



# Operational Trust Frameworks: Current State Analysis

Joseph W. Grubbs, Ph.D.  
Enterprise Information Architect  
Presentation to the  
Identity Management Standards  
Advisory Council  
March 7, 2016



# Operational Trust Frameworks: Principles, Components and Current-State Examples



# Trust Framework 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.*

*§ 59.1-550, Code of Virginia*

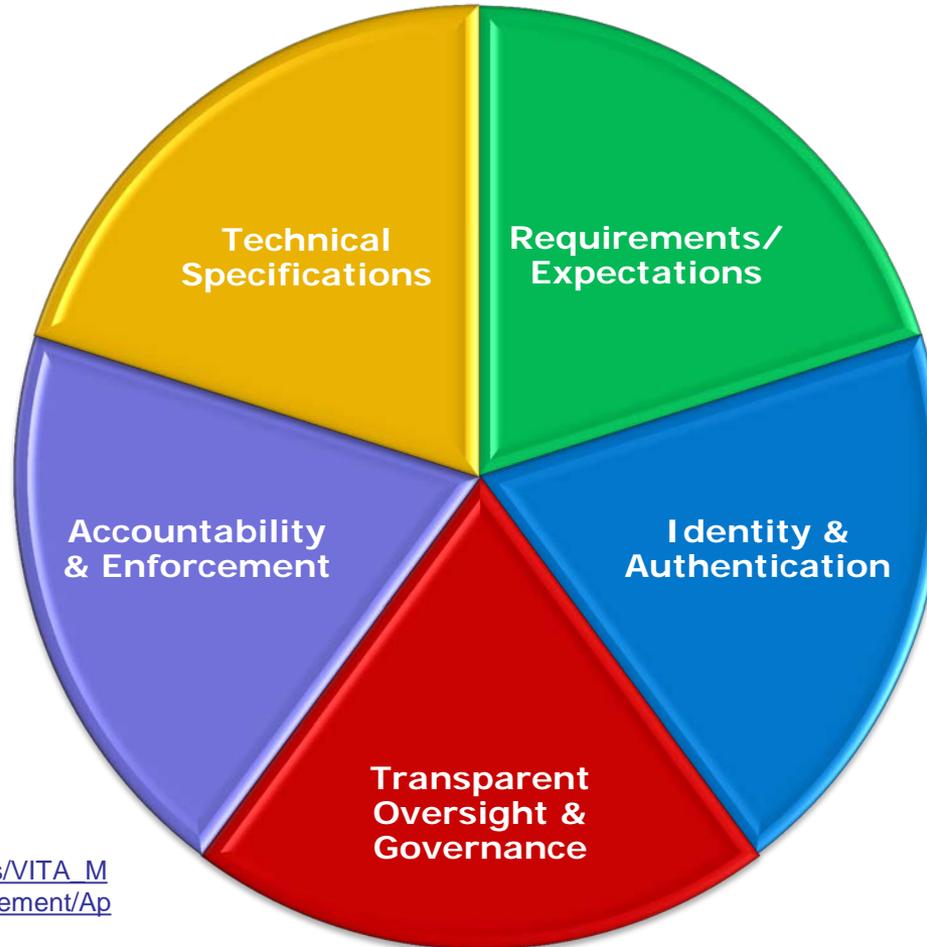


# Trust Frameworks

- Multi-party agreements among participants in an identity management community
- Scalable alternatives to point-to-point agreements
- Certification programs to implement common business, legal and technical requirements
- Founded on and compliant with applicable law
- Living documents that evolve based on the trust framework's governance model



## Trust Framework Elements



Source: Gravely, Steven D. 2011.  
[http://www.vita.virginia.gov/uploadedFiles/VITA\\_Main\\_Public/EAD/Enterprise\\_Data\\_Management/AppendixC\\_DURSA\\_overview.pdf](http://www.vita.virginia.gov/uploadedFiles/VITA_Main_Public/EAD/Enterprise_Data_Management/AppendixC_DURSA_overview.pdf)



# Current Trust Framework Models

- General Services Administration (GSA): Identity, Credential and Access Management (ICAM)
- Open Identity Exchange (OIX): Open Identity Trust Framework Model (OITF)
- SAFE BioPharma Association: U.S. Government Approved Trust Framework Provider
- InCommon: Trust Framework Provider and Assurance Assessment Framework for Higher Education
- Kantara Initiative: Certification authority for trust frameworks; Identity Assurance Program



# Building Blocks of Trust Frameworks

- Clear business drivers (executive/ legislative mandate) and value proposition
- Articulated requirements and expectations under the agreement
- Enforceable compliance and accountability (applicable law, consent, authorization)



