AAMVA

American Association of
Motor Vehicle Administrators

Electronic Identity

The Who, What, Why, and How eID Will Impact the AAMVA Community

September 2013

eID WORKING GROUP

Cover photo credits: iStockPhoto/Thinkstock.com

Contents

Executive Summary

Increasing numbers of people are using the Internet to perform tasks that once could only be done in person. The rise of this reality has given way to a new frontier—dealing with electronic identities (eID). A chief focus of the eID Working Group is to identify solutions and standards that yield a high level of identity assurance for online transactions. The actual driver license/identification card (DL/ID) is the identification credential of choice throughout North America, with growing popularity elsewhere. Online, the information used in connection with the DL/ID can become an eID. A subtle difference between a physical DL/ID and eID is that the information connected to a claimed identity (the vetting/proofing of a claim of identity) can serve the purpose of an eID. The White House initiative, National Strategy for Trusted Identities in Cyberspace (NSTIC), is working collaboratively with the private sector, consumer/privacy advocates, public sector agencies, and other organizations to improve the privacy, security, and convenience of sensitive online transactions.

In this new era we will operate within an "Identity Ecosystem" that will protect the privacy of individuals by reducing the need for individuals to share personally identifiable information (PII) in order to identify themselves at multiple web sites and by establishing consistent policies about how organizations use and manage PII in the ecosystem. NSTIC provided grant opportunities in which AAMVA was selected to demonstrate four capabilities: 1) to verify attributes, 2) to enable identity providers to use verified attributes to issue a "leveled-up" credential, 3) to authenticate credential, and 4) to enable relying parties to use verified attributes to make authorization decisions. According to the 2010 United States Census, it places the number of Internet-connected Americans at an estimated 245 million[1]. A broad study conducted in 2007 by Microsoft with 540,000 participants suggests that online users maintain approximately 25 online accounts[2]. The complexity of how vulnerable people are with the sheer volume of information that exists in the "ID cosmos" is staggering.

The Identity, Credential, and Access Management (ICAM) subcommittee was established by the Federal CIO Council's Information Security and Identity Management Committee, and tasked with aligning the Identity Management activities of the U.S. Government. Ultimately, two significant implementations have arisen from this—a federal roadmap and then by adoption a state roadmap. The Federal Identity, Credential, and Access Management (FICAM)[3] and the State Identity, Credential, and Access Management (SICAM)[4] provide states and provinces a set of solutions for increasing security, enhancing compliance capabilities, improving interoperability, eliminating redundancy, and, most important, enhancing the protection of PII contained within information

1 https://www.cia.gov/library/publications/the-world-factbook/geos/us.html
2 http://research.microsoft.com/pubs/74164/www2007.pdf
3 http://www.idmanagement.gov/documents/ficam-roadmap-and-implementation-guidance
4 http://www.nascio.org/publications/documents/SICAM.pdf

systems. SICAM, and to a lesser degree FICAM, provide public and private entities with the tools to guide them through to developing a secure identity infrastructure.

Ultimately, in order for the ecosystem to deliver on its objective there must be a framework that enables trust in the electronic identities individuals and entities use and rely upon. The development of such a framework will not only benefit the AAMVA community but will serve to benefit similar communities of interest. In the end, all participants in a standardized, properly implemented Identity Ecosystem will realize tangible benefits from greater security, privacy, and trust in online transactions.

Introduction and Background

With the advancement of technology, more and more people are using the Internet to perform tasks that historically were required to be done in person. In light of these realities, AAMVA created a working group to monitor this progression and guide its membership in addressing the issues surrounding these changes.

Government agencies at all levels, not just those involved in motor vehicle administration, face challenges regarding their dependence on identification. This dependence relates to the issuance of credentials and the privileges that the credential makes available to the individual[5]. As has been referenced in similar efforts, one privilege that the credential affords citizens is electronic access to federally funded programs (such as health and wellness, for example—Medicaid). However, issuance remains program-specific and has redundancy issues for many of the impacted agencies. In issuing an electronic (digital) identity, built with multi-platform options, the aim is to yield outcomes that result in a more efficient and convenient system for all stakeholders, including issuing authorities, identity providers, and relying parties. An additional goal is to allow for commercial entities to participate in order to expand benefits of an architecture that can provide secure online transactions. These transactions should not only be between citizens and government, but also between citizens and business, as well as government and business.

Initially AAMVA's working group was mandated to explore, study, and test the identity verification and proofing functions of the Motor Vehicle Administrations (MVAs). The scope of the Association's focus will first be the vetting process that needs defining and the technical recommendations on what an electronic identity credential should conform to. AAMVA recognizes that partner organizations like the National Association of State Chief Information Officers (NASCIO) and those in the Federal government are pursuing electronic identification at a higher level with an emphasis on the role as a relying party. To that end, the Association plans to support and participate in their activities like the SICAM subcommittee.

In addition to the constant evolution of technology, mounting budget pressures in many jurisdictions continue to motivate the desire to migrate transactions out of the office to the Internet. The move to online services offers a key opportunity for cost reduction and improved citizen experience. The current situation is such that citizens need to create and maintain many different identities for access to services. Since the assurance level of these electronic identities is low, there is a lack of confidence in performing high-value transactions such as title transfers online. Another focus of the working group is to define, describe, and deploy (and/or enable deployment of) solutions and standards that yield a high level of identity assurance for online transactions in intra- and inter-state/province scenarios.

Electronic Identity Defined

The driver license/identification card (DL/ID) is now the identification credential of choice throughout North America, with growing popularity as a means of identification in many other countries. With a photo, signature, and physical description, the DL/ID

5 AAMVA DL/ID Security Framework – February 2004

assumes a role beyond its original purpose. The credential is now readily accepted as an official identification document for both licensed drivers and non-drivers (issued by same authority that issues the driver license). The MVAs who issue these documents have unique, continuous and long-lasting contact with most of their constituents from the individual's pre-teenage years onward. It's this contact that over time has made the DL/ID issuers the most experienced in assuring that people are who they say they are.

Online, the information (some to all) used in connection with the DL/ID can become an eID. A subtle difference between a physical DL/ID and eID is that the information, also referred to as attributes, connected to a claimed identity can serve the purpose of an eID.

National Strategy for Trusted Identities in Cyberspace

As stated on the U.S. NSTIC[6] web site, it is a White House initiative to work collaboratively with the private sector, advocacy groups, public sector agencies, and other organizations to improve the privacy, security, and convenience of sensitive online transactions. The Strategy calls for the development of interoperable technology standards and policies — an identity ecosystem — where individuals, organizations, and underlying infrastructure — such as routers and servers — can be authoritatively authenticated. The goals of the strategy are to protect individuals, businesses, and public agencies from the high costs of cyber crimes like identity theft and fraud, while simultaneously helping to ensure that the Internet continues to support innovation and a thriving marketplace of products and ideas.

