within each state, but also among them.[2]

Many states currently issue or rely upon credentials such as the First Responders Authentication Credential (FRAC), the Airport Credential Interoperability Solutions (ACIS) and the Transportation Worker Identity Credential (TWIC). Like the PIV, these credentials, too, can be trusted and interoperable under PIV-I. Given these many benefits leading to broader trust and interoperability, the NASCIO Digital Identity Work Group recommends that State CIOs build their digital identity solutions to comply with the PIV-I standard.

State-issued PIV-I credentials could be used for functions such as—

- Physical Security, including facility access and video analytics
- Logical Access, including network and application access
- Incident monitoring and response
- Encryption and protection of sensitive data

3. Choose the Right Path for Your State: Key Considerations

Given the current economic climate, governors may be hesitant to support new digital identity credentialing initiatives without convincing evidence that the initiatives will improve efficiencies and convenience for both users and issuers. Commercial entities, too, will need to realize improve efficiency and security of commercial transactions, including on-line transactions, if they are to rely upon a state-provided digital identity. Below are a few key questions states should consider as they contemplate implementing such a program:

- Has your state identified ways to implement an identity management system that is sustainable or can demonstrate a measureable return on investment?
- What state programs would be strong candidates for using an interoperable identity credential, particularly at the beginning of your program? Some to consider:
    - Entitlement programs such as Medicaid and Medicare
    - Emergency response such as the First Responder Authentication Credential program (FRAC)

- Health care information exchange
- Enterprise-wide identity and access management programs
- Cloud Computing
- Digital Records Management

- Has your state defined the key functional requirements for a digital identity program, and what are the processes, policies and technologies available to achieve these goals?
- Is your state's political and fiscal landscape conducive to such a project, and has your state considered the cost, security and privacy implications of digital identity initiatives?

4. Share Your Experiences with Other State Programs

Through its Digital Identity Working Group, NASCIO brings key state implementers together to share best practices and information critical to successful identity programs. Multi-agency, multi-state trust and interoperability require agreement and coordination among not only issuing parties, but among relying parties, as well. The Working Group urges NASCIO members to participate in the group's calls and meetings and to share with other state members their experiences and views.

For more information contact:
Chad Grant
Policy Analyst
National Association of State Chief Information Officers (NASCIO)
201 East Main Street, Suite 1405
Lexington, KY 40507
Phone: 859.514.9148
Email: cgrant@AMRMS.COM

[1] "Personal Identity Verification Interoperability for Non-Federal Issuers," Version 1.1, Federal CIO Council, July 2010. http://www.idmanagement.gov/drilldown.cfm?action=pivi_cross_cert
[2] "Personal Identity Verification Interoperability (PIV-I) for Non-Federal Issuers: Trusted Identities for Citizens across States, Counties, Cities and Business." Smart Card Alliance, January 2011. http://www.smartcardalliance.org/articles/2011/02/03/piv-i-credentials-provide-efficiency-and-trust-for-state-and-local-governments-according-to-new-smart-card-alliance-white-paper