Federated Identity:

Are We There Yet?

Prepared by the NECCC Identity Authentication Federation XBI Work Group

NATIONAL ELECTRONIC COMMERCE COORDINATING COUNCIL

NECCC
2401 Regency Road
Suite 302
Lexington, KY 40503
(859) 276-1147
www.ec3.org

Made in the United States of America.

NECCC is a consortium of national organizations and public and private sector leaders identifying best practices for strategic change within government.

Alliance partners are:

National Association of State Auditors, Comptrollers and Treasurers
National Association of Secretaries of State
National Institute of Governmental Purchasing

NECCC also works in partnership with these affiliate organizations:

Association of Government Accountants
Information Technology Association of America
National Automated Clearing House Association
National Association of Government Archives and Records Administrators
National Association of State Treasurers

Forward

The concept of federation, while extremely ancient, always requires cutting edge thinking when applied to any particular set of people, interactions and surrounding circumstances. Examples of federations from other contexts and through history can help to form a framework and place the relevant foundational issues in sharper relief.

One can see the binding together of Greek city states in the golden age as a type of federation. In that case, however, the federation was very loose and for the main purpose of common defense. An even closer historical example would be the Native American League of the Iroquois. This federation, comprised five nations and was governed based upon consensus, a retained right for each nation to act independently provided it did not harm another nation of the federation, and a hereditary and well as a merit based set of representatives to the central government. No two federations are alike - each depending for its precise form, governance, authority and rules upon the unique circumstances and interests involved. This is exactly the case with so-called identity federations.

Among nation states, when individual entities retain the right of secession, the term "confederacy" is typically used, while "federation" describes a much stronger role for the national government. However, for purposes of this paper, we use the term "federation" generically, to describe the relationship of partnering entities. Anytime a variety of entities come together for a common purpose, while retaining their individual autonomy to a significant degree, then in the broadest sense it can be said that federation has occurred.

There are certain similarities in the core issues that arise, whether in the context of a multi-corporate joint venture to co-market a set of products, or a combining of former British colonies into the American nation through the Articles of Confederation. One key issue is balance between maintaining individual decision prerogatives against the need for joint action and common positions. Another way to look at this aspect is as a balance between control by a central authority versus control at lower levels. Beyond operational control, however, is the basic question of authority to decide. In the case of a public entity the concept is "sovereignty," while with private institutions we talk about "ownership".

The way this question plays out in military federated actions has to do with the command structure. In WWII, for example, perhaps the most important strategic management decision that was made was to insist on a unified command structure. This meant that the allies, led by the United States and Great Britain, created a combined high level military decision making structure, headed by a single Supreme Commander. The alternative was to maintain a coordinated but separate set of command structures which would lead and control the forces of each country's armed forces. The gaps, duplication, conflicts and confusion that follows such fractured command structures was unacceptable, given the stakes. However, in peace time, none of the allied countries would be willing to cede so much authority to command their troops to a foreign officer corp and political leadership. Rather, countries seek to maintain authority over their own forces.

Similarly, with federations in the technology enabled business context, the individual entities comprising any given federation will usually seek to retain maximum governance and control over their own resources, users and systems. There will be a desire to interoperate, but not necessarily to subordinate processes to a common set of business, policy and technical systems. But when the stakes are high enough, much deeper partnerships will result, just as happened with the Greek city states who sought to repel invading armies by forming a coordinated defense.

Trust, it is said in this paper, is a key component. It is proportional to the stakes. And the stakes are based on mission, goals and objectives of the participating entities. Trust is not a component that can be added to an architecture. Rather, it is the subjective result of trustworthy systems - systems of business, law, technology and policy. Basically, systems comprised by people using tools, such as the Internet.

For a system to be deemed trustworthy, the safeguards, protections and integrity of each of the sub-systems involved must be proportional to the value at risk. In other words, trust is proportional to the stakes, and depends on how well the stakes are protected and the value is attained. In a federation, this will depend on multiple entities working together, but not necessarily always doing the same the things the same way. In fact, in many documented cases, security is better when interrelated systems use different platforms, applications and security approaches, thus creating a robust, evolving system that is hard to understand by outsiders or defeat by a central attack.

An identity federation that exists to provide a small convenience for the participants (such as a slight improvement of the log on experience of their customers) may not be of compelling enough value to justify much if any real ceding of authority, control or other resources to the common enterprise. However, a deep integration of entities (such as with some tightly integrated supply chains, critically important joint ventures, etc) may warrant greater investment in a new layer of governance, management, business process, personnel, legal, technical, marketing and other new pooled resources necessary for the success of the initiative.

Just as with the federation out of history, people leading entities today that wish to federate for the purpose of using federated identity solutions stand to benefit by joint action on common issues, but will need to meaningfully address questions of governance, risk allocation, continuing autonomy of partners to make decisions and to use different approaches, and the degree to which the overhead and sacrifice of authority are justified by the underlying business or public purposes at stake. Early indications are that in many arenas, federated identity management is well worth the effort, and this paper will explore many examples where it makes sense, and describe precisely how they work.

Daniel J. Greenwood, Lecturer, MIT

Cambridge, Massachusetts, October 27, 2005

Identity Federation

Since the invention of the first computer we have witnessed a separation or “decoupling” of information technology components, infrastructure and associated resources: input separated from processing, data manipulation separated from format or output, communication separated from storage. Separating the various components of IT infrastructure has enabled the explosive growth of and uses of IT. This separation has allowed the mind-boggling increases in speed, processing and storage. It has helped to provide an incredible flexibility of system design and function while dramatically reducing unit costs.