# Cross Sector Digital Identity Initiative (CSDII)

## National Strategy for Trusted Identities in Cyberspace (NSTIC)

### Trust Framework Gap Analysis



# Trust Framework Gap Analysis

- Assess model trust frameworks (TFs) on business, legal, technical dimensions using analytic device
- Evaluate how selected model TFs aligned with TF requirements for the NSTIC Pilot
- Identify components, processes and sample agreements from model TFs that may be “reused” for the NSTIC Pilot TF



# Model Trust Frameworks

- AAMVA DL/ID Security Framework
- eHealthExchange DURSA
- InCommon
- Kantara Initiative
- Open Identity Exchange (OIX)/OITF
- CIVICS/IDCubed.org



# Analytic Approach

- Built from existing research and subject matter expertise to develop analytic device covering business, legal and technical components
- Framed analysis on components, processes and agreements in model trust frameworks that could be adopted for the CSDII Pilot
- Assumed that the CSDII trust framework would need to be scalable (horizontally & vertically) and support post-pilot implementation



# Analytic Device

	Trust   Security Frameworks – Key Elements & Provisions for CSDII Pilot Project			
	Business	Legal	Technical	Other
Trust   Security Framework Comparison	<ul style="list-style-type: none"> <li>• Definitions for “Permitted Purpose”</li> <li>• Governing Body &amp; Change Processes</li> <li>• Operating Policies &amp; Procedures</li> <li>• Security, Privacy &amp; Confidentiality-Business: Consent/Auth.)</li> <li>• Suspension &amp; Termination (Voluntary &amp; Involuntary)</li> <li>• Data Elements &amp; Data Classification (Attribute Level/PII)</li> <li>• Expectations of Performance</li> <li>• Use Cases (Exchange &amp; Participant Types)</li> </ul>	<ul style="list-style-type: none"> <li>• Definition/Identification of “Applicable Law”</li> <li>• Legal Agreements (Set) for Exchange Structure (IdPs/RPs/ITSPs)</li> <li>• Security, Privacy &amp; Consent Provisions</li> <li>• Assignment of Liability &amp; Risk for Participants</li> <li>• Representations &amp; Warranties</li> <li>• Grant of Authority</li> <li>• Dispute Resolution</li> <li>• Authorizations for Data Requests by Participant</li> <li>• Open Disclosure &amp; Anti-Circumvention</li> <li>• Confidential Participant Information</li> <li>• Audit, Accountability &amp; Compliance</li> </ul>	<ul style="list-style-type: none"> <li>• Performance &amp; Service Specifications</li> <li>• Security, Privacy &amp; Confidentiality (Technical: Infrastructure/ Architecture )</li> <li>• Breach Notification</li> <li>• System Access (ID/Authentication)</li> <li>• Provisions for Future Use of Data</li> <li>• Duty of Response by Participants (IdPs/RPs/ITSPs)</li> <li>• Onboarding, Testing &amp; Certification Requirements</li> <li>• Handling of Test Data v. Production Data</li> <li>• Compliance with External/SDO Standards</li> </ul>	<ul style="list-style-type: none"> <li>• Openness &amp; Transparency</li> <li>• TF Lifecycle Management (“Living Agreement”)</li> <li>• Support &amp; Capacity Building (IGs)</li> <li>• Scalability to Support Array of Participants (Horizontal/Vertical)</li> <li>• Glossary of TF Terms/Definitions</li> <li>• Modular Approach for TF Elements – IdPs, RPs &amp; ITSPs</li> <li>• Law Enforcement (LE) Use Case: Support for Data Sharing</li> <li>• Federal Government Use Case: Federal Agency as RP (FICAM)</li> </ul>



## Summary of Findings

- Model trust frameworks ranged along a continuum from the Descriptive to Prescriptive
- Issues of specificity and applicability at the Descriptive end of the continuum
- Concerns over scalability and legal constraints at the Prescriptive end of the continuum



# CSDII Trust Framework Development

- Built from the gap analysis to develop a detailed outline (core components, processes and agreements) for CSDII trust framework
- Engaged InCommon to learn from its trust framework experience, components and processes
- Focused development efforts to design a trust framework for CSDII that reflected best practices and met all requirements



# IMSAC Current State Analysis

- Extend the analytic device used for the CSDII trust framework Gap Analysis to focus on IMSAC requirements
- Apply the extended analytic device to map alignment/gaps in operational trust frameworks to IMSAC requirements
- Prepare a summary white paper on findings, requirements and recommendations from the current-state analysis to inform IMSAC



# Discussion

Joseph W. Grubbs, Ph.D., AICP, GISP

Enterprise Information Architect

Virginia Information Technologies Agency

Phone: (804) 467-7729

Email: [Joseph.Grubbs@vita.virginia.gov](mailto:Joseph.Grubbs@vita.virginia.gov)