March 31, 2020

Description of Federal Identity Issues in Support of the FedID Call for Program Ideas

INTRODUCTION

The Federal Identity Forum (FedID) has been the U.S. Government's annual identity conference since 1995. Its **mission** is to bring together identity experts to exchange information and enhance public-private collaboration to **solve the federal government's toughest identity challenges** and **help ensure a vibrant identity community.**

While beginning to develop FedID 2020, Planning Committee members decided to significantly focus on three fundamental areas of utmost importance to federal identity activities over the next few years and request input from the identity community on how to best address them during the event. Our objective is for the public-private FedID community to collaboratively develop consensus recommendations for these areas, which the government can then leverage as they plan and implement their identity strategies.

Each of these three fundamental areas are introduced in the following sections, with issues of interest further described. We are asking for the community's input on these issues:

- Is there an issue that we mention that is not well understood by the private sector, and thus the government needs to better explain at FedID?
- What are the innovative ideas out there, or experiences from other sectors, that the government needs to be aware of for a specific issue, & who would be best to present those ideas at FedID?
- Do you have ideas on how to best investigate an issue and develop public-private consensus on the way forward (such as a panel discussion, small group workshop, a hackathon-like activity, etc.) that we could implement at FedID?
- (Marketing pitches are not allowed at FedID, and stovepiped solutions aren't really "solutions" in the federal space, so submissions on these lines will not be considered.)

Note that not all of the issues identified below will be addressed during the conference due to time constraints, and it is highly likely that submitted ideas will be merged and evolved while developing the program.

AREA 1: GOVERNMENT-CITIZEN INTERACTION

Introduction

Government to citizen interaction is the heart of the mission for many Federal departments and agencies. As citizens interact with the government for benefits, jobs, taxes, and education, digital identification underpins all those interactions. With more and more services moving online, citizens are finding more reasons than ever to interact digitally with the government; and agencies are looking to improve and streamline those transactions. In this track we will explore and highlight ways that agencies can leverage and reuse data, attributes, and fully verified identities to minimize the friction between citizens and the services they receive.

Issues of Interest

Issue #1-1: Federation

Federation allows identities to be shared across autonomous domains securely allowing users to access data or systems in those domains without redundant identity processes. Federation can occur at every step of the identity process – from proofing and verification to authorization and authentication. There are many examples of success uses of federated identities in the private sector. However, federation for citizen services in the public sector has been notoriously difficult – especially when looking at proofing and verification. This track will explore what has worked and what has not worked in the federal government as well as the best practices in the private sector that can be leveraged to enable the development and implementation of truly federated citizen identities. Questions include:

- What are the citizen services that would most benefit from federated identity solutions? Services at VA, CMS, Education, IRS, and SSA come to mind. What others are out there?
- What programs/pilots are currently happening in the government that can be leveraged/grown?
- What has prevented wide adoption of a federated credential strategy thus far?
- What are the federated identity practices that work in the private sector?
- Are there specific technologies, standards, use-cases that need to be highlighted to help drive federation across those agencies?
- How do we get beyond NIST 800-63-3 C? How does a citizen get a credential and then transfer it between and among agencies?

Issue #1-2: Attribute Validation

The U.S. government houses a number of authoritative identity systems that play an important role in building an identity ecosystem that citizens can leverage when interacting with both public and private sector entities. The creation of "Government Attribute Validation Services" can help to transform legacy identity verification processes and help consumers and businesses alike improve trust online. Such services could be offered by an agency itself, or through accredited, privately run "gateway service providers" that would administer these services and facilitate connections between consumers, online services providers, and governments. In fact, the Social Security Administration (SSA) is currently leading the way through its electronic consent based social security number verification (eCBSV) service. However, SSA is by no means the only authoritative data source in the government that can be leveraged to improve the identity ecosystem and support a trusted digital identity ecosystem. This track will look at use

cases and incentives to offer validation services. It will also look at how these services can build robust digital identification that can be used in both the public and private sector. Questions include:

- What are the barriers and incentives for agencies to offer validation services?
- What are the authoritative data sources that agencies have that could be leveraged?
- What lessons have we learned from the eCBSV service?
- How do validated attributes build trusted identities in the private sector? How can citizens leverage those identities to access services?
- What role do the state DMV's play in this effort?
- How does can mobile driver's licenses be leveraged to access citizen services?
- How will the REAL ID implementation impact these efforts?