The ever-present twin desires of reducing costs and improving functions have led to further distribution of components, specialization of skills and sharing of information resources. Today the machines, people, information and services that form an information infrastructure may be spread around the globe to achieve the desired combination of skills, cost, availability or other system requirements. These resources may couple and uncouple in various combinations to meet changing conditions and demands.

Until very recently, the only option for the owner/operator of an application was to create and maintain the identity management process. Each application incorporated a means of identifying, proofing, provisioning, authenticating, securing, managing and otherwise maintaining the base of application users. For example a large department, say Human Services, performed these same processes on the same people many times. Multiply this situation across, federal, state and local governments, the many departments at each level, the public and private sectors. An individual registered and provided personal information dozens of times. Government still collects, maintains and spends taxpayer dollars dozens of times to recognize and provide access to a single individual.

Former White House adviser urges high standards for ID cards

Source: Government Computer News
Date Written: 2005-09-15
Date Collected: 2005-09-16

Richard Clarke, former cyber security and counterterrorism advisor to Presidents Bill Clinton and George W. Bush, speaking at a conference hosted by the Center for Strategic and International Studies, called for the federal government to establish open and transparent standards for a federated identity card system. Federated identity creates a network of trusted certificate authorities; one service that trusts another authority will accept credentials issued by that authority, allowing users to have a single identity across multiple systems. Rather than creating a national identity card, federated identity would allow the government to use cards issued by private entities for authentication. Such a system should have third-party audits of companies that issue credentials. An independent civil liberties board could oversee federated identity use to protect citizen's privacy.

Similar forces to those that have acted on other parts of the IT infrastructure have come to bear on identity, ID management and related access functions. The emergence of distributed Web services

enabling ever larger-scale e-commerce and e-government applications that cross a wide array of traditional boundaries combined with an increased awareness of identity management and network security issues has given rise to a new paradigm in identity authentication – that of identity federations. Identity federations provide for the relatively transparent movement of a user between Web sites and applications participating within a given federated environment through the use of commonly accepted identity credentials.

What is an Identity Federation?

An identity federation is an organization within which participants act according to a set of agreements, rules and/or specifications and the identity functions and resources are shared among participants. Generally, there are three functional roles, a set of operating rules and a technical infrastructure, although many variations and subdivisions are possible.

The first role is that of consumer of identity information or Relying Party (RP). The consumer is an application or system (and/or its owner) that is configured to accept credentials issued by participants in a particular federation. The second role is that of identity information provider. This is the system (and/or its owner) that provides the identity information. This identity information is usually expressed as a set of credentials which might be a username and password set, a PIN number, a PKI credential or public, private key set, a set of personal information attributes, an electronically readable card, a thumbprint, a voiceprint or other variations.

Many federations have adopted, for the role of ID information provider, the second role, the concept of Credential Service Provider (CSP) to identify the component(s) and its owner(s) that perform(s) an array of identity related functions. CSPs are entities acknowledged, approved or certified by a federation to perform identity validation, provisioning and/or authentication services, in other words the identity information consumed by those in the first role.

The third role is that of the user, the individuals, whose identities are proofed, to whom credentials are issued and who use the systems that grant access based upon the work completed by the CSPs.

The guiding principles and specifications that direct the provision and consumption of the identity information are a set of operating rules. These can be a short set of suggestions or a lengthy set of documented requirements covering all or a part of the overall operations of the federation. Some topics covered may be enrollment of users, payments, fees, liability, eligibility for participation, approval or certification of participants or systems, duties and responsibilities among a wide range of other possibilities.

The technical infrastructure, including documentation, policy and IT components, stores, manages and transports the interactions of participants. There are many options for the components of the technical infrastructure, but special focus should be paid to security and reliability to meet the requirements of the transactions to be facilitated by the federation.

Variations on a Theme

All identity federations have some general aspects in common, for instance the trusting of a set of credentials by participating organizations (POs). There are wide variations in major functions' design and implementation. Some federations start with a relatively strong central management that holds significant power delegated or agreed to by participants. These tend to create and enforce a relatively strong set of rules and procedures directing the behavior of POs and users. (Included in the documents and links in the Appendix are examples of operating rules.) Other federations are loose and have little central management, choosing instead to leave to individual or a group of POs the duties of coordinating activities. POs may self-police to set and observe rules, agreements, processes, etc. In some instances there may be an organized effort to create and share components and technical infrastructure.

The Pharmaceutical Research and Manufacturers of America (PhRMA) "represents the country's leading pharmaceutical research and biotechnology companies, which are devoted to inventing medicines that allow patients to live longer, healthier, and more productive lives"

Eight Pharmaceutical Leaders Initiate New Company to Manage and Promote Digital Identity Assurance Standard Across the Biopharmaceutical Industry

February 09, 2005

Washington, D.C. — Eight global pharmaceutical organizations, including AstraZeneca, Bristol-Myers Squibb, GlaxoSmithKline, Johnson & Johnson, Merck, Pfizer Inc., Procter & Gamble and Sanofi-Aventis have come together as the founding members to form SAFE–BioPharma, LLC, a not-for-profit limited liability company, to support widespread adoption of the global digital identity standard, Secure Access for Everyone - SAFE. SAFE-BioPharma, LLC will establish and maintain the standards and operating rules for the provisioning and management of digital credentials that will be used in electronic clinical research records between the biopharmaceutical industry and government regulatory agencies globally. As an industry initiative, SAFE-BioPharma, LLC, will continue to encourage other biopharmaceutical companies of all sizes to join the organization and leverage the standard. Amgen Inc. has also agreed to be a member of the newly incorporated company.

