OBAMA-BIDEN TRANSITION PROJECT

THIS DOCUMENT WAS PRODUCED BY AN OUTSIDE PARTY AND SUBMITTED TO THE OBAMA-BIDEN TRANSITION PROJECT.

Industry Advisory Council
Transition Study Group

Government Federated Identity Management

Companion Paper to Identity and Access Management

December 9, 2008

Industry Advisory Council

Industry Advisory Council

The Industry Advisory Council (IAC) is a non-profit, non-partisan organization dedicated to fostering improved communications and understanding between government and industry. Through its affiliation with the American Council for Technology (ACT), the Industry Advisory Council provides a forum for industry to collaborate with and advise government executives on IT issues.

The Industry Advisory Council in cooperation with ACT is a unique, public-private partnership dedicated to helping government use technology to serve the public. The purposes of the organization are to communicate, educate, inform and collaborate. ACT-IAC also works to promote the profession of public IT management. ACT and IAC offer a wide range of programs to accomplish these purposes.

ACT and IAC welcome the participation of all public and private organizations committed to improving the delivery of public services through the effective and efficient use of information technology. For membership and other information, visit the ACT-IAC website at **www.actgov.org**.

Disclaimer

This document has been prepared to provide information regarding a specific issue. This document does not – nor is it intended to – take a position on any specific course of action or proposal. This document does not – and is not intended to – endorse or recommend any specific technology, product or vendor. The views expressed in this document do not necessarily represent the official views of the individuals and organizations who participated in its development. Every effort has been made to present accurate and reliable information in this report. However, ACT-IAC assumes no responsibility for consequences resulting from the use of the information herein.

Copyright

© Industry Advisory Council, 2008. This document may be quoted, reproduced and/or distributed without permission provided that credit is given to the American Council for Technology and Industry Advisory Council.

Further Information

For further information, contact the Industry Advisory Council at (703) 208-4800 or www.actgov.org.

Executive Summary: Government Federated Identity Management

Our nation's system of identity management is fragmented, inefficient and to put it bluntly, broken. It does not have to be this way.

The Obama administration has an opportunity to make significant changes and transform the landscape that exists today. This means developing a reliable, secure and centralized federal identity management and credential issuance system.

The concept is to create single globally unique personal identities, independent of any relationship that an individual has with a particular government agency or other enterprises. It also means developing mechanisms for federating identity, authentication, authorization and attribute management in a national framework that includes federal government agencies, state, tribal, and municipal governments, and industry partners.

The technology and know-how exists. It is now a matter of planning, coordination, political will, resources and a decision to act in concert with other stakeholders.

Such a program, while ambitious, would facilitate architectural conformity, process and procedure standardization. It should lead to an operating agreement framework and contain oversight capability to ensure system integrity. Upon widespread adoption, the federal government could elect to relinquish or delegate its oversight role in favor of federation partnership for self-governance.

This model could provide tremendous benefits for government, commerce, and private citizens in terms of security, privacy, convenience, and efficiency in managing identity and identity attributes. Much work has already been done. It is now time to take the next set of big steps.

Identity and Access Management

The Need for Centralization

The federal government has an opportunity to implement a centralized identity management framework that is based on the use of a single identity.

Identity is a collection of the attributes or characteristics that define the "oneness" of a discrete and unique physical individual. The notion of identity is contextual and is an often misunderstood subject in cyberspace. Comprehension of the subtleties of this topic is impeded by the imprecise nature of language. We are accustomed to thinking of a person's identity in a person-centric model where a name (first name/last name) is a "handle" or a shorthand mechanism for referencing an individual. When we encounter a name conflict where two or more individuals we know have the same name, we use nicknames or additional descriptors to referentially describe known individuals. When we deal with names for individuals we do not personally know, we often treat the name itself as the unique identity.