The strategy was developed with substantial input from the private sector and the public. It calls for the effort to be led by the private sector, in partnership with the federal government, consumer/privacy advocacy organizations, privacy experts, state and local agencies, and others. Establishment of an Identity Ecosystem would allow individuals to validate their identities securely when conducting sensitive transactions (such as banking or viewing health records) and let them remain anonymous when they're not (for instance, while blogging or surfing the Web). The Identity Ecosystem would protect the privacy of individuals by reducing the need for individuals to share PII in order to identify themselves at multiple web sites and by establishing consistent policies about how organizations use and manage PII in the Identity Ecosystem.

The Identity Ecosystem would protect the privacy of individuals by reducing the need for individuals to share PII in order to identify themselves at multiple web sites and by establishing consistent policies about how organizations use and manage PII in the Identity Ecosystem.

Cross-Sector Digital Identity Initiative

NSTIC provided grant opportunities in which AAMVA was selected as one of five grantees (out of 180 applicants). AAMVA is leading a consortium of private industry and government partners to

6 http://www.nist.gov/nstic/

implement and pilot the Cross-Sector Digital Identity Initiative (CSDII). The goal of this initiative is to produce a secure online solution within the Identity Ecosystem that will lead to safer transactions by enhancing privacy and reducing the risk of fraud in online commerce. In addition to AAMVA, the CSDII pilot participants include the Commonwealth of Virginia Department of Motor Vehicles, Biometric Signature ID, CA Technologies, Microsoft, and AT&T. The CSDII demonstrates four capabilities: 1) to verify attributes, 2) to enable identity providers to use verified attributes to issue a "leveled-up" credential, 3) to authenticate credential, and 4) to enable relying parties to use verified attributes to make authorization decisions.

The goal of this initiative is to produce a secure online solution within the Identity Ecosystem that will lead to safer transactions by enhancing privacy and reducing the risk of fraud in online commerce.

Identity Credential and Access Management (Federal and State)

The ICAM subcommittee was established by the Federal CIO Council's Information Security and Identity Management Committee and tasked with aligning the Identity Management activities of the U.S. Government.

ICAM mission includes:

- Aligning federal agencies around common practices by fostering effective government-wide identity, credential, and access management;
- Collaborating with federal government and external identity management activities (non-federal, commercial, and more) to leverage best practices and enhance interoperability; and
- Enabling trust and interoperability in online transactions, through the application of common policies and approaches, in activities that cross-organizational boundaries.

Federal Implementation

Thanks to the work conducted by ICAM, a federal road map came into being, FICAM[7]. Its aim is to provide agencies with architecture and implementation guidance that addresses existing ICAM concerns and issues faced daily. In addition to helping agencies meet current gaps, FICAM provides significant benefits around security, cost, and interoperability which will have positive impacts beyond an individual agency in improving the delivery of services by the federal government. It also seeks to support the enablement of systems, policies, and processes to facilitate business between the government and its business partners and constituents.

The benefits associated with the implementation of ICAM converge in increased security, which correlates directly to reduction in identity theft, data breaches, and trust violations. Specifically, ICAM closes security gaps in the areas of user identification and authentication, encryption of sensitive data, and logging and auditing. ICAM also addresses compliance with laws, regulations, and standards as well as resolution of issues highlighted in Government Accountability Office (GAO) reports of agency progress; improved interoperability, specifically between agencies using their personal identity verification (PIV) credentials along with other partners carrying PIV-interoperable or third party credentials that meet the requirements of the federal trust framework. Additional benefits include minimizing the number of credentials requiring lifecycle management; enhanced customer service, both within agencies and with their business partners and constituents; facilitating secure, streamlined, and user-friendly transactions—including information

7 Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance Version 2.0, December 2, 2011.

sharing–which translates directly into improved customer service scores, lower help desk costs, and increased consumer confidence in agency services; elimination of redundancy, both through agency consolidation of processes and workflow, and the provision of government-wide services to support ICAM processes. This results in extensibility of the information technology (IT) enterprise and reduction in the overall cost of security infrastructure; increase in protection of PII by consolidating and securing identity data, which is accomplished by locating identity data, improving access controls, proliferating use of encryption, and automating provisioning processes. These benefits combine to support an improvement in the cyber security posture across the federal government, with standardized controls around identity and access management.

The ICAM target state closes security gaps in the areas of user identification and authentication, encryption of sensitive data, and logging and auditing. It supports the integration of physical access control with enterprise identity and access systems and enables information sharing across systems and agencies with common access controls and policies. Leveraging the digital infrastructure in a secure manner will enable the transformation of business processes, which is vital to the future economic growth of the United States. This document presents the Federal Government with a common framework and implementation guidance needed to plan and execute ICAM programs. While progress has been made in recent years, this document is a call to action for ICAM policy makers and program implementers across the Federal Government to take ownership of their role in the overall success of the federal cyber security, physical security, and electronic government (E-Government) visions, as supported by ICAM.

State Implementation

The SICAM[8] Guidance and Roadmap outlines a strategic vision for state-based identity, credential, and access management efforts, and emphasizes the importance of implementing the SICAM architecture and services in support of the challenges associated with trust, interoperability, security, and process improvement. States must provide a secure, auditable environment for the processing and exchange of information across the entire spectrum of state business. SICAM consists of the programs, processes, technologies, and personnel used to create trusted digital identity representations of individuals and/or non-person entities. This guidance promotes a federated approach where the identification of the information requester and supplier are guaranteed. This is of vital importance in an environment where phishing, scamming, and identity theft are rampant. It is essential that state governments take the initiative to ensure the integrity of the data entrusted to them and provide a high level of security and privacy to citizens, customers, and partners. The SICAM architecture enables states and their partners to share and audit identification, authentication, and authorization across state enterprise boundaries. This architecture will significantly reduce administrative and technological overhead caused by incompatible and un-auditable identity management systems (silos), lead to improved business processes and efficiencies, and reduce cyber security risk.

Multiple initiatives are underway to address these challenges—PIV cards are being issued in increasing numbers, the public key infrastructure (PKI) has connected government and commercial PKIs via a trust framework, working groups are tackling relevant process, technology, and operational questions for mission-specific functions, and many others are leveraging digital identities to enable trusted government to citizen, government to business, and government to government transactions. The primary

8 State Identity Credential and Access Management (SICAM)—Guidance and Roadmap Version 1.0, September 2012.

audience for the document is the state Chief Information Officer, state Chief Information Security Officer, state Enterprise Architect, and other SICAM implementers at all stages of program planning, design, and implementation; however, the document may also be used as a resource for systems integrators, end users, other entities, and commercial business partners seeking interoperability or compatibility through state programs. While this document serves to outline a common framework for SICAM in the state government, it is understood that agencies are at different stages in the implementation of their SICAM architectures and programs. As a result, they will need to approach alignment with SICAM from varying perspectives. The SICAM Guidance and Roadmap will also serve as an important tool for providing awareness to external mission partners and drive the development and implementation of interoperable solutions.