The SAFE digital credential standard was developed to simplify business partner interactions across the biopharmaceutical industry through a policy and technology framework for digital signature and authentication. This allows the SAFE community to eliminate the need for multiple identity credentials when interacting with each other and business partners.

The SAFE coalition has been working together for more than a year to develop the policies, procedures and technical specifications that form the SAFE standard. To ensure the standard meets global regulatory requirements, SAFE-BioPharma, LLC has collaborated with the Food & Drug Administration (FDA), the European Agency for the Evaluation of Medicinal Products (EMEA), the European Federation of Pharmaceutical Industries and Associations (EFPIA), and Pharmaceutical Research and Manufacturers of America (PhRMA).

The initial version of the SAFE standard was completed in June 2004. SAFE sponsors are now implementing the digital credential standard across a wide variety of applications to securely authenticate business partners to review, edit and digitally sign business documents.

The not-for-profit limited liability company, SAFE-BioPharma, LLC is expected to be in operation by March 2005. SAFE-BioPharma, LLC will:

- Manage and maintain the SAFE standard
- Provide accreditation and certification programs to ensure that SAFE-enabled applications and identity credentials are commercially available
- Establish best practices to simplify the implementation and use of the SAFE standard by biopharmaceutical companies, regulators and industry business partners
- Operating the SAFE-BioPharma Bridge to provide seamless interoperability of credentials issued by Accredited SAFE Issuers into the SAFE environment

(continued on page 7)

according to the organization's Web site. PhRMA appears to be a strong organization with significant support and involvement of members. Responding to member companies' requirements to address growing costs and complexity of corporate functions, compliance and reporting to government organizations around the world, PHRMA undertook to establish SAFE-BioPharma, LLC (www.safe-biopharma.org). Many of the processes and filings mandated for compliance or otherwise needed by participating organizations are carried out through paper-based procedures resulting in tens or hundreds of thousands of pages of documents being created and filed with government organizations around the globe. Reducing costs, complexity, and security of compliance requirements was a significant driving force and expected benefit of implementing SAFE.

SAFE, among other things, is an identity federation with relatively strong central organization, strong operating rules and detailed prescriptions for processes and technology infrastructure. The transactions facilitated by SAFE can be very high value to the participating individuals and organizations. SAFE was designed and built from inception to meet the requirements of a high level of security and control of the transactions conducted and information collected or transmitted.

Another approach to identity federation is exhibited by developers and participants of Shibboleth-based federations. The development of the Shibboleth software was undertaken as a project of the Internet2 Middleware Initiative (middleware.internet2.edu).

> Middleware, or 'glue,' is a layer of software between the network and the applications. This software provides services such as identification, authentication, authorization, directories, and security. The Internet2 Middleware Initiative (I2-MI) promotes standardization and interoperability and is working toward the deployment of core middleware services at Internet2 universities.[1]
>
> Shibboleth® Software was developed by Internet2 to enable the sharing of Web resources that are subject to access controls such as user IDs and passwords. Shibboleth leverages institutional sign-on and directory systems to work among organizations by locally authenticating users and then passing information about them to the resource site to enable that site to make an informed authorization decision. The Shibboleth architecture protects privacy by letting institutions and individuals set policies that control what information about a user can be released to each destination. For more information on Shibboleth please visit http://shibboleth.internet2.edu/shib-uses.html.[2]

[1] www.Internet2.edu Web site: http://middleware.internet2.edu.

[2] www.internet2.org website: http://www.incommonfederation.org/glossary.cfm#Shibboleth®.

The Shibboleth federations use Shibboleth software as the core technology for federating identity related functions. These participants have produced an excellent body of supporting documentation and produced tremendous innovations in the operating of federations. Take, for example, the InQueue/InCommon Federations for higher education institutions and sponsored partners.

One such innovation is the creation of two federations, one to serve as a learning and transitional "sandbox" to the other.

> The InQueue Federation (http://inqueue.internet2.edu), operated by Internet2, is designed for organizations that are becoming familiar with the Shibboleth software package and the federated trust model. Participating in InQueue permits an organization to learn about the Shibboleth software via the experience of multi-party federated access, while integrating its services into the organization's procedures and policies. It is also available as a temporary alternative to sites for which no suitable production-level federation exists.
>
> The InQueue federation is specifically not intended to support production-level end-user access to protected resources. Organizations providing services are strongly discouraged from making sensitive or valuable resources available via the federation. Specifically, certificate authorities with no level of assurance may be used to issue certificates to participating sites, and therefore none of the interactions can be trusted.[3]

"Over the past year, the SAFE coalition sponsors have provided the resources and leadership to develop the standard needed to solve a common business problem," said Gary Secrest, director of World Wide Information Security at Johnson & Johnson and chairman of the SAFE initiative. "With the establishment of SAFE-BioPharma, LLC, the industry can begin commercial implementations and use of the standard."