Identity management presents a challenging problem because there is a disconnection between an individual person and all logical representations of that person. All mappings between the two are currently based on attributes or collections of attributes that uniquely describes an individual. To be reliable, the collection must consist of unalterable attributes about the person and, as it turns out, there are actually very few personal attributes that generally do not change. Name, hair color, eye color, address, phone, weight, height, and even gender can change over time. Place of birth, date of birth, and Social Security number are among the few relative constants. It is precisely these unique attributes that comprise the most sensitive elements of Personally Identifiable Information (PII). Paradoxically, these PII attributes must be protected and their presence minimized in distributed systems. The best hope for securing PII is to eliminate its storage except where absolutely necessary.

The foundation of a comprehensive and rational approach to identity management is predicated on the concept of single identity. This does not imply that a given user is represented in a single identity system but more significantly that all representations of a given user's identity, across all discrete systems, are mapped to a single identity and without direct reliance on PII. The solution requires the use of a Person Identifier (PID) that maps to the union of SSN and either the date of birth and or place of birth will provide a distributable unique identifier for person identification.

Homeland Security Presidential Directive 12 (HSPD-12) was a reasonable attempt to standardize the identity credential process with goals of improving the security of federal resources and reducing the number of credentials an individual would need to maintain. The concept of identity management was not directly addressed in FIPS-201, but it was generally

understood that identity management was a prerequisite to HSPD-12 implementation. As HSPD-12 has developed, the tendency has been to think of the PIV credential as a secure token representing identity within the scope of an agency relationship.

Without a centralized federal identity framework, identity management and credential issuance became agency-specific. This constrains the identity and access management model from dealing with the underlying identity management and security challenges it was intended to address. Furthermore, managing identity solely in the context of an agency or operating entity relationship is inefficient. An individual with a relationship with Departments of State, Interior and Agriculture will require three PIV cards even though each agency can read other agency's cards. HSPD-12 heavily relies on the use of PIDs, but has neglected to provide a centralized authority or standards for PID issuance and management. Unfortunately, this means that PIDs are guaranteed to be unique only with the boundaries specific to the department such as the HSPD-12 PIV Card issuing authority.

How Centralization Could Work

In reality, the individual user exists independent of any agency relationship held in the past, present, or future. A centralized framework model would mean that possession of a PIV card makes no warrant other than that the cardholder has been adjudicated by a federal government entity and is who he or she claims to be. This model is agency-neutral and implies no relationship with any agency whatsoever, but it does provide a standard identity container in which agency relationships can be stored and managed.

One possible approach is to have Person Identifiers issued by a centralized authoritative body that stores and manages the critical PII used to test for PID exclusivity. The issuance process must first test new applicant PII to ensure the applicant has not been previously issued a PID. If not, the authoritative body should issue a PID that can be considered "a serial number for a belly button." This globally unique PID is assigned to the individual for life, independent of any relationship this person has with government entities at any point in time. The Office of Personnel Management (OPM) may be an appropriate authority to manage this responsibility. Government agencies would use this unique PID to identify users in their systems without the need to store PII in a distributed fashion.

With the introduction of background investigation adjudication standardization and reciprocity, it may be worthwhile to reexamine the costs and benefits of continuing distributed adjudication versus a centralized and potentially programmatic approach. Since OPM manages the background investigation process already, allowing OPM to be authoritative for adjudications may be considerably more effective.

Designating OPM as the authoritative source of both PIDs and background adjudications would allow HSPD-12 enrollment processes and OPM EQIP processes to be tightly integrated to improve efficiency and system integrity. One-to-many PIV card issuance authorities could

leverage the OPM identity store to minimize the distribution of PII and biometric data. This provides a centralized authoritative store, delegated issuance and administration. It provides for increased privacy and efficiency while reducing costs and redundancy.

Implementing a change from the confused identity-and-relationship model to the centralized identity framework would go a long way toward solving actual problems and would allow identity, agency relationships, and credentials to be more effectively managed. This would result in a stronger security foundation.