The Issue of Electronic Identities

The World Fact Book, with corroborating information from the 2010 United States Census, places the number of Internet-connected Americans at an estimated 245 million[9]. A broad study conducted in 2007 by Microsoft with 540,000 participants suggests that online users maintain approximately 25 online accounts[10]. By simple calculation, this equates to roughly six billion distinct accounts. To further complicate, each Internet site offering one of these six billion accounts has its own criteria for maintaining a user account; one might enforce a minimum password criteria of six characters comprised of letters, numbers, and special characters which is changed every 60 days, and another may enforce a password minimum of four characters comprised of numbers only. The onus then is on the user to maintain account information according to the varying levels of characteristics. This invariably leads to a minimalist mentality for the end user, using easily remembered and frequently re-used passwords, making the interaction ripe for fraud. The account username and password pair, a simple online credential, is the most untrusted form of credentialing available for online transactions, short of anonymous transactions.

The compromised username and password pair represents a small portion of the online theft and fraud that consumers experience in online transactions. The overarching problem, however, is so prevalent that the Federal Bureau of Investigation and the National Center for White Collar Crimes established the Internet Crime Complaint Center[11], a clearinghouse organization for online theft and fraud activities. While the areas identified include issues such as the Nigerian money laundering scheme and the Scottish lottery scheme, many of these nefarious activities are based on the online information maintained by consumers on the Internet. How can we secure that piece of the puzzle, ensuring that consumer information is secured and trustworthy across the Internet landscape?

One answer is trust. Trust, when considering online credentials, carries many connotations—trust in the credential's integrity, trust in the individual using the credential, trust in the methods used to define and vet the credential, and trust that the level of vetting completed is sufficient to meet your business requirements. Trust is the basis for ensuring that online transactions are accurate, valid, and secure. Trust, in today's online world, is based almost entirely on the online credential based on the username and password pair. Oftentimes, especially in merchant situations, this trust is backed by the consumer's credit card, hardly a secure control. Simple online credentials provide access to an online resource for an individual but are not adequate for security and are not constructed for cross-organization utilization (federation).

Fortunately, for consumers, and public and private organizations, the online credentials that are commonplace on the Internet today represent a starting point in securing online transactions. That starting point represents the baseline from which public and private entities can start developing an integrated approach to Identity, Credential, and Access Management. The FICAM[12] and the SICAM[13]

9 https://www.cia.gov/library/publications/the-world-factbook/geos/us.html
10 http://research.microsoft.com/pubs/74164/www2007.pdf
11 http://www.ic3.gov/default.aspx
12 http://www.idmanagement.gov/documents/ficam-roadmap-and-implementation-guidance
13 http://www.nascio.org/publications/documents/SICAM.pdf

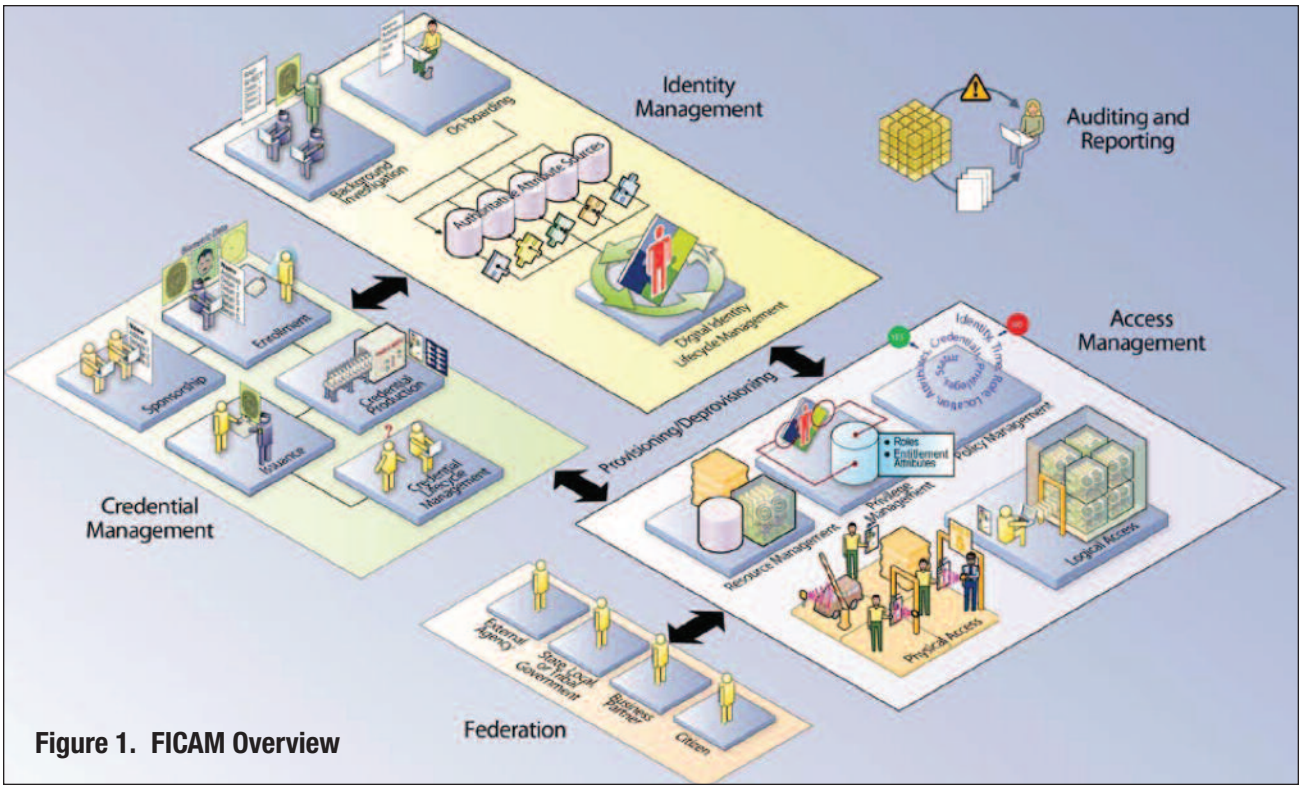

Figure 1. FICAM Overview

roadmaps provide a set of solutions for increasing security, enhancing compliance capabilities, improving interoperability, eliminating redundancy, and most importantly enhancing the protection of PII contained within information systems.

At the high level, Figure 1 displays the interactions associated with electronic identities as a FICAM overview. The figure illustrates the identity life-cycle and underscores some of the potential application of electronic identity across jurisdictional and corporate borders.

Roles in Electronic Identity (Government and Commercial)

SICAM, and to a lesser degree FICAM, provide public and private entities with the tools to guide them through to developing a secure identity infrastructure. Building trust frameworks across the public and private sector provides many potential benefits.

- Entities can leverage identity establishment and vetting processes based on agreed upon standards for identity providers, ensuring that credentials match their business requirements.
- Entities have the ability to provide products such as hardware tokens and smartcards to enable deeper assurance levels for consumers.
- Entities share in the governance process necessary for operating a successful Identity Ecosystem based on standards.
- All parties benefit from consumer information not being propagated throughout the Identity Ecosystem, instead relying on token passing and attribute validation.
- Entities benefit from increased security as public and private entities can work to actively establish the governing principles for a successful Identity Ecosystem.

The true benefit of a federated secure identity infrastructure is the ability to leverage the identity systems across an entire domain, to the benefit of partner organizations. It also means that public and private entities have the ability to provide ancillary services to further vet credentials to match agreed upon assurance levels. Naturally, this extends to new business opportunities.