"Our members are already implementing the SAFE digital credential standard for authentication and digital signing to help streamline clinical trials processes. As an industry, we can now simplify our business partner interactions and increase our electronic submissions to the regulatory agencies globally. SAFE-BioPharma, LLC provides reduced costs through a shared cost model, and sponsors benefit from the shared experience of developing and implementing the standard," Secrest continued.

"The formation of SAFE-BioPharma, LLC is a powerful demonstration of how the industry and global regulators can work together toward a common set of goals that will benefit the entire process of developing new drugs," said Alan Goldhammer, an associate vice president for Science and Regulatory Affairs at PhRMA. "SAFE has broad applicability that can simplify the life of the doctor in a clinical trial. With the ever-increasing cost of drug development, it is essential that we rally as an industry around standards such as SAFE to ensure electronic health information is reliably protected."

About The SAFE Standard

The SAFE (Secure Access for Everyone) coalition was formed in 2003 to develop SAFE as a biopharmaceutical industry trust standard. The mission of SAFE is to deliver unique electronic identity credentials for legally enforceable and regulatory compliant electronic signatures across the global biopharmaceutical environment. The SAFE standard is intended for business-to-business, and business-to-regulator transactions. SAFE-BioPharma, LLC offers a variety of membership options for organizations seeking to join or leverage the SAFE standard.

For more information, visit www.safe-biopharma.org

For more information, contact:
Jill Ryan or Bree ClidenceStauch

Vetromile & Mitchell

401-438-0614

jill.ryan@svmpr.com or bree.clidence@svmpr.com*

*PHRMA website--
http://www.phrma.org/mediaroom/press/releases/09.02.2005.1127.cfm

Institutions, when comfortable with the Shibboleth software and federation participation, can apply for membership and if qualified join InCommon. "The InCommon federation supports user access to protected resources by allowing organizations to make access decisions based on the user's home institution exchanging agreed upon traits with the resource provider."[4] InCommon is a robust production federation. The Shibboleth software is available for

[3] http://inqueue.internet2.edu/.
[4] http://www.incommonfederation.org/.

download from the Shibboleth Web site (http://shibboleth.internet2.edu/release/shib-latest.html#Download) along with a wide array of supporting code and documentation.

The contrast between the SAFE and InCommon federations can be informative. SAFE is a "tight" federation in which interactions and processes are highly circumscribed. The operating rules require strong user identification, strong credentials, and robust related processes to support the anticipated high-value interactions of participants. A substantial amount of effort is spent in the upfront user registration and provisioning process. The CSP function is a robust process which at its conclusion enables the CSP to assert during a transaction that "we know who this person is and you should trust them for that reason." InCommon is a much "looser" federation in which participating organizations have much more latitude in performing federation related functions. The institutions may be issued strong credentials but for the participants this is not necessarily the case. The transaction "conversation" that occurs in InCommon is currently along the following lines (although this is evolving rapidly). "This person is on our network and we know some things about this user, and we will facilitate a conversation between the user and you to ask questions and receive responses should the user choose to give them, until you are satisfied that you know enough information to make a decision on allowing them access to a protected resource." SAFE participants invest a lot of effort into securing the system through robust processes such as validating the identity of users and issuing strong credentials. InCommon focuses significantly on providing user privacy and control of personal information. InCommon, through creation and use of InQueue, provides a natural, easy learning and transition environment to protect participants from costly and damaging production environment mistakes.

> The Liberty Alliance Project (www.projectliberty.org/index.php) is an alliance of more than 150 companies, nonprofit and government organizations from around the globe. The consortium is committed to developing an open standard for federated network identity that supports all current and emerging network devices. Federated identity offers businesses, governments, employees, and consumers a more convenient and secure way to control identity information in today's digital economy, and is a key component in driving the use of e-commerce and personalized data services, as well as Web-based services. Membership is open to all commercial and noncommercial organizations.[5]

The Liberty Alliance Project develops specifications through the collaboration of five expert groups that are coordinated and driven by the Liberty Alliance Management Board.

- **Technology**: The Technology Expert Group is in charge of creating the Liberty specifications and driving the development of sample implementation and interoperability tests.
- **Public Policy**: The Public Policy Expert Group drives dialogue with government and non-government groups concerned with the many issues pertaining to identity, and data management and ensures that the Liberty specifications enable compliance with pertinent laws and regulations.

[5] http://www.projectliberty.org/about/index.php.

- **Business and Marketing**: The Business and Marketing Expert Group is tasked with identifying market requirements and driving adoption of the Liberty specifications. It is also the central point for all the Alliance's communications, and drives the creation of Liberty's Business Guidelines.
- **Conformance**: The Conformance Expert Group defines and manages the process for validating vendor interoperability and manages the overall conformance testing program.
- **Services**: The Services Group defines and manages the process and development for creation of new identity service specifications.[6]

The Liberty Alliance is in many ways somewhere between InCommon and SAFE. The membership is open to a lot of organizations who wish to participate, but there are significant requirements for participating. Joining the Liberty Alliance is a relatively simple matter, but there is a membership fee. Membership instructions and a membership kit can be found at www.projectliberty.org/membership/become_member.php. Technology choices are varied but require compliance to an open-standard based specification. There is a significant body of documentation that has been developed by participants and a formal certification program for products utilizing Liberty specifications.