Advantages:

- Fully leverages universal scope of HSPD-12 solution.
- Single PIV card-issuing authority obviates need for coordination between PIV Card issuing authorities for card status.
- More economical than multiple card issuance.
- Tightly integrates background investigation process into HSPD-12.
- No card re-issuance required if any or all agency relationships are terminated.
- Closely maps real problems to solutions, thereby minimizing design obstacles.
- No longer can use as a badge or flash pass showing access privileges. It must be read electronically and can be checked against a revocation list at same time.

Disadvantages:

- Requires modification of FIPS-201-1 as currently written.
- Raises potentially complex control and billing issues.
- Pricing model may discourage agency funding for individuals with multiple agency relationships.
- Card can no longer be used as a visual badge or flash pass to convey access privileges (e.g., in a hostile environment to electronic verification)

The Need for Federation

In traditional physical and logical access systems, the scope of user identity and access management (IAM) was limited to an application or point solution. Each application managed a stovepipe view of a user's identity, credentials, authentication, authorization, and associated attributes. With the introduction of Kerberos, the scope of identity and access control expanded to include operating unit or possibly enterprise scope. With the combined introduction of HSPD-12 and SAML 2.0, it is now practical to scope identity, credential issuance and management, authentication, authorization and attribute management across multiple enterprises (credential or identity providers - IdPs) to the extent they are willing and able to agree upon attribute definitions and authentication procedures, and mutually support the means to exchange credentials.

Organizations of all types and sizes typically manage a hybrid solution of authentication domains and stand-alone systems where users handle multiple credentials for resource access. Even the most progressive organizations using single sign-on generally manage IAM only within the scope of their own enterprise. There is often a tremendous cost, much of it hidden, in verifying identity, and in managing credential issuance, support, authentication and authorization services, and user attributes. Further, attack vectors are inevitably exposed in each IAM instance. It is commonly argued that distributed IAM is inherently more secure since a successful attack in one sector is prevented from metastasizing into other sectors. Without a doubt, metastasis mitigation is a critical element of security design but distributed IAM as currently practiced is not the answer, it's the root problem.

Currently, users maintain multiple sets of unsynchronized username/password pairs for authentication to discrete security domains. These credentials frequently require password changes and with the recent adoption of the Federal Desktop Core Configuration (FDCC), passwords must be at least 12 characters and change every 60 days. Users typically keep these difficult-to-remember passwords on paper near their workstations or in clear text files on their PCs, both of which are vulnerable to compromise. Self-synchronizing passwords for simplification further obviates the argument for distributed IAM. A compromise of user credentials in the weakest system is quickly metastasized into the strongest system.

The notion of a user's identity in one security domain is wholly unrelated to any notion of that user's identity in any other security domain. Subsequently, organizations waste resources on duplication of effort. Changes in user status such as termination or material change in the job are not reflected without specific updates. In every domain, the user's identity is represented, often resulting in failure to properly and promptly eliminate user access to protected systems and data. Further, unsavory users are able to manipulate association attributes without detection since each system has an isolated world-view.

While HSPD-12 is not perfect, it is an excellent start that holds the promise to radically improve the security posture of the federal government. The scheduled deployment of HSPD-12 must be aggressive to deliver on its promise. To be effective, HSPD-12 requires a trustworthy and standardized identity foundation and the correction of myriad deficiencies, inconsistencies, and conflicts of current HR and identity management practices across agencies. It also requires integration with stove-piped logical and physical access systems.

The promise to improve the security posture rests on the use of two-factor (what you have/what you know) smartcard authentication, and the widespread deployment of a common identity and authentication and access control infrastructure. The Personal Identity Verification (PIV) smartcard provides a *de facto* standard that is moving the market beyond vendor-specific solutions, and is now being adopted by state governments and the emergency responder community.

The combination of these factors opens the door to tremendous opportunity for federal, state, tribal, and municipal governments, commercial entities, and private citizens by reducing the friction and security vulnerabilities inherent in working beyond the boundaries of individual enterprises or security domains.