Besides the benefits to the business and government communities, consider the following scenarios that may underscore the point. For example, a company that sells online products and provides online support communities implements a full-scale identity management system. The company has the responsibility to manage all of the customer information related to the customer identity credential. This may include personally identifiable and financial information. In this case, the company holds singular responsibility for user data, authorization, and authentication, ultimately being responsible for managing the identity of the user for enabling a secure purchase transaction.

If, however, the company participated in an Identity Ecosystem where they were a relying-party, the company could enjoy the benefits associated with the full-scale identity management system, with few of the pitfalls. In an Identity Ecosystem, the company may not need to maintain repositories of personally identifiable or financial information on customers, and may be able to focus instead on validating attributes of the customer identity credential with identity service providers. This scenario provides the merchant with the ability to scale back on their identity management system and focus on their core mission, sales. An example of this type of identity case is found in the OpenID standard in use by online payment companies to streamline online purchases.

In addition to the online merchant scenario, the interaction between citizens and varying levels of government cannot be overlooked. This scenario describes the interactions between a user of government services (citizen beneficiary) and a government organization, from the citizen perspective. The citizen has a clear need to interact with government to obtain services such as registering a vehicle or requesting benefits. The citizen establishes an electronic identity with one of the identity providers within the Identity Ecosystem. The citizen performs the actions required by the Identity Ecosystem to establish an electronic identity at a certain level of assurance (as approved by the operating or "trust" rules of the federation). The citizen may elect to utilize a private sector entity such as Microsoft Account™ to establish an electronic identity. Once the citizen has completed the vetting process as required, the credential can be utilized across the federated entities.

The citizen, using a vetted credential, logs into a government portal offering the services required. The portal directs the transaction based on the assurance level required and requests additional information from the citizen as needed to grant the necessary authorization for the transaction. The citizen opts-in as necessary and successfully completes the transaction at the first department. As indicated earlier, the citizen also needs to complete a second transaction, such as a vehicle registration and logs in to the appropriate government web site using an established credential (notice no additional credential is necessary as the information on the citizen is federated across the Identity Ecosystem). At this point, the second system requests information as necessary to provide appropriate authorization and the transaction is completed. The citizen has the benefit of interacting with public and private sector entities using a single credential, only providing additional information as necessary to authorize the user to complete transactions. An example of this type of credential would be university and college systems utilizing InCommon to federate identities across the education community. The benefits of this use case:

- Citizen views government (services and benefits) through a single point of entry, providing additional information as necessary to increased authorizations.
- Citizen data is more secure, as less information is stored in centralized repositories and transmitted less often.
- Citizen can further secure credential and PII by increasing the assurance level of a credential by adding multi-factor authentication[14] mechanisms to the credential.
- Citizen saves time, effort, and reduces opportunity for error through less duplication in entering information multiple times across web sites to obtain government services and benefits.

The scenarios presented here have a common thread in that they are based on standards adopted by an Identity Ecosystem. The standards allow the Identity Ecosystem participants to play multiple roles in enabling a secure federated trust model. These standards allow for advanced security measures to the benefit of users of the system and minimize the propagation of public and private information to that necessary to complete a transaction. The trust framework that specifies the standards is critical to the success of the Identity Ecosystem.

These scenarios represent the potential to streamline identity management from the consumer and business perspective, offer enhanced security including advanced multi-factor authentication, and have the capability to cross online domains. The Identity Ecosystem based on trust also brings in new opportunities for public and private sector entities to grow business value while enhancing the services provided to their respective customer communities.

Roles in electronic identity have been defined in many trust frameworks and carry monikers such as "identity provider," "relying party," and "assuring party," among others. They are all based on standards that have been developed through the concerted efforts of many dedicated individuals the world over. The federations that are based on these standards likewise have implementations that speak to the validity, security, and benefit of the new online identity model.

14 Multi-factor authentication is an approach which requires the presentation of two or more of the three authentication factors: "has", "knows", and "is".

Building Trust and Longevity in Electronic Identities

In order for the ecosystem to deliver on its objective there must be a framework that enables trust in the electronic identities people use and rely on. The framework is a compilation of enforceable rules, defined governance, and standards. For the AAMVA community in the wake of 9/11 a framework was developed around the challenge of issuing DL/IDs. What was developed then is similar to what is needed now—rules for how an identity is vetted/proofed; methods for ensuring those within the community are all operating by the same set of rules; a system for dealing with those that are not. These basic principals are at the heart of what is referred to as a "trust framework (TF)" in the NSTIC space. Not wanting to reinvent the wheel the CSDII team has performed a comparative analysis of those most prevalent frameworks in existence in order to make a recommendation on a way forward. Having completed this, a decision was made to endorse the use of the InCommon TF (for the CSDII pilot).

Model TFs reviewed in the analysis:

- AAMVA DL/ID security framework—Set of requirements, recommendations, and standards maintained by AAMVA for use by Motor Vehicle Administrations to ensure drivers license and identification security.
- eHealth Exchange Data Use & Reciprocal Support Agreement (DURSA)—Trust framework established to support the exchange of health information and messaging within the Nationwide Health Information Network (NwHIN, now eHealth Exchange).
- InCommon Trust Framework—Trust framework designed to facilitate authentication and identity management for students, faculty, staff, and other service providers for institutions of higher education.

In order for the ecosystem to deliver on its objective there must be a framework that enables trust in the electronic identities people use and rely on.

- Kantara Initiative Trust Framework—Trust framework developed on a for-profit, subscription basis to enable secure, identity-based, online interactions in a secure environment.
- Open Identity Exchange (OIX)/OITF Model—Set of guidelines and recommended mechanisms (Level of Assurance and Level of Protection) for developing and implementing a trust framework for secure, confidence-based exchange of information.
- CIVICS/IDCubed.org Trust Framework—Model designed by Civics (in partnership with the MIT Media Lab) and IDCubed.org, a private non-profit organization, which outlines the business, legal, and technical elements of a trust framework.

Key Findings

The model TFs ranged on a continuum from "descriptive," those setting minimum standards for trust-based information exchanges without actually structuring an exchange, to "prescriptive," those establishing specific agreements, policies, procedures, and specifications to support an information exchange.

Substantive gaps in alignment with the Project TF requirements were observed along this continuum.

Primary gaps in alignment included the following:

- The more descriptive TFs lacked the level of specificity required for the Project TF; these descriptive TFs may be used as high-level checklists for the Project TF but failed to provide the necessary business, legal, and technical (BLT) provisions for the Project exchange; the Project TF will need to cover the full range of BLT requirements.
- The prescriptive TFs tended to be either excessively domain-centric or failed to take account of the unique legal status of government agencies, particularly state government; issues of sovereignty, statutory authority, liability, and grant of authority will need to be fully addressed in the Project TF.