Each approach to federation has strengths and weaknesses. Most have grown well beyond their initial development phases. SAFE was developed to facilitate particular electronic business processes meant to lower costs of doing business for business related participants. Shibboleth is open-source middleware developed by Internet2 and serves identity management functions and a basis on which federations can be built. Liberty Alliance began as an open standard development to provide a competitive system in the market place. There is a significant amount of interaction between participants in various types of federations which is leading to some convergence of policies and processes and to the federation of federations. Federations are developing the methods of interaction under which users in one federation will be able to access resources of another federation. Despite beginning from different starting points federations tend so far to develop along fairly common pathways and arrive at a point at which participants recognize a value in communicating and working with other federations to extend the scope of benefits beyond the limits of any particular federation.

What are the Common Functions and Components of a Federation?

Identity federations are tending toward a handful of common components and functions. This may be due to inherent requirements of an organization of this type or it could be a result of this field being relatively new and practitioners few in number and relatively tightly woven into cooperative organizations or ventures. A great deal of the information concerning the development of federations is shared openly. There are, however, significant differences in the manner in which these are designed, implemented or

[6] http://www.projectliberty.org/activities/index.php.

function. The list of components and functions that follows is by no means comprehensive, but is representative of those required for most functioning identity federations.

Intake or Registration of Users

Intake or registration is the process, or start of one, in which the CSP becomes acquainted with the user. The user may provide and/or the CSP otherwise obtain personal identifying information about or known by the user. The information may be simply stored for later use or it may be compared to parallel information from internal or external sources to check its validity.

Many federations rely heavily on the intake or registration process to support a level of trust afforded to users. Generally, more stringent intake supports higher levels of trust and thus facilitation of more important or valuable transactions. Some federations collect user information without validation. Other federations, notably some of the Shibboleth-based federations use a hybrid approach, verifying some information and collecting other items for later use under control of the user. Some of this collection may occur at various times in support of particular transactions. Some federations, such as the E-Authentication Federation may include various methods to support different levels of trust and transactions of varying importance or value.

The starting point of participation in a federation for most users will be the intake process. Federations employ a variety of methods to accomplish this function. Some users may be automatically enrolled as part of another transaction or process, there may be a registration process conducted independently of other processes or it may be integrated into an initial transaction. This process may be completed in "real-time" during a transaction, it may be discontinuous, started at one point and completed later, or it may be a lengthy and intense process of acquiring and checking data about the user. The intake process may be conducted online or by phone or may require an in-person meeting with a registration agent or authority.

> **One observation about federations, registration processes, levels of trust and value of the transactions facilitated is important to note. It may be tempting to employ or join a federation that employs a relatively easy or relaxed intake process in order to minimize user impact or resistance. However, federations tend to experience rapidly escalating requirements requested or imposed by participants to support ever higher value transactions. As participants come to understand the value of the federation structure there is a strong tendency to want to do more with it. It is difficult and expensive to impose increased identity validation requirements and stronger security processes on existing users. Prospective participants in federations should expect that the value of transactions desired to be conducted by users will increase, often dramatically, in a short time frame and plan to meet such demands.*

Identity Management

There are a number of functions that can be grouped under the title of identity management (IDM) to be performed in the operation of a federation that will require a combination of technology, policy and process. These generally include the information about participant organizations and individual users, the ways in which that information is shared between CSPs and consumers or "assertions" about the identity of a user. An assertion states, in essence, that a CSP has collected and/or verified information about a user's identity according to federation requirements, then at the time of a transaction has authenticated or verified the credentials submitted by the user and now attests to the identity of the user. They include the management of what users are allowed to do or see within the systems accessed through the federation.

Performing these IDM functions may require hardware and software to operate a directory or directories of users, communication of attributes or assertions according to standards or protocols, access controls, permissions, roles, provisioning and others. These IT systems may be centralized or distributed, but some components will be spread across all participating organizations. Each will need to have the ability to create and/or consume the information communicated across the federation.

Federations develop formal or informal rules or practices to govern these IDM functions. Federations may choose to strongly direct the IDM of members or leave it to participants' discretion. The E-Authentication Federation (www.cio.gov/eauthentication) (EAF) has and is creating policies that significantly control some IDM practices. One example would be in the handling of Personally Identifiable Information or PII. The U.S. government in the Privacy Act of 1974 (http://www.usdoj.gov/04foia/privstat.htm) and other legislation has created significant controls for federal government agency use of PII. EAF policy directs the actions of participants in the management of PII to meet related legal requirements. The Shibboleth-based technology facilitates significant individual participant organization control of policy and user control of information and the federations exhibit substantial variations in IDM policy.

The EAF operates a lab to test interoperability of IDM products to ensure that software from various vendors will communicate successfully with each other for the purposes of the federation. The lab publishes the "Approved E-Authentication Technology Provider List" (www.cio.gov/eauthentication/documents/ApprovedProviders.htm) for use by agency participants to use as an aid in choosing a technology vendor.

Trust

The concept of trust can be difficult to adequately define and may be almost impossible to quantify, but everyone has a sense of what it means. Can participants and users rely on the systems and practices of the federation? Will either be harmed by acting on that trust? Trust is the outcome as expressed and

experienced by participants and users of the interaction of all the components of a federation. Trust could be considered the “wealth” of a federation. The collective sense of trust by participants and users is the quantification of it. How much trust federation participants and users perceive is the sum of the value or wealth of a federation. Investing the resources of the federation and its participants appropriately, and building and operating the necessary systems, processes and security build the wealth of the federation. Should this trust, the wealth of the federation, be taken or lost the federation will be bankrupt and cease to function.