Issue #1-3: Verifiable Credentials

Verifiable Credentials are one of the latest technologies promising to enable a secured digital credential. One of the benefits touted is the creation of an identity ecosystem that preserve an individual's privacy while decentralizing the verification of identity attributes. However, there are many challenges facing the wide adoption of Verifiable Credentials including the current lack of protocol standards.

- What are the current pros and cons of Verifiable credentials?
- Where is the market in adopting Verifiable Credentials and what are the hurdles that need to be conquered?
- Is there an approach where Verifiable Credentials can be used to augment existing digital credentials by simply verifying attributes and not the core identity itself?
- Will state and federal governments accept the adoption of an identity assertion that is decentralized on the block chain?

Issue #1-4: Payment Integrity

Payment integrity is a major federal concern: $175B in losses in FY19 (which is greater than the federal government's entire R&D budget), and one of the areas of focus within the President's Management Agenda. Identity issues are one of the two largest components of payment integrity (alongside benefits eligibility) but is a "known unknown" because there is no known way to obtain accurate metrics. Questions:

- Are there ideas on how to assess federal identity practices within the payments space, to both find areas of fraud and provide better estimates on its impact?
- What practices have been successful in minimizing identity issues within the payments community that the government should investigate?

Issue 1-5: Remote Submission and Verification of Breeder Documents

As the government continues providing more virtual services, the desire to remotely establish your initial identity for government applications will continue to grow. Citizens will desire a way to provide breeder documents (such as birth certificates) in a secure online manner, while governments will need new ways of verifying them to prevent fraud.

- Are there lessons-learned on how this has been done in other jurisdictions?
- Most breeder documents were issued prior to the digital age. How could they be submitted and verified remotely?

Issue #1-6: Regulations and Compliance for Identifying Individuals and Legal Entities

Digital identity can enable improved customer identification and verification in the digital age, with a promise of greater efficiency, security, interoperability, and trust in a variety of settings. However, the development of a digital identity ecosystem touches on issues that cross sectors and industries, such as policies and regulations related to anti-money laundering and combating the financing of terrorism (AML/CFT), critical infrastructure safety and soundness, privacy and fairness controls, and healthcare quality and protection. To prevent abuse of industry sectors and citizen data while also enabling access to key services, U.S. government regulators often require private organizations to identity counterparties in their lines of business, including individuals, corporations, or even products and services. This can include implementing "know your customer" (KYC) procedures, due diligence processes for business relationships, supply chain verification, and other protections that protect against fraud, inequity, and other illicit or undesirable outcomes. As technologies and business models evolve, regulators face the need to assess the effectiveness of the regulatory environments in mitigating risks and achieving desired outcomes without stifling appropriate innovation.

- How are innovations in identity-related solutions enabling compliance with varying regulations across industry sectors? How are identity solutions useful in combating risks across sectors, including risks related to cybersecurity, fraud, privacy, inclusion, and illicit finance?
- How are emerging technologies and threats hindering compliance with and effectiveness of identity-related regulations and laws?
- How are cross-sector regulatory or legislative environments hindering or enabling responsible innovation that leverages industry standards?

AREA 2: IDENTITY & THE FEDERAL ENTERPRISE

Introduction

Identity and the Federal Enterprise represents a complex ecosystem of identities, resources and data enabling the public service mission. While the phrase, "Right individual to the right resource at the right time for the right reason," is simple on the surface, identity in the federal enterprise represents multiple, sometimes conflicting, drivers in cybersecurity.

Issues of Interest

Issue #2-1: PIV Interoperability

A Personal Identity Verification (PIV) is a governmentwide credential (which contains certificates and key pairs, pin numbers, biometrics, and other unique identifiers) used to access federally-controlled facilities and information systems at the appropriate security level. The government is interested in leveraging or creating non-vendor specific federation protocols for authentication interoperability between federal agencies within the next generation of PIV. What technical or policy gaps remain to enable this objective and how should the community best overcome them?