Conclusion

The InCommon TF Model was found to be the most robust, mature, and scalable of those reviewed for the Project. Primary strengths of the InCommon TF:

- Addressed the cited concerns relating to legal issues for state government agencies, including sovereignty, statutory authority, liability, and grant of authority.
- Provided detailed guidance, agreements, and support documentation for structuring an exchange in the ID assurance and management space.
- Established binding BLT requirements for all relevant participant types, including identity providers (IDPs), relying parties (RPs), and assurance providers.
- Featured extensive use-cases demonstrating the types of participants, types of exchanges, operational/functional elements, and other dimensions of the exchange.
- AAMVA would seek to imitate InCommon and its architecture to use as a baseline/model for our members and the larger state/provincial government community of interest.

Final Thoughts

Much of this document has been dedicated to defining electronic identities, defining the value in reigning in the propagation of electronic identities, and the potential we have in building a secure Identity Ecosystem to the benefit of our respective constituents. In no uncertain terms, building better electronic identities based on a trust framework in a trusted Identity Ecosystem will benefit citizens, government, and businesses.

All participants in a standardized, properly implemented Identity Ecosystem realize tangible benefits from greater security, privacy, and trust in online transactions. Entities building identity systems realize cost avoidance benefits by not building unnecessarily redundant systems while users realize reduced occurrence of theft and fraud due to data loss and realize increased overall security through the implementation of multi-factor authentication methods.

Online service delivery is becoming the norm for public services. Examples include the purchase of products, payment of government fees and taxes, banking, and social media interaction. Each of these services requires some sort of credential to be established by the user and is a username/password pair in most cases. Account credentials require the use of PII for creation. Since the required information varies among providers, the user eventually has a majority of their PII housed in multiple databases increasing the risk of misuse of personal information that could lead to fraud and stolen identities.

The eID will reduce these risks and protect user privacy by requiring the users to provide minimal personal information to create one account that can be used for any online transaction. This cross platform approach will lead to application development efficiencies, a more efficient service delivery model, and a seamless user experience and benefit to all participants.

Glossary of Acronyms

AP	attribute provider
BLT	business, legal, and technical
CIO	chief information officer
CSDII	Cross-Sector Digital Identity Initiative
DL/ID	driver license/identification card
DURSA	Data Use & Reciprocal Support Agreement (DURSA)
eID	electronic identity
FICAM	Federal Identity, Credential, and Access Management
GAO	Government Accountability Office
ICAM	Identity Credential & Access Management
IDP	identity provider/proofer
IT	information technology
MVA	Motor Vehicle Administration
NASCIO	National Association of State Chief Information Officers
NSTIC	National Strategy for Trusted Identities in Cyberspace
OIX	Open Identity Exchange
PII	personally identifiable information
PKI	public key infrastructure
PIV	personal identification verification
RP	relying party
SICAM	state identity, credential, and access management
TF	trust framework

Bibliography

AAMVA DL/ID Security Framework—February 2004, http://www.aamva.org/Identification-Security/ (Background Information Tab)

Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance Version 2.0, December 2, 2011, http://www.idmanagement.gov/documents/ficam-roadmap-and-implementation-guidance

State Identity Credential and Access Management (SICAM) – Guidance and Roadmap Version 1.0, September 2012, http://www.nascio.org/publications/documents/SICAM.pdf

http://www.nist.gov/nstic/

https://www.cia.gov/library/publications/the-world-factbook/geos/us.html

http://research.microsoft.com/pubs/74164/www2007.pdf

http://www.ic3.gov/default.aspx

http://www.idmanagement.gov/documents/ficam-roadmap-and-implementation-guidance

http://www.census.gov/compendia/statab/2012/tables/12s1055.pdf

http://www.incommon.org/

Appendix

CSDII Pilot Project Trust Framework (TF) Gap Analysis

	Trust I Security Frameworks – Key Elements & Provisions for CSDII Pilot Project			
	Business	**Legal**	**Technical**	**Other**
Trust I Security Framework Comparison	• Definitions for "Permitted Purpose" • Governing Body & Change Processes • Operating Policies & Procedures • Security, Privacy & Confidentiality (Business: Consent/Auth.) • Suspension & Termination (Voluntary & Involuntary) • Data Elements & Data Classification (Attribute Level/PII) • Expectations of Performance • Use Cases (Exchange & Participant Types)	• Definition/ Identification of "Applicable Law" • Legal Agreements (Set) for Exchange Structure (IdPs/RPs/ITSPs) • Security, Privacy & Consent Provisions • Assignment of Liability & Risk for Participants • Representations & Warranties • Grant of Authority • Dispute Resolution • Authorizations for Data Requests by Participant • Open Disclosure & Anti-Circumvention • Confidential Participant Information • Audit, Accountability & Compliance	• Performance & Service Specifications • Security, Privacy & Confidentiality (Technical: Infrastructure/ Architecture) • Breach Notification • System Access (ID/Authentication) • Provisions for Future Use of Data • Duty of Response by Participants (IdPs/RPs/ITSPs) • Onboarding, Testing & Certification Requirements • Handling of Test Data v. Production Data • Compliance with External/SDO Standards	• Openness & Transparency • TF Lifecycle Management ("Living Agreement") • Support & Capacity Building (IGs) • Scalability to Support Array of Participants (Horizontal/Vertical) • Glossary of TF Terms/Definitions • Modular Approach for TF Elements – IdPs, RPs & ITSPs • Law Enforcement (LE) Use Case: Support for Data Sharing • Federal Government Use Case: Federal Agency as RP (FICAM)

Trust I Security Framework – Exchange Assessment	Alignment (+) with Required Elements & Provisions for CSDII Pilot Project			
	Business	**Legal**	**Technical**	**Other**
AAMVA DL/ID Security Framework	+ Data element-level verification and validation (§1.3 #9, §1.4 #10, §1.4 #13, §3.3.4, §7.4, Appdx.) + Data (Name) collection, use and maintenance (§3.3.4, §7.1, Appdx.) + AAMVA DL/ID Personal ID Card Design Specification (§1.4 #12, §3.3.4, 7.3, Appdx.) + Procedures for initial customer ID and validation (§3.3.3, §6.0) + Record & document use, permitted purpose (§3.3.5, §4.6, §7.1, §8.0) + Benefits/ business drivers (§2.0, §3.1) + Business-driven agreement among MVAs (§3.1, §3.3, §4.5) + Business requirements for P&Ps, document issuing systems, and internal controls, Driver License Agreement (DLA) (§3.3.1, §4.2, §4.5, Appdx.)	+ Assumes MVA compliance with applicable law, document use, data sharing (§1.5 All Recs., §3.1, §3.2, §3.3.5, §4.5, §8.3, Appdx.) + Enforcement thru business requirements (§2.0, §3.1, §4.5) + Audit plan (§1.1 #2, §1.2 #5, §3.3.2, §5.1, Appdx.) + Compliance and oversight, internal controls (§3.3.2, §4.4, §5.2) + Risk assessment & management (§1.1 #3, §3.3.5, §4.2, §4.4, §8.0) + Privacy (§1.1 #4, §4.2, Appdx., §3.3.4, §3.3.5, §4.5, §4.6, §7.1, §7.4, §8.3) + Common set of verifiable resources (§1.3 #8, §3.3.3, §6.2, Appdx.) + Machine-Readable Technology (MRT) (§3.3.5, §8.2, Appdx.) + Restrictions, minimum penalties and sanctions (§3.3.5, §8.1, Appdx.)	+ Electronic verification (w/issuing entity) of DL/ID data elements (§1.3 #9, §3.3.3, §6.3) + Standards for MVA system integrity, interoperability & reciprocity (§2.0, §3.1, §3.3.2, §4.2, §4.5) + Compliance & oversight with adopted standards (§3.3.2, §4.5, §5.2) + System integrity, security & privacy (§4.6)	+ Compliance and implementation support thru FDR employee training (§1.1 #1, §3.3.1, §4.1) + Common definition of “residency” (§1.3 #6, §3.3.3) tied to DL/ID verification (§1.3 #7, §3.3.3, §6.1) + “End of stay” on immigration doc. as expiration date for DL/ID - data element derivation (§1.4 #11, §3.3.4, §7.2, Appdx.) + Horizontal scalability thru reciprocity (§3.1) + Openness enforced thru privacy provisions (§4.6, §7.1) + Limits on disclosure enforced thru privacy provisions (§4.6, 7.1) + Glossary of abbreviations/ acronyms (§9.0) + LE Use Case (§1.5 Rec. #8, data sharing §3.3.5, §8.3, Appdx.)