Security

If trust is the wealth of a federation then security is the vault, the guards at the doors are the rules about how to act and react to threats. The building of a federation creates a potentially high-value target for criminals and mischief makers. It adds layers and types of potential compromise as access is extended to new systems, people and organizations. Threats of compromise are not just greater in number and scope, they are different. In addition to IT security requirements with which an organization may be familiar, there may be new types of security requirements as networks open new access points or kinds of access and new users enter in new ways based upon relationships to an organization that are different than previously known. As such security must be a consistent, strong focus of the federation and all of its participants. Each participant of a federation relies to some greater or lesser extent on every other one.

Internet2 at http://security.internet2.edu/ describes its efforts and provides links to documents and presentations related to meeting evolving security requirements. The National Institute of Standards and Technology, NIST, produces a wide range of materials which can be found at http://csrc.nist.gov/. Some of the material of particular relevance for federations are 800-63: Electronic Authentication Guideline, Personal Identity Verification of Federal Employees/Contractors, Federal Information Processing Standards (FIPS) publication 201, and the Federal Information Security Management Act (FISMA) Implementation Project.

Risk Management

Participation in a federation brings exposure to new risks, which can be surprising and difficult to anticipate. As such significant attention should be focused to understand, anticipate and address these new risks. Some federations may create a unit to specifically address these risks with the ability to change federations’ rules and participants’ activities while others may leave risk management entirely to individual participating organizations. Several federations have created and published substantial materials on risk management. The EAF makes available a tool developed by the Software Engineering Institute at Carnegie Mellon University to help participants self-assess some categories of risk in order to

align their choice of assurance levels with their associated risk. At the Web page http://www.cio.gov/eauthentication/era.htm, the tool and guide are available for download.

Business or Operating Rules

Federations, being groups of organizations, create and maintain new relationships. The business or operating rules that define and guide these relationships can be formalized or not, simple or detailed, open or tightly circumscribed. Federations may elect a board to make decisions for the organization, hire staff to conduct federation activities or a committee of participants can direct federation activities. There may be control structures created or adopted from parent or participant organizations or newly developed to meet specific needs of the new organization.

Contracts or agreements between the federation and participants, among participants, and between participants and users vary widely (but seem to be converging as best practices develop) as federations develop to meet a variety of participant requirements.

As an example included in the appendix is a draft of the EAF business rules which are in the development process. This document covers many common facets of federation activities and functions such as the following:

- ***Participation***: Relying parties (consumers of ID information) and CSPs.
- ***Roles and obligations***: Those specific to the General Services Administration, the relying parties and CSPs and those shared by participants such as:
  - PKI policy governing participation.
  - Record keeping.
  - System security and reliability.
  - Policy and technology requirements.
  - End-user privacy.
- ***Enforcement***: Dispute resolution and recourse.
- ***Liability***.
- ***Rules amendment***-how rules can be changed.

Technology Infrastructure

The technology infrastructures (TIs) of the various federations have developed along a variety of paths generally exposing the some of the underlying reasons that led to their development. The Liberty Alliance TI resulted from a group of companies cooperating to produce an open standard cooperative development venture in which a number of potential competitors and partners could work together to

produce technology that, as long as built to the standard, should function together. The arrangement has allowed for vendors, customers and users to cooperate to better understand the needs of each and to meet a wide range of requirements while competing to provide innovative functions and features in products. Control structures have been created, a certification program (https://www.projectliberty.org/activities/testingprocedures.php) and Liberty Alliance Project Interoperability Trademark License Agreement (https://www.projectliberty.org/activities/conformance/LAP_Iop_TMLA_120503_final.pdf) to assure interoperability.

The Shibboleth TI was developed by a long-standing community experienced in open source development to meet the needs of participating organizations. This community expands and upgrades its suite of software to meet a wide variety of organizational functions. The software and support material is made available to participants for download at http://shibboleth.internet2.edu/ under a form of general public license, which does not cost the user, but does carry requirements. Participation in some of the Shibboleth federations may entail a fee for recovery of the costs of operating the organization.

The EAF TI (E-Authentication Technical Architecture) was developed on the basis of a handful of core concepts to meet the requirements of federation in the federal government.

> (T)he E-Authentication Program Management Office (PMO) decided to implement E-Authentication infrastructure as a federated architecture called the Authentication Service Component (ASC). The ASC leverages credentials from multiple credential providers through certifications, guidelines, standards adoption and policies. The ASC accommodates assertion-based authentication (i.e., authentication of PIN and Password credentials) and certificate-based authentication (i.e., Public Key Infrastructure (PKI) digital certificates) within the same environment. Over time, the ASC will support multiple schemes such as the Security Assertion Markup Language (SAML) and Liberty Alliance, and therefore is not built around a single scheme or commercial product. In this light, the ASC is more precisely defined as an architectural framework. The ASC is targeted for incorporation into the Federal Enterprise Architecture (FEA), as its government-wide authentication component.
>
> The technical approach presented in this document is aligned with Office of Management and Budget (OMB) M-04-04, which provides policy guidance for identity authentication. It is also aligned with National Institute for Standards and Technology (NIST) SP 800-63, which is the technical companion document to OMB M-04-04. While the ASC architecture addresses authenticating end users to applications, authorization privileges at the application are beyond the scope of the ASC architecture and this document.
>
> Core architectural requirements derived from the E-Authentication Strategic Plan are discussed, including high-level requirements (leverage credentials, single sign-on, privacy, and governance) and design goals (standards based, use of commercial off the shelf products, federation, durability, and flexibility). Key components (agency applications (AAs), credential services (CSs), end users, and the E-Authentication Portal) are defined and discussed, as well as session types within the framework (browser session, authentication session, and agency session). The technical approaches to assertion based authentication and certificate-based authentication are then discussed in separate sessions, recognizing the significant difference between them.
>
> The EAF in development of its TI has been supported strongly by substantial Federal resources from the majority of federal agencies and in particular NIST.[7]

[7] http://www.cio.gov/eauthentication/documents/TechApproach.pdf.

