

The New Virginia Digital Identity Law



TIMOTHY S. REINIGER

JUNE 18, 2015

**COMMONWEALTH OF VIRGINIA HEALTH IT STANDARDS
ADVISORY COMMITTEE**

CHESTER, VA

Virginia Digital Identity Bill History



- January 2011 – Bill introduced in General Assembly and referred for study to the Joint Commission on Technology and Science (JCOTS)
- June 2011 through December 2014 – JCOTS forms an Identity Management Subcommittee that studies the bill and actively solicits participation and input from industry and state government stakeholders
 - Active participants included: CertiPath, Verizon, CITI, Symantec, VA Banker Association, Microsoft, Amazon, USAA, DigiCert, American Bar Association, VA DMV, VA CIO, VDH, Governor's Office
- 3 December 2014 – JCOTS votes to endorse the bill for introduction and passage in the 2015 General Assembly.
- January 2015 – SB 814 is introduced in Senate by Sen. John Watkins (chair of the JCOTS Identity Management Subcommittee) and HB 1562 in the House by Delegate John Rust (overall JCOTS chair) as companion bills
- February 26 2015 – both bills, in the same form, are approved by the General Assembly and sent to Governor McAuliffe
- 23 March 2015 – Governor McAuliffe signed the bill into law eff. July 1, 2015
- June 2015 – Proposal to UN by Austria, Belgium, France, Italy, and Poland

Key Discussion Topic in JCOTS

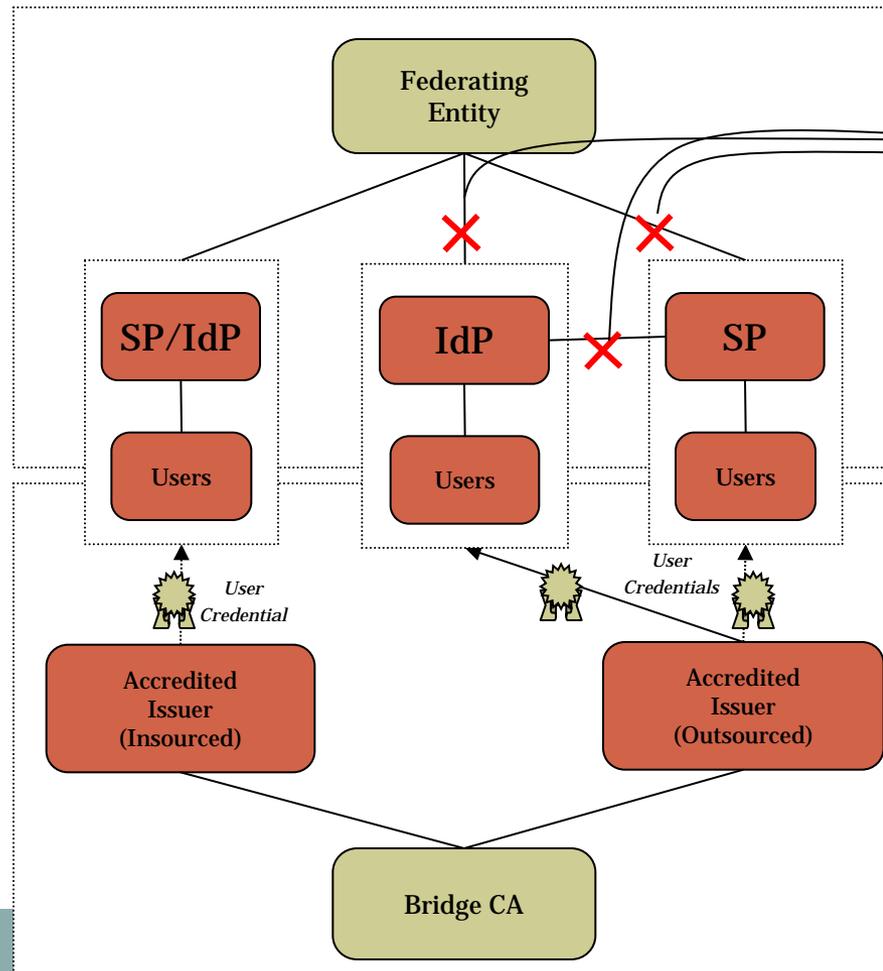


- Overall scope
 - Placement in Code
 - Definitional language
- Role of Commonwealth of Virginia government
 - Designating a lead
 - Minimum standards
- Liability Allocation
 - Limitation of liability for identity credential providers and trust framework providers
 - Trustmark warranty established

Legal Gaps Addressed



Federation and third party bridges don't solve all trust issues...



