



IMSAC: Overview & Health IT Use Case

Dave Burhop
Deputy Commissioner & Chief
Information Officer
Department of Motor Vehicles
Presentation to HITSAC
May 12, 2016



Identity Management Standards Advisory Council (IMSAC) Overview



IMSAC Background

- Created by the General Assembly during the 2015 Session (Senate Bill 814)
- Consists of seven members, appointed by the Governor for four-year terms
- Membership includes representatives from the Department of Motor Vehicles and the Virginia Information Technologies Agency, as well as five representatives from the private sector with expertise in identity management



Why The IMSAC Was Created

- Pocket markets of e-ID credentials (also referred to as “communities of interest”) continue to grow
- Limited interoperability of effective e-identity frameworks equals limited consumer protection
- Barriers to adoption were identified by the major credential service providers (CSPs) – “why aren’t CSP organizations able to get the e-credential into the hands of the average citizen?”
- Needed to do something to jumpstart e-ID use on a broad scale



The Intent Of The Law

- Making the Internet a safer place to do business
- Enabling e-ID markets for the average citizen
- Limiting liability through a common legal framework that incentivizes CSPs
- Establishes standards and guidelines that support the common legal framework



IMSAC Responsibilities

- Responsibilities codified under § 2.2-437.A and § 2.2-436.A, *Code of Virginia*
- Advises the Secretary of Technology on the adoption of identity management standards and supporting guidance documents
- Recommends to the Secretary guidance documents relating to:
 - Nationally recognized technical and data standards regarding electronic authentication and identity management
 - Minimum specifications and standards that should be included in an identity trust framework (defined in § 59.1-550)
 - Any other related data standards or specifications concerning reliance by third parties on identity credentials



IMSAC Health IT Use Case



Background

- Health Care System Requirement: Trustworthy, compliant and secure solution for electronic authentication (e-authentication) and identity management (IdM) for patient and provider access to electronic health records (EHRs)
- Current State: Application-centric or custom e-authentication and IdM solutions
- Immediate Result: Proliferation of duplicative, non-standardized and inefficient authentication mechanisms
- Long-term Impact: Increased risk, inefficiency and threats to EHR privacy and security



Description

- Use case targets trustworthy, compliant and secure solution for e-authentication and IdM to serve as a gateway for patient and provider access to electronic health records (EHRs)
- Use case envisions a secure, standards-based, privacy-enhancing alternative to the current application-centric or custom solution for electronic authentication
- Use case leverages technical, governance and business-related advances made under the National Strategy for Trusted Identities in Cyberspace (NSTIC), and supporting efforts of the Identity Ecosystem Steering Group (IDESG), but broadens perspective to incorporate other governance models, standards and communities of interest



Stakeholders

- Health Care Systems
 - EHR Operations and Management Staff
 - Information Security Staff
 - Privacy and Compliance Staff
- Health Care Providers (Physicians, Nurses, Therapists and other Providers)
 - Providers – In the Primary Healthcare System
 - Providers – Out of the Primary Healthcare System
- Patients
 - Patients – In the Primary Healthcare System
 - Patients – Out of the Primary Healthcare System



Use Case Scenarios

- Patient
 - Patient enrollment to EHR within the health care system of the primary care physician or principal provider
 - Patient access to EHR in the primary health care system
 - Patient access to EHR in practices or other facilities outside of the primary health care system
- Provider
 - Provider access to EHRs in the primary health care system
 - Provider access to EHRs in practice office in primary health care system
 - Provider access to EHRs in facilities outside of the primary health care system



Next Steps

- Engage subject matter experts in the health care sector and IdM space to build out the use case in greater detail
- Identify and refine use case scenarios around patient and provider access to EHRs
- Document workflows and data flows for the patient and provider scenarios
- Prepare a formal use case document to enable identification of standards for IMSAC consideration
- Present use case to the Health IT Standards Advisory Committee (HITSAC)



Questions