To Join or Not To Join, That is the Question: The Business Case for Federation

At first glance there is a strong business case for joining an identity federation. Spreading the costs of identity verification, provisioning and management should allow an organization to do more for its users for less cost. But, there are risks and new costs to be weighed in the calculation of net gain or loss resulting from federation participation. Making a decision on whether to join a federation should include but not be limited to consideration of various factors.

Generally, federations perform the same or similar functions. The process of deciding to join a particular federation should include consideration of the problem to be solved or the functions to be accomplished by participation and which federation "culture" is most compatible with that of the organization. Does a prospective participant require a lot of structure and detailed procedures or a lot of flexibility to determine the policy and technology employed? Does the organization need strong direction in establishing and operating technology? Or does the staff have skills, experience and comfort operating open source or public license software?

Benefits

Expected benefits of federation participation may include reduction of costs, increased functionality, improved IDM, improved user experiences (such as fewer usernames and passwords to remember) and others. A student or faculty member at a particular university could become a registered user in InCommon as a part of the process of registering for class or being employed at and receiving a credential from the university. The faculty member might be able to apply for research privileges at national parks. The student may be able to apply for student loans or grants and later manage the repayment using the university-issued credentials. A U.S. government employee may be eligible to use the EAF by receiving certain credentials issued by their employer. In the near future a member of the particular university above may be eligible to access the EAF as the federations work together to overcome policy and technology issues. Customers of participating financial institutions will be able to employ the username and password from their online banking activities to access Social Security Administration or Veterans Affairs applications.

Identity management and related policy, security, access and control functions evolve very rapidly to meet an ever-changing virtual environment. It is very difficult to keep up with changes even when devoted exclusively to these areas and few organizations can afford all the specialists needed with the requisite experience and expertise to meet the challenges facing IT organizations today. Federations usually have a large number of participants who focus on IDM, security and other functional specialties key to every organization, whether or not participating in a federation. Joining a federation may provide access to a

body of knowledge and a group of experts to assist an organization in upgrading IDM and security skills and techniques.

Costs

The costs associated with participating in a federated identity system can be substantial and must be planned for. However, precise dollar amounts will vary from enterprise to enterprise, organization to organization. Varying costs are based on an organization's existing infrastructure, speed of adoption, size of the enterprise, as well as the technology solutions that will be integrated to support federation. Typically these solutions are part of IDM components. These components consist of authentication and access management services, user provisioning processes (that include single or reduced sign-on and password management functions), as well as directories, meta- and virtual directories at their foundation. It is important to note that some of these costs and subsequent return on investment cannot be adequately determined at this point in time due to the cutting-edge factor of identity federation.

Once the business case for federation has been accepted by an organization, the usual technology costs apply. Again, the disparity in costs will depend on the scope of implementation, design and implementation variables including system integration, support staff development and training. Other standard costs include hardware purchases and maintenance support, software licenses and maintenance, along with any operational costs such as administration or resource staffing.

The other significant cost impact centers around the time it takes to actually complete the federated identity picture. The toll that time to implementation takes on an organization's energy and resources, human or otherwise, should not be marginalized.

Savings

Initially, it is important to point out that when an organization commits to implementing federated identity technologies as a strategic business initiative, the notion of savings may not be realized early on. Once having elected to do so, an organization may hope to gain a competitive advantage or be better positioned to provide entitlement services by the benefits of these technologies. Again, due to the cutting-edge technologies involved, those ROIs, will be determined at some point in the future.

As a result of underlying identity management infrastructure that must be in place to provide identity federation, there are generally acknowledged savings associated with the provisioning and lifecycle management of user accounts that can be viewed as a benefit of identity federation. These include administrative cost reduction in both the management of user accounts and password management, along with cost reductions as a result of more self-service functionality tied to user provisioning services.

In addition, there are productivity gains from access management component standardization for application development. Since identity management systems also provide provisioning integration to non-digital assets, there are savings associated with the on and off boarding of employee assets such as ID cards, computers, phones, pagers etc.

Most importantly, however, are the savings associated with an organization's use of identity management components to meet legal, regulatory and security requirements. These components typically provide greater access auditing capabilities than those without IDM components. The access management functionality ensures that privacy and security policies are deployed consistently and are enforced across the enterprise. This becomes even more significant when participating in a federation, where consistent security and privacy policies are often required to be adopted beyond an organization's boundaries.

In the end, despite the initial start up costs and a slow ROI, adopting the use of federated identity may be less costly. An organization that does not integrate the back end identity management components into its infrastructure will be left with silo-type systems that cannot keep pace with online service delivery. They will be faced redundancy of user accounts across those silos and will be unable to offer a better user experience for clients.