Trust I Security Framework – Exchange Assessment	Gaps (–) with Required Elements & Provisions for CSDII Pilot Project			
	Business	**Legal**	**Technical**	**Other**
AAMVA DL/ID Security Framework	– Does not bind RPs or ITSPs to same set of business requirements as IdPs – Fails to establish governing body (also no granting of authority) or change processes to maintain framework – Does not address participant suspension or termination – Structured as a voluntary agreement rather than a binding contract; inadequate to structure an exchange	– Does not contain necessary set of legal agreements to structure an exchange – Lacks the force of law (i.e., legal contract) to compel participant compliance or performance – Fails to establish P&Ps for dispute resolution – Does not bind RPs or ITSPs to same legal requirements as IdPs – Does not include anti-circumvention provisions (one-off agreements) – Due to scalability issue, fails to assign liability & risk to non-MVA participants – "Thin" assumption of participant compliance with applicable law may be inadequate to meet legal (OAG) scrutiny	– Contains only limited operational/technical components – Fails to clearly establish performance & service specifications or applicable standards – Does not bind RPs or ITSPs to same set of technical requirements as IdPs – Does not address breach notification or related security requirements – Limited specifications for system access policies – Lacks requirements on participant duty to respond to requests – Does not address treatment of test data v. production data; future use of data	– Does not support or anticipate non-MVA participants, except for LE (horizontal/vertical scalability) – Does not bind RPs or ITSPs to same set of training requirements as IdPs – Lacks governance provisions to ensure a "living" framework

Trust I Security Framework – Exchange Assessment	Alignment (+) with Required Elements & Provisions for CSDII Pilot Project			
	Business	**Legal**	**Technical**	**Other**
eHealth Exchange Data Use & Reciprocal Support Agreement (DURSA)	+ Definitions of permitted purpose (§1.jj; §3; §5.01-5.03) + Governing body (§4) & change processes (§10.03; §11.03) + Operating policies & procedures (§11; Appdx.; change process in §11.03) + Security, privacy & confidentiality (§7; §8; §14) + Suspension & termination (§19) + Data elements & data classification (attribute level/PII) (§1.v; §1.w; §1.kk) + Expectations of performance (§12)	+ Definition/ compliance w/ applicable law (§1.a; §15.11; §23.01; Appdx.) + Legal agreements (set) for exchange structure (recitals; §1.ee; §3.01; §23.07) + Security, privacy & consent (§14) + Liability (§18) + Representations & warranties (§15; disclaimers in §17) + Grant of authority (§4.03) + Dispute resolution (§21; Appdx.) + Authorizations for data exchange (§12; §13) + Open disclosure & anti-circumvention (§15; §23.04; §23.07) + Confidential participant information (§16) + Audit (§9) + Accountability & compliance (§10.01; §11.01; §15.03; §15.06)	+ Performance & service specifications (§10; Appdx.; change process in §10.03) + Security, privacy & confidentiality (§7; §8; §14) + Breach notification (§14.03) + System access (§6) + Provisions for future use of data (§5.02) + Expectations of participants (§12) + Duty of response by participants (§13) + Onboarding, testing & certification (§10.01) + Handling of test data v. production data (§15.07)	+ Openness & transparency (overview; recitals) + TF lifecycle management (“living agreement”) (overview; §4; §10.03; §11.03) + Scalability to support array of participants (horizontal/vertical) (participant types defined in §1; expectations in §12.02; duties in §13) + Glossary of TF terms/definitions (§1) + Modular approach for different participant types (types defined in §1; expectations in §12.02; duties in §13; warranties in §15)

Trust I Security Framework – Exchange Assessment	Gaps (–) with Required Elements & Provisions for CSDII Pilot Project			
	Business	**Legal**	**Technical**	**Other**
eHealth Exchange Data Use & Reciprocal Support Agreement (DURSA)	– Definition of "permitted purpose" assumes all participants will exchange same type of data/message content; no distinction between participant types (IdPs; RPs; ITSPs) – Governing body not established in statute/regulations may have limited capacity to issue binding actions – Legal status of TF may be too limited to bind government agencies to operational P&Ps – Governing body action to suspend or terminate may be interpreted as a government agency ceding its statutory authority – Assumes transmittal of a standardized "document" (HL7 CCD) and message content; does not specify down to the attribute level	– Definition of "applicable law" would need to be expanded to cover required data elements and domains – Uncertain whether state agencies would have legal ability to execute TF agreements, and if so at what level (agency head? Secretariat?) – Assignment of liability, representations and warranties, as written, would be barriers for state agencies – Grant of authority to governing body would not be possible for state agencies (sovereignty) – Audit, compliance and dispute resolution requirements may be interpreted as a government agency ceding its statutory/ regulatory authority – Does not provide guidance on risk analysis or management	– Regulations governing security, privacy & confidentiality differ based on government agency levels and domains; TF needs to address (or at least take into account) – Breach notification and other technical requirements would need to be reconciled with applicable statutes/regulations – Expectations for participants may be interpreted as a government agency ceding its statutory/ regulatory authority	– Limited scalability outside of the health IT/HIPAA domain; requires expanded scope of applicable law and participant types (IdPs; RPs; ITSPs) – Acts as a blanket TF under which each participant must fully execute/comply or forfeit participation; no modular approach for different participant types (IdPs; RPs; ITSPs) – Training and implementation support (IGs) left up to individual participants or vendors; disparate mechanisms – Contains only general references to use cases and other business elements