A contract may not exist between all parties or may not address identity federation issues

Legal Barriers to Federated Identity



- Unpredictable Liability for Identity Providers
- Lack of a Common Legal Framework for Identity System Participants
- Trust Frameworks and Trustmarks Lacking Statutory Authorization

New Digital Identity Law Overview



- Chapter 483: <http://lis.virginia.gov/cgi-bin/legp604.exe?151+ful+CHAP0483>
- Provides Common Legal Framework for Identity System Participants
- Creates the Commonwealth Identity Management Standards Advisory Council
- Provides Limitation of Liability for Identity Providers and Identity Trust Framework Operators
- Creates Additional Relying Party Incentives

Identity Provider Liability Limitation



- Liable for *Issuance* of Credentials not in Compliance with State Minimum Standards, Existing Contracts, or Trust Framework Rules.
- Not Liable for Improper *Use* of Credential by Holder or Any Other Person.

First Key Definition



"Identity Credential" means the data, or the physical object upon which the data may reside, that an identity credential holder may present to verify or authenticate his identity in a digital or online transaction.

Second Key Definition



“Identity Provider” means an entity, or a supplier, employee, or agent thereof, certified by an identity trust framework operator to provide identity credentials that may be used by an identity credential holder to assert his identity, or any related attributes, in a digital or online transaction. For purposes of this chapter, “identity provider” includes an attribute provider, an identity proofer, and any suppliers, employees, or agents thereof.

Third Key Definition



“Identity Trust Framework” means a digital identity system with established identity, security, privacy, technology, and enforcement rules and policies adhered to by certified identity providers that are members of the identity trust framework. Members of the identity trust framework include identity trust framework operators and identity providers.

Fourth Key Definition



“Trustmark” means a machine-readable official seal, authentication feature, certification, license, or logo that may be provided by an identity trust framework operator to certified identity providers within its identity trust framework to signify that the identity provider complies with the written rules and policies of the identity trust framework.

Key Points of the Law



- Intended to help enable a third party digital identity credential/assurance market
- Creates common legal foundation for identity trust frameworks and trustmarks
- Intended to make liability predictable and bounded for identity providers and identity trust framework operators

Virginia Identity Management Standards



- Commonwealth of Virginia establishes minimum specifications and standards that should be included in an identity trust framework so as to warrant liability protection.
- The Secretary of Technology approves upon the recommendation of the Identity Management Standards Advisory Council.
- Based on 1) **nationally recognized** technical and data standards regarding the verification and authentication of identity in digital and online **transactions** and 2) **any other related data standards or specifications concerning reliance by third parties on identity credentials.**

Topics Covered in Virginia Standards



- Identity Assurance Levels and Policies
- Privacy Policies
- Security Policies
- Technology and Data Requirements
- Business Rule
- Legal Rules

Healthcare Considerations for Standards Effort



- Existing HITSAC Standards Relating to Identity
- Patient Consents for Access, Use, and Disclosure (Virginia and Federal Requirements)
- Licensing Regime for Patient Authorization
- User-Managed Access (Kantara Initiative)
- Trustmarks

Opportunities for the Healthcare Industry



- **Cybersecurity**
- **Identity Credential Marketplace**
- **Multi-Factor Authentication Enabled**
- **User-Centric Policies (NSTIC) Supported**

Contact Information



Timothy S. Reiniger, Director
Futurelaw, LLC Digital Services Group
1802 Bayberry Court, Suite 403
Richmond, Virginia 23226
treiniger@futurelaw.net
www.futurelaw.net
804-525-2944