Governments Struggle to Gain Trust in Online Identity Management (Opinion)

Many challenges remain to establishing digital identities, but state and local governments must act quickly.

BY DAN LOHRMANN (HTTP://WWW.GOVTECH.COM/AUTHORS/98566464.HTML) / DECEMBER 16, 2010

Dan Lohrmann, Chief Technology Officer, Michigan PHOTO COURTESY OF DAN LOHRMANN

Who are you? What information are you allowed to access? Where do you live? What financial assistance are you eligible for? How much do you owe the government? Are you qualified to do that job? Can I verify the information you provided is accurate?

When it comes to online transactions, these questions are difficult for government organizations to answer. And yet, verified credentials are required to enable government efficiency efforts over the next decade. Whether streamlining health records, processing taxes, verifying unemployment benefits, approving student loans, planning transportation needs, accessing criminal justice records, issuing business licenses, reforming correctional facilities or improving dozens of other processes, the use of identity management and provisioning is an essential component to lasting improvements in business processes.

Getting this right won't be easy. Similar opportunities about single sign-ons were discussed in the '90s. Privacy groups also raise legitimate concerns about centralized identity management solutions that must be addressed.

Progress has been slow — with only pockets of success across the nation. State and local governments still face many challenges to implementing federated digital identities that are trusted by the public and private sectors. Some of these challenges include value proposition and benefits, defining the business drivers, building the architecture and standards, enrollment process and issuance, funding and acquisition, and sourcing options.

Meanwhile, the federal government has made steady progress in the past eight years, e.g., the Federal Public Key Infrastructure Policy Authority (2002); First Responder Authentication Credential (2006); Federal Identity, Credentialing and Access Management (2009); Cyberspace Policy Review (2009); and The National Strategy for Trusted Identities in Cyberspace (2010 draft).

What must governments do now? For one, partner with groups like NASCIO on this topic. According to the association's leadership, we can't afford to work alone or on proprietary systems. We must have solutions that interoperate across all governments using a federated approach that's competitively sourced. One answer includes adopting the Federal Identity, Credential and Access Management Roadmap and Implementation Guidance as a framework. Most state technology funds come from the federal government, so states must work closely with federal partners in this area. NASCIO created several working groups on identity and access management with emphasis on identity assurance. Another goal is to streamline federally funded and state-administered programs' business processes to obtain cost reductions. Establishing trustworthy digital identities paves the way for many government efficiency efforts. The level of trust must match the situation. The time to act is now. ¨

Dan Lohrmann is Michigan's CTO and was the state's first chief information security officer. He has 25 years of worldwide security experience, and has won numerous awards for his leadership in the information security field.

Dan Lohrmann (http://www.govtech.com/authors/98566464.html) | Contributing Writer

Daniel J. Lohrmann is an internationally recognized cybersecurity leader, technologist and author. During his distinguished career, Dan has served global organizations in the public and private sectors in a variety of executive leadership capacities, including enterprise-wide Chief Security

Officer (CSO), Chief Technology Officer (CTO) and Chief Information Security Officer (CISO) roles in Michigan.

Dan Lohrmann joined Security Mentor, Inc. (http://www.securitymentor.com) in August 2014, and he currently serves as the CSO and Chief Strategist for this award-winning training company. Lohrmann is leading the development and implementation of Security Mentor's industry-leading cyber training, consulting and workshops for end users, managers and executives in the public and private sectors. Read Dan's full bio (http://www.govtech.com/authors/MT-Author-GT-Dan-Lohrmann.html).