Issue #2-2: Exemplars from CDM Phase 2

Phase 2 of DHS' Continuous Diagnostics and Mitigation (CDM) program (an approach to fortifying the cybersecurity of government networks and systems) focused on identifying who is on the network – an identity-focused task that addressed privilege management and infrastructure integrity by allowing agencies to monitor users on their networks and to detect whether users are engaging in unauthorized activity. We are seeking to identify exemplar pilots, unique insights and consistent best practices that can be leveraged elsewhere within the federal enterprise:

- Acquisition
- Agency Implementation
- Smaller agencies that leveraged shared services

Issue #2-3: Zero Trust & ICAM – The Need for Risk-Based Access Control

Zero Trust is a cybersecurity strategy and framework that embeds security throughout the architecture for stopping data breaches. This data centric security model eliminates the idea of trusted or untrusted networks, devices, personas, or processes; and shifts to multi-attribute based confidence levels that enable authentication and authorization policies under the concept of least privileged access. Zero Trust requires a paradigm shift, from a legacy defense-in-depth security model that is hierarchical and transport focused to a data centric model optimized for the enterprise. Security strategies must be designed around a Zero Trust approach—in other words, one that trusts nothing outside or inside an organization.

- How do we adopt and implement digital identity best practices in a Zero Trust environment?
- How do we implement ICAM capabilities in a data centric environment?
- The Office of Management and Budget (OMB) released their new identify guidance for federal and government workers. How does the ICAM updates (OMB memo 19-17) for credentialing for people and devices pave the way to a Zero Trust environment?

Issue #2-4: ICAM in the Cloud

Protecting data in the cloud has its own unique challenges, especially if additional compliance regulations need to be met. Building in layered security, especially identity, credential and access management (ICAM) controls around your data, regardless of where that data resides is essential to operate in the cloud. Protecting cloud-based data becomes even more complicated when industry or governmental regulations require that the data be protected to meet compliance regulations, such as Payment Card Industry Data Security Standards (PCI DSS) for credit card or personally identifiable information, and the Health Insurance Portability and Accountability Act (HIPAA), or Health Information Technology for Economic and Clinical Health Act (HiTECH), for data in the healthcare industry.

- It seems obvious that companies will build in such controls around their most valuable data within their data center, but how does one protect private data when it resides on someone else's data center in the cloud?
- ICAM in the cloud, which is slowly being mitigated with technology advancements, is identity management across multiple independent organizations. How do users properly authenticate and manage access to data when integrating applications with cloud computing solutions?
- The biggest challenge for cloud services is identity provisioning. This involves secure and timely management of on-boarding (provisioning) and off-boarding (deprovisioning) of users in the cloud. How are organizations addressing this challenge?

Issue #2-5: Innovative programs or concepts

Those working in the identity area are extremely knowledgeable, experienced, and collaborative, which has been a key reason for its growing successes over the past few years. While that is mostly positive, it does have some drawbacks, such as potential of "groupthink" and making it difficult for outsiders to raise new ideas. Thus, we are purposefully seeking to hear of different ideas or implementations from nontraditional players, which could have positive ramifications, or alter the plans of, the federal government.

AREA 3: HOMELAND/NATIONAL SECURITY AND LAW ENFORCEMENT APPLICATIONS

Introduction

Homeland/National Security and Law Enforcement identity activities have long been driven by federal agencies, with FedID playing an important information exchange and collaboration-building resource into the design of federal programs in the post-9/11 environment. These programs are looking for innovative ways to improve – by strengthening security and law enforcement capabilities and simultaneously enhancing privacy and civil liberties protections. One of the most significant security threats our nation faces is the increase in cyber threats. Maintaining confidence to protect our information and privacy and ensuring that federal, state, and local governments as well as the private sector can perform their missions is essential to protecting our democracy and standard of living in today's competitive environment.

Issues of Interest

Issue #3-1: Advancing Biometrics & Leveraging within Homeland/National Security & Law Enforcement Applications

Biometrics have been a critical component of our homeland and national security activities since the days immediately following 9/11, with law enforcement applications even predating that. Federal agencies implemented collaborative R&D strategies & worked together to implement and enhance numerous federal programs. FedID is interested in investigating newly discovered best practices, both operational and oversight, as well as technological gains that will drive next-generation capabilities.