Trust I Security Framework – Exchange Assessment	Alignment (+) with Required Elements & Provisions for CSDII Pilot Project			
	Business	**Legal**	**Technical**	**Other**
InCommon Trust Framework	+ Definitions of permitted purpose (ICPOP; IAS; limits on use of ID information in PA §9) + Governing body & change processes ICBL; ICPP; ICPOP; PA §17) + Operating policies & procedures (ICBP; ICPP; ICPOP) + Security, privacy & confidentiality (PA §6, §9; ICPOP) + Suspension & termination (PA §5.b, §5.c; ICBL) + Data elements & data classification (attribute level/PII) (IAS; FTG; PA §6.b) + Expectations of performance (ICBP; PA §6, §7) + Use cases and examples (InCommon Website; ICBP; Participants)	+ Definition/ compliance w/ applicable law (PA §15) + Legal agreements (set) for exchange structure (ICB; ICPP; PA §6, §7.b) + Security, privacy & consent (PA §6, §9) + Liability (PA §11, includes disclaimer & limitations) + Representations & warranties (addressed in PA §7.b) + Grant of authority to executive (PA §18) + Dispute resolution process (PA §10; ICBL §5) + Authorizations for data exchange (PA §18) + Open disclosure & anti-circumvention (PA §14, §16) + Confidential participant information (PA §8, §9) + Audit (IAF) + Accountability & compliance (PA §15; IAF)	+ Performance & service specifications (FTG; ICBP; PA §6, §7) + Security, privacy & confidentiality (ICBP; ICPOP) + Breach notification (PA and addenda; ICPOP) + System access (ICBP) + Provisions for future use of data (ICPOP) + Expectations of participants (ICBP; PA §6, §7) + Duty of response by participants (ICBP; PA §6, §7) + Onboarding, testing & certification (ICBP) + Handling of test data v. production data (ICPOP)	+ Openness & transparency (ICBP; ICBL) + TF lifecycle management (“living agreement”) (ICBL; ICBP; PA §17) + Implementation support (ICBP; ICPOP) + Scalability to support array of participants (horizontal/vertical) (participant types defined in Join §1, Participants; ICBP) + Glossary of TF terms/definitions (InCommon Website) + Modular approach for different participant types (ICB; Participants)

Join=www.incommon.org/join.html; Participants=www.incommon.org/participants/
FTG=InCommon Federated Technical Guide; ICBP=InCommon Basics and Participating in InCommon, Jan. 21, 2011
ICPP=InCommon Policies and Practices; ICPOP=InCommon Participant Operational Practices; ICBL=InCommon Bylaws
PA=InCommon Participation Agreement; IAS=InCommon Attribute Summary; IAF=InCommon Assurance Framework

Trust | Security Framework – Exchange Assessment	Summary of Alignment with Required Elements & Provisions for CSDII Pilot Project
InCommon Trust Framework	The analysis failed to identify any substantive gaps in the InCommon TF Model, which ranked as the most robust, mature, and scalable of those reviewed for the CSDII Pilot Project. Primary strengths of the InCommon TF: • Addressed the cited concerns relating to legal issues for state government agencies, including sovereignty, statutory authority, liability, and grant of authority. • Provided detailed guidance, agreements, and support documentation for structuring an exchange in the ID assurance and management space. • Established binding BLT requirements for all relevant participant types, including Identity Providers (IdPs), Relying Parties (RPs), and Assurance Providers. • Featured extensive use-cases demonstrating the types of participants, types of exchanges, operational/functional elements, and other dimensions of the exchange.

Trust I Security Framework – Exchange Assessment	Alignment (+) with Required Elements & Provisions for CSDII Pilot Project			
	Business	**Legal**	**Technical**	**Other**
Kantara Initiative Trust Framework	+ Definition of permitted purpose (KTR MTAU) + Governing body (BL §4; OP §2) & change/ amendment processes (BL §12; OP §9; MA §3) + Operating policies & procedures (OP) + Security, privacy & confidentiality (AP; MA) + Suspension & termination (MA §2; BL §8.11; KTR MTAU) + Data elements & data classification (KTR; KIC) + Expectations of performance (AP; KTR MTAU; KIC) + Use cases (Working groups for business cases-trusted federations)	+ Definition/ identification of applicable law (KTR MTAU; see also "Governing law and jurisdiction" provision in KTR MTAU) + Legal agreement for exchange structure (MA) + Security, privacy & consent provisions + Liability (KTR MTAU) + Warranty (KTR MTAU) + Grant of authority (MA) + Authorizations for data requests by participant + Open disclosure & anti-circumvention (Other agreements in KTR MTAU) + Confidential participant information (Options set in IPRP; IPRP Art. 3) + Accountability & compliance (w/ antitrust laws in BL §17; MA)	+ Performance & service specifications (AP; KTR/KTV; KTR MTAU; KIC; Member protection & treatment in IPRP) + Security, privacy & confidentiality (AP; MA) + Technical certification & testing (AP; KIC) + Standards for technical & operational interoperability (KTR; MA goal #3; #7; KIC)	+ Open & transparent governance model (MA goals #3, #4; op; BL §3) + TF lifecycle management (MA goals #4, #6) + Support & capacity building (IGs) + Scalability to support array of participants (horizontal/vertical) (member types BL §8) + TF definitions (BL §1; OP §1; IPRP Art. 2)

BL=Bylaws; IPRP=Intellectual Property Rights Policies; MA=Member Agreement; OP=Operating Procedures
KTR=Kantara Trust Registry; KTV=KTR Trust Validation; KTR MTAU=Metadata Terms of Access & Use; KIC=Kantara Interoperability Cert.-SAML, OATH, etc.
AP= Assurance Programs; Identity Assurance Accreditation & Approval and Interoperability Certification Programs

Trust I Security Framework – Exchange Assessment	Gaps (–) with Required Elements & Provisions for CSDII Pilot Project			
	Business	**Legal**	**Technical**	**Other**
Kantara Initiative Trust Framework	– Permitted purposes limited to assurance & interoperability dimensions; "thin" on provisions for RP use – Governance model & operational procedures do not structure an actual exchange rather designed to be used by members for their exchanges – TF focuses on IdPs, Credential Service Providers & Assurance Providers; provisions limited for RPs	– TF contains a well established legal framework for membership & governance but does not structure an actual exchange – "Thin" statements re compliance with applicable law – TF limited to setting requirements for member use of technical and operational assurance programs for their own exchanges – TF does not fully address audit requirements – Legal provisions contain only limited provisions for RPs; main focus on IdPs, Credential Service Providers & Assurance Providers – Bylaws and operational policies do not provide for dispute resolution	– Performance, service and other technical specifications set for IdPs, Credential Service Providers & Assurance Providers; limited coverage for RPs – RPs play narrow role as inputs on IdP and assurance requirements – Specifications do not cover an actual exchange but designed to support member use in their exchanges – Certification & testing but "thin" coverage for RPs or other potential participant/member types	– Governance model sets up for a "living" TF thru an extended lifecycle, with horizontal and vertical scalability; however, limited on RPs and other potential participant/member types