How Federation Could Work

The Internet2 (or MACE Shibboleth) Initiative is a not-for-profit advanced networking consortium comprising more than 200 U.S. universities in cooperation with 70 leading corporations, 45 government agencies, laboratories and other institutions of higher learning as well as over 50 international partner organizations. In 2000, the Internet2 Middleware Architecture Committee for Education (MACE) began work on a state-of-the-art federation-enabling software platform (Shibboleth) for universities, partners, and government agencies. That work greatly influenced the development of SAML 2.0, in that the Shibboleth project principals were and are actively involved in its development. This helped create a trust fabric that allows organizations to trust other organizations to assert user authentication, describe user relationships to the asserting organizations through attributes, and in some circumstances, describe authorization privileges. The Shibboleth project led to the creation of the InCommon Federation as a common framework for collaborative trust in support of the U.S. research and education (R&E) community. This provides a working example of advanced federation concepts that could be extended as a proven mechanism for federating identity, authentication, authorization, and attribute management in a national IAM framework that includes federal government agencies, state, tribal, and municipal governments, and industry partners.

The SAML-based federation consists of Identity Providers (IdP), Service Providers (SP) and users. Identity Providers manage user identities and provide authentication and authorization services, and assert attributes about users in a secure, trusted, and flexible manner. Service Providers deliver and manage Internet-based resources to users by making access control decisions based upon bilateral agreements and the receipt of the required attributes about the requesting user or system. When a user requests access to a SP resource, they are redirected to their IdP which authenticates the user and returns a SAML assertion digitally signed by the IdP and thus verifiably secure and trustworthy. In the Shibboleth model, the IdP assertion is unusual in that it has the optional ability to utilize privacy protection attributes that do not necessarily include user identity. In this case, the IdP asserts (1) the user authenticated his identity to the IdP, and (2) the user has an active relationship with the IdP and has certain attributes which would qualify the user for access to the protected resource.

It is important to note that the holder of the resource (SP) always retains control over access control decisions. This control is not surrendered to external entities by participation in a federated access model. If the attributes received are deemed by the resource holder to be insufficient to adequately identify the requesting user and thus grant access, the organization hosting the SP can work with the organization hosting the IdP to release the required additional attributes. The IdP can agree to supply these additional attributes or not, according to local

policy and bilateral agreements between the security domains or agencies. Ultimately, if the supplied attributes don't satisfy the SP's requirements, access would be denied. There is a continuum of identity, ranging from very basic affiliation (user is an employee of USDA) or presence (user is physically located at a particular kiosk) all the way to detailed identifying information. The Shibboleth model is flexible enough to support the exchange of whatever level of identifying information is appropriate to the task and security policies at hand.

While the Shibboleth model does not currently support individual real-time management of attribute release, this is in the project roadmap for future inclusion. Currently, this is handled by administrators.

As an example, both University of Colorado (CU) and University of Washington (UW) are InCommon federation members. Let's assume CU manages a climate modeling application that it exposes to authorized users within the atmospheric sciences research community. CU is an SP in this instance. Dr. John Smith is a research scientist with the Atmospheric Sciences Department at UW. When Dr. Smith attempts to access the climate modeling application at CU, the SP service redirects him to the UW IdP service, which authenticates him and searches its identity store to determine that Dr. Smith is associated with the UW Atmospheric Sciences Department. The UW IdP creates a SAML assertion that obfuscates Dr. Smith's identity but affirms that the user bearing the SAML assertion has been authenticated and is associated with the UW Atmospheric Sciences Department. The UW IdP digitally signs the assertion, provides it to Dr. Smith's Internet browser, and redirects him back to his original target. If the CU SP does not require Dr. Smith's identity and considers UW Atmospheric Sciences to be within its authorized user community, Dr. Smith is granted access to the target application. If instead, the CU SP requires knowing the user's identity, it returns a message to Dr. Smith indicating this requirement. If Dr. Smith's institution agrees to provide his identity for this scenario, it accepts the request and supplies the required information. The request is returned to the UW IdP which returns a new SAML assertion that includes Dr. Smith's identity and he again requests and, this time, is granted access. If he declines the request to provide his identity, his request for access is denied.