- What operational or oversight best practices have been discovered over the past year that could be applied to other federal systems?
- What research outcomes do federal agencies need to be aware of, either to improve current operations or to drive our next generation systems?
- What are the critical gaps in the national biometrics R&D portfolio?

Issue #3-2: Face Recognition (& other Biometrics) - Protecting Privacy & Civil Liberties

The robustness of artificial intelligence and availability of data has made it much easier to create biometric recognition algorithms than in the past, with a corresponding growth in fielded applications. This has led to a growing consensus on the need to construct *comprehensive* regulations and oversight structures, particularly and most vocally for face recognition applications, that provide oversight for data collection, storage and use in order to maintain civil

liberties and protect the privacy of our citizenry. These positive efforts have been hampered by significant promulgation of incorrect information about the technology and a growing proliferation of systems that were not developed or implemented by those with knowledge of identity & privacy community norms and best practices.

- How do we best update the identity community's existing best practices on collection, use, and management of biometric data? More importantly, how do we indoctrinate these practices into those new to the community?
- How do we overcome misinformation about biometric technologies and identity-focused federal programs, and replace sentiment-driven reactions with evidence-driven data, so that national debates can be properly grounded?
- How do we create regulatory and oversight practices that enable needed government biometric applications while simultaneously enhancing our ability to protect our citizens' privacy and civil rights?

Issue #3-3: ICAM Policy for National Security Systems & Other High-Value Assets

All federal departments and agencies, contractors, agents, and non-Federal affiliates (that support federal activities) that own, procure, operate, or maintain National Security Systems on the Federal Secret Fabric must follow the *National Directive for Identity, Credential, and Access Management (ICAM) on the (US) Federal Secret Fabric.* The Department of Homeland Security has similar requirements for additional high-value assets. Issues under consideration as these directives and implementation guidance evolve include:

- How to implement a data-centric approach?
- What are the optimal alternatives to PIV/CAC for improving authentication to these networks and resources (e.g., MFA)?
- What are the best practices to deploy shared services for implementing enterprise ICAM capabilities?
- What ICAM capabilities exist to support identity analytics for detecting insider threats and external attacks?

Issue #3-4: Identity Applications for Public Safety, Emergency Preparedness & Response

It is increasingly important for first responders, paramedics, law enforcement agencies, emergency medical service providers, public health and hospital infection control experts, and other public safety entities to have identity solutions that can speed emergency/incident response across multiple jurisdictions. Current manual credentialing of new users needs to be replaced by dynamic vetting across a federated environment.

- How can we leverage this community's current identity structure to enable rudimentary cross-jurisdictional ICAM in the near-term?
- What unique insights or best practices are available that will help build a next-generation federated environment that enables dynamic vetting?
- What are the remaining technological gaps preventing this next-generation environment from being developed? Regulatory limitations?

Issue #3-5: Leveraging Identity to Counter Criminal Activity

Identities can help protect citizens and ensure they get access to key services and control their sensitive information. Identities can also be high value targets for criminals that seek to unlawfully access those services and information, or to obscure their illicit activities by exploiting stolen or fabricated identities. Criminals often exploit vulnerabilities in government and industry identity services and processes in the conduct of fraud, theft, sanctions and tax evasion, money laundering, human trafficking, terrorist financing, and cybercrime. Law enforcement and other national security agencies face the challenge of having to investigate these criminals, generally requiring them to find the true identity of individuals and corporations across vast networks of illicit activity.

- What are the novel ways criminals are exploiting identities and identity-related information to support illicit activity, such as fraud, theft, sanctions and tax evasion, money laundering, human trafficking, terrorist financing, and cybercrime?
- What innovative identity solutions can enable law enforcement, national security agencies, and critical infrastructure organizations in detecting, investigating, and/or preventing illicit activity or actors affecting their organization or mission set?
- How can agencies and industry share identity information securely, and in respect of citizen liberty and privacy, to better identify illicit actors?