Trust I Security Framework – Exchange Assessment	Alignment (+) with Required Elements & Provisions for CSDII Pilot Project			
	Business	**Legal**	**Technical**	**Other**
Open Identity Exchange (OIX)/OITF Model	+ Definitions of permitted purpose (OITF §III.B, §III.C, §V) + Governing body & change processes (OIX; OITF §III.C) + Operating policies & procedures (OIX; OITF §II, §III.B, §III.C) + Security, privacy & confidentiality (OIX; OITF §III.A, §V) + Suspension & termination (OITF §III.C) + Data elements & data classification (attribute level/PII) (OIX; OITF §III.A, §III.B) + Expectations of performance (OIX; OITF §II, §III.C) + Use cases for agreement, transaction & participant types (OITF §I, §III; OIX)	+ Compliance w/ applicable law (OIX; OITF §V) + Legal agreements (set) for exchange structure (OIX; OITF §II, §III.C) + Security, privacy & consent (OIX; OITF §III.A) + Liability, representations & warranties (OITF §III.C) + Grant of authority (OIX; OITF §III.C) + Dispute resolution (OITF §II, §III.C, §V) + Authorizations for data exchange (OIX; OITF §III.A) + Anti-circumvention & open disclosure (OITF §V) + Audit (OIX; OITF §II, §III.B, §V) + Accountability & compliance (OIX; OITF §II, §V)	+ Performance & service specifications (OIX; OITF §II, §III.A, §III.B) + Security, privacy & confidentiality (OIX; OITF §III.A; §V) + Expectations of participants (OIX; OITF §III.A, §III.B, §III.C) + Onboarding, testing & certification (OIX; OITF §II, §III.B)	+ Openness & transparency (OIX; OITF §I; statement in OITF §V, §VI) + TF lifecycle management (OIX; OITF §II) + Scalability to support array of participants (horizontal/vertical) (OITF §II, §III.C, §IV) + High-level definitions (OITF §I) + Modular approach for different participant types (OIX; OITF §II, §III.C) + Use cases & examples of TFs (OITF §IV)

Trust I Security Framework – Exchange Assessment	Gaps (–) with Required Elements & Provisions for CSDII Pilot Project			
	Business	**Legal**	**Technical**	**Other**
Open Identity Exchange (OIX)/OITF Model	– Highlights primary business-related TF elements and requirements; however, fails to provide level of specificity needed for structuring an exchange – Reads more like a high-level checklist for TF elements & provisions rather than an actual TF (That said, OITF will be useful as a checklist to ensure alignment for the CSDII TF; also, OITF provides several use cases and examples of an ID exchange)	– Outlines primary legal TF elements and requirements; however, fails to provide documents/ agreements needed for structuring an exchange – Provides a checklist for the set of necessary legal agreements for the TF and a high-level identification of the issues to be covered in the agreements (i.e., grant of authority, liability, warranties, authorization, etc.); however, no "concrete" examples or agreement models – States the requirement for participants to comply with applicable law but does not cite governing statutes, laws and regulations for an actual exchange	– Identifies primary technical elements and requirements to be covered in a TF; however, fails to provide level of specificity needed for structuring an exchange – Provides a checklist for the set of necessary technical specifications, certification and testing of those specifications; however, OITF stops as simply identifying the specifications and LOA certification without giving detailed content provisions	– Addresses the necessary principles of openness, transparency, scalability and full lifecycle management; however, as with the other domains fails to provide the degree of specificity needed for structuring an exchange

Trust I Security Framework – Exchange Assessment	Alignment (+) with Required Elements & Provisions for CSDII Pilot Project			
	Business	**Legal**	**Technical**	**Other**
CIVICS/ IDCubed.org Trust Framework	+ Definitions of permitted purpose (ID3LA §3, §5.2 §5.3; CTA §2.4.2.5) + Governing body & change processes (ID3LA §9.8) + Operating policies & procedures (ID3LA) + Security, privacy & confidentiality (ID3LA §6, §17; CTA §2.4.2.7) + Suspension & termination (ID3LA §4.4, §11) + Data elements & data classification (attribute level/PII) (ID3LA §3, §5.2 §5.3; CTA §2.4.2.2.3.1) + Expectations of performance (ID3LA §4, §9; CTA §2.4.2.2.3.1)	+ Compliance w/ applicable law (ID3LA §9.7, §18, §24.8) + Legal agreements (set) for exchange structure (ID3LA; CTA §2.2) + Security, privacy & consent (ID3LA §6, §17; CTA §2.4.2.7) + Liability (limitations ID3LA §13.2; CTA §2.5.2) + Representations & warranties (ID3LA §19) + Grant of authority (ID3LA §24; CTA §2.2.1) + Dispute resolution (ID3LA §21) + Authorizations for data exchange (§12; §13) + Non-exclusivity (ID3LA §5.4, assignment ID3LA §24.3) + Confidential participant information (ID3LA §7, §10, §17; CTA §2.3.1.1) + Audit (ID3LA §16.2; CTA §2.4.2.8) + Accountability & compliance (ID3LA §16.3, §18; CTA §2.4.2.8)	+ Performance & service specifications (ID3LA §9) + Security, privacy & confidentiality (ID3LA §6, §17; CTA §2.4.2.7) + Breach notification (ID3LA §17.3) + System access (ID3LA §7.2) + Provisions for future use of data/services (ID3LA §3.8) + Expectations of participants (ID3LA §4, §9; CTA §2.4.2.2.3.1) + Duty of response by participants (ID3LA §4, §9; CTA §2.4.2.2.3.1) + Onboarding, testing & certification (ID3LA §4; CTA §1.3.1)	+ Openness & transparency (ID3LA §1; CTA §2.4.2.1) + TF lifecycle management (ID3LA §1) + Scalability to support array of participants (ID3LA §1, participant types defined in Schedule 2; CTA §1.2) + Glossary of TF terms/definitions (ID3LA Schedule 2; CTF Addenda 2) + Modular approach for different participant types (ID3LA §1, participant types defined in Schedule 2; CTA §1.2) + ID3LA= IDCubed.org Legal Agreement for Trust Framework Data Store, Nov. 8, 2012/CTF=Civics Model Trust Framework for Person Data, Feb. 22, 2012

Trust | Security Framework – Exchange Assessment	Gaps (–) with Required Elements & Provisions for CSDII Pilot Project			
	Business	**Legal**	**Technical**	**Other**
CIVICS/ IDCubed.org Trust Framework	– CIVICS Model TF contains the high-level elements & provisions to support business-related requirements for an exchange; however, the model has not achieved a level of maturity needed to fully support the CDSII Pilot Project – Additional model documentation & examples, particularly of the Commonwealth of Massachusetts, would be needed to make a final determination – Model does not fully address data elements & permitted purposes	– CIVICS Model TF features legal agreements to support an exchange; however, it is unclear whether the model's legal framework would be adequate to cover state agency participants – For future analysis, it would be beneficial to have examples of other implementations, particularly the Commonwealth of Massachusetts procurement TF (referenced during presentation on 2/14/2013)	– Model TF does not provide level of specificity in key technical areas, including performance & service specifications; onboarding, testing & certification; breach notification & system security	– Model could be supported more fully by use cases, examples of participants & transactions, & implementation guides

American Association of Motor Vehicle Administrators
4301 Wilson Boulevard, Suite 400
Arlington, Virginia 22203
703.522.4200 | **aamva.org**