The value of identity obfuscation is often not immediately obvious to those used to the traditional stovepipe IAM model. Upon consideration, many, if not most, applications need to confirm only that the user is a member of a given community and/or has a particular role within that community. Further, there are a number of law enforcement and national security application communities where identity obfuscation is quite beneficial. For those applications where user identity is required, the Shibboleth model provides a unique and compelling solution. For the majority of applications, identity obfuscation provides appropriate privacy protection to users. Access data and Personally Identifiable Information (PII) cannot be stolen in transit nor does it reside on remote systems since it's not transmitted over the network. In the event of suspicious user activity, the SP has an audited assertion which can be referenced to an audited IdP authentication event. In other words, end-to-end audit trails are available and can be accessed

when there is a compelling reason to do so without unnecessarily trampling on users' expectations to privacy.

We can further extend this example to show four additional important concepts available in the federated model:

1. Reciprocity - UW also may have a climate application and a climate researcher at CU needs access. UW would then be the SP and CU would provide IdP services. In short, all participating entities in the federation can offer Identity Provider and/or Service Provider services.
2. Attribute Aggregation – Although Attribute Aggregation is not currently a supported feature in the Shibboleth architecture, its need is understood and it is on the Initiative roadmap. Let's assume that the CU climate application user community membership requires an association with cooperating university atmospheric science program and postdoctoral work at the National Center for Atmospheric Research (NCAR). UW, in this case, provides the IdM service with attributes regarding Dr. Smith's relationship with UW, but cannot be authoritative for any attribute describing Dr. Smith's relationship with NCAR. Instead, NCAR must now be part of the Federation and must provide a specialized service by providing association attributes through a Linking Service (LS) to the UW IdP. With Attribute Aggregation, the UW IdP assertion will now encapsulate NCAR's assertion of association attributes along with its original payload.
3. Web-Based Management Tools – Internet2/MACE Signet and Grouper software toolkits provide open source web-based tools for managing user authorization (aka privilege management) and group management respectively.
4. Web-Based Collaboration Platform – The feature-rich collaboration platform being developed by Internet2/MACE, known as COmanage, allows federation partners to build topical collaborative information-sharing communities on-demand. Program and project managers can quickly instantiate a collaborative environment, assign access to particular federated users, designate user permissions, and support bi-directional communication. Sites can also be quickly abolished as needed with content archival features to optimize resource allocation.

In a traditional approach, CU would have to manage identities for every individual in every application community for which it hosted services. The CU climate application would contain a user store that holds Dr. Smith's identity. Further, CU would have to issue Dr. Smith an authentication credential and provide an authentication service and finally manage information that describes Dr. Smith's association with UW and his level of authorized access. When Dr. Smith leaves UW, CU must somehow become aware of that change or Dr. Smith will retain access rights even though he no longer retains the seminal relationship. If we momentarily set aside the gross inefficiencies and duplication of effort related to managing IAM in a stovepipe fashion, we see the crux of the fundamental security flaw: application owners and managers of application communities are authoritative only for defining the business logic that maps user's association attributes into application access roles or groups, but are not authoritative for

managing user associations with their respective home security domains. Put simply, applications are consumers, not providers, of association attributes and are often the last to know of changes to a user's association status. In most cases, this is a key element in making an informed access decision. It is important to understand, as described above, that participation in a federation does not obviate access control decisions by resource owners, but rather eliminates the inefficiencies of distributed identity management. Resource owners/managers continue to maintain exclusive control of access privileges to their assets but now have the capability to leverage authoritative information to optimally implement business logic.

Participation in a national federation model would leverage the concepts illustrated that support a common approach built on top of the SAML 2.0 standard. It is not necessary to use Shibboleth per se nor does this paper recommend that specific solution. Rather, the federation concepts including Identity Providers, Service Providers, digitally signed attribute assertion and aggregation, privacy protection capabilities where appropriate, and collaboration systems built upon this flexible infrastructure provide a crucial foundation to build upon.

While the specific technical details of implementation of a national federation are beyond the scope of this discussion, the recommendation of how and where to begin is at the core. A federation is essentially a common architecture and framework of operating agreements and agreed syntax for attribute assertions. The federal government can provide a critical role in facilitating architectural conformity, process and procedure standardization, an operating agreement framework, and an oversight role to ensure system integrity in Identity Provider and Service Provider certification during the embryonic phase of the Federation lifecycle. The InCommon Federation has made significant progress, much of which may be leveraged in a government federation. Also notable is the fact that several government agencies and research labs have seen the value proposition in supporting their interactions with the U.S. higher-education community, and have joined or are in the process of joining the InCommon Federation. They include as of Sept. 1, 2008 the Energy Sciences Network (ESNet), Lawrence Berkeley National Laboratory, Moss Landing Marine Laboratories, National Institutes of Health (NIH), and TeraGrid. Shibboleth-based federations similar in scope and purpose to the InCommon Federation that support research and education are rolling out around the world, and most are connected to and supported by national governments. There are also commercial SAML-based federated identity projects underway around the world supporting a growing number of industries. The Liberty Alliance Project is the center of this activity[1]

[1] The InCommon Federation current participant list is available at http://www.incommonfederation.org/participants/. A list of Shibboleth participants is maintained at https://spaces.internet2.edu/display/SHIB/ShibbolethFederations. For the Liberty Alliance, see http://www.projectliberty.org/liberty/membership/current_members/ and http://www.projectliberty.org/liberty/about/.

In the same way that data networks can interconnect or "peer," work is underway to establish a foundation for the peering of federations to prevent an organization or agency from having to join multiple federations to interact with all of its business partners.

Just as HSPD-12 facilitated evolution in both the fingerprint biometrics and smartcard industries from competing technologies to competing solutions by establishing a de facto standard, a national federation initiative can facilitate evolution of interoperable federated identity and access management solutions. The key to success lies in creating a sizeable market opportunity, and such an opportunity is readily available.

Glossary

Authentication - The act of establishing or confirming that someone is who they claim to be. In an information technology sense this is confirming that someone is authentic typically by validating their credentials.

Authorization - A process of controlling access to information or resources only to those specifically permitted to use them.

Credential - A defined collection of attributes that are asserted to meet the level required to validate the user and authenticate them.

E-Authentication - A federal government secure on-line access authentication initiative, see http://www.cio.gov/eauthentication/index.cfm for more information.

Electronic Identity - Digital identity, the representation of identity in terms of digital information or online identity.

Entitlement - Permission to access a resource. This may be based on a role, rules, or attributes.

Federated identity - Identity management with defined trust relations between independent principals.

Identity fraud (Identity Theft) - The deliberate appropriation of someone's identity without gaining that person's permission for criminal purposes.

Laws of identity – Concepts that define a unifying identity meta-system for online identity management.

Liberty Alliance — A consortium promoting federated identity management.

Security Assertion Markup Language (SAML) - SAML is a standard for exchanging XML-based authentication and authorization assertions between identity providers and service providers (assertion consumers).

Shibboleth (Internet2) - Shibboleth is an open source standards compliant federating software platform. Essentially it is a transport mechanism for digitally signed SAML assertions.

Acknowledgements

Writing Team
John Bird, BT Conferencing
Mark Cohn, Unisys
Joe Cuddihy, McConnell International
Bill Harrod, CA
Vivek Kumar, Softchoice Corporation
Dean Lindstrom, Cyberstorm
Kovelevenni Ramaswamy, QSSI

Transition Study Group Leadership
Mark Forman (Chair), KPMG
Roger Baker (Vice Chair)
Mary Ellen Condon, Booz Allen Hamilton
Judy Douglas, EDS – an HP Company
Dee Lee, Compusearch
Brian Lorenz, Bearing Point
Leslie Steele, InterImage

ACT-IAC Staff
Ken Allen
Sarah Lindenau