Security

The challenge for organizations considering participation in a federation is how can they exchange identity information across boundaries without increasing risk or liability? Distributed network models are becoming increasingly more prevalent and as a result any one organization becomes a component of a larger network. Boundaries are broken down in an ecosystem where identity information isn't controlled by a single organization. This enables increased access to information for customers, employees, and partners but do these interdependencies and increased complexities allow for improved security?

The answer is yes. In a federation, an organization can realize improved security at lower cost particularly because operating rules and standards can be defined, accepted, implemented and certified by all members of the federation.

Operating rules, for instance can define credential revocation procedures or set minimal levels of assurance for a transaction which increase the confidence in how access is managed. Other rules can be put in place for auditing to include the entire evidence chain used to make access control decisions. The evidence serves as a legal record of who accessed what data at what time, why and on whose authority.

Standards are an essential element of federation security in that they define the protocols for communication and acceptance of identity information. This is where Security Assertion Markup

Language (SAML) plays an important role. SAML v2.0, approved as an OASIS Standard in March 2005, improves upon earlier work achieved in SAML v1.1 and adds attributes from both the Shibboleth initiative and the Liberty Alliance's identity federation framework.

SAML has become the leading Web services standard for federated identity management. Using a defined set of XML formats, it can represent identity and attribute information, as well as protocols for requests and responses for access control information. SAML is based on the idea of assertion, or a statement made by a trusted party to another. An assertion can be made about the identity and access rights of a user which are trusted by another party. That party need not have access to a directory service or need to trust the user – they only need to trust the assertions source.

Security is vastly improved through the use of the SAML standard. For one, this greatly improves risk mitigation as it places liability for user actions with the authenticating party. It also facilitates the use of encryption, so that assertions about identity or attributes can be secured. SAML protocols can be transported over HTTP over SSL 3.0 to ensure the confidentiality of a message and frequently the asserting and trusting party have a pre-existing relationship built on public key infrastructure (PKI).

Using SAML within a federation to improve security can also reduce costs. Instead of the many business units within a federation or even within a single organization needing to be reconfigured for central directory access, they can remain in place and be linked together through common SAML interfaces. It is this open Web services standard which eliminates the need for costly custom API programming and central directory service management allowing organizations to leverage their existing investments.

Privacy

Privacy need not be a victim in the identity management model found within a federation. In fact, the basis of the federation, the distributed network, ensures that an individual’s information is spread across participating organizations and not as vulnerable if it is kept in a central repository.

Furthermore, a federation can be designed so that users have more control over their information, a practice that is a key feature of any privacy policy. Participation in the federation is often made voluntary for users who can withdraw their consent or terminate when they wish. Account linking is a feature of SAML v2.0 although users can have control over which accounts are linked. In addition, anonymity and pseudo-anonymity as defined in SAML v2.0 allows for protection of identity information of users.

A common set of policies and operating rules within a federation also improves privacy by ensuring that all members meet a certain standard of compliance. Provisions can be implemented to protect the accuracy and validity of data that might be corrupted by such things as human error (e.g., data entry,

transposition, translation, carelessness), poor integration of data from multiple data sources and erroneous linking of information and data cleansing.

An overall privacy policy is an important part of any federation as it will define how information is collected, stored, accessed, shared, corrected and purged. It should contain provisions to handle different information needs applicable to employees, non-employee users, contractors, third parties (i.e., the media or information brokers), and the public. A privacy policy should also include the results of a legal analysis to ensure compliance with both the letter and the intent of all applicable local, state, tribal, and federal laws about what information may be collected, what information may not be collected, how the information can or cannot be collected, how long it may be retained and with whom it may be shared. The analysis will also identify gaps where there is no law to guide the policy or where there are conflicts in laws and practices that need to be reconciled before drafting a policy.

Other components of a federation's privacy policy should include a defined process for notifying users if their data are released for other than the originally intended uses. It should ensure that there is a process established to allow users to review what is in their files and correct the information if needed. And if there is an unauthorized release or use of information, legal provisions for sanctions, penalties, or other remedies should be defined.

While users may have significant experience sharing information within an informal circle of trust, they should be able to have confidence that when they turn over information that will now be digitized, stored and available to a potentially larger group of individuals outside of their circle, they can trust the federation to keep it secure and private.

What Are the Issues and Challenges of Identity Federation?

One of the major challenges is that most or all identity federations are very new. The concept of an identity federation is only a few years old. Virtually everything about federations is rapidly evolving and will change dramatically over short periods of time. Risks will explode and disappear. Technology will diverge and converge often at the same time. Policies, processes and other components of federations will be rapidly moving targets until there appear a few dominant entities in this area. Following are some of the issues and challenges that federations face.

Policy

Federations face challenges in the creation and maintenance of policy, rules standards, etc. in balancing the often competing needs of CSPs, relying parties and users. The federation policy must be flexible

enough to meet rapidly evolving requirements, yet constant enough to engender trust among participants and users and to allow participants a stable environment in which to operate. Participating organizations and users face challenges in assessing whether federation policy will serve their needs or desires and protect their interests. Is federation policy compatible with the culture of the organization? Does federation policy instill confidence in the user?

This section and the next on legislation focuses on federation in the federal government, but the lessons and recommendations are applicable to government organizations at all levels, specifically if contemplating participation in the E-Authentication Federation or conceptually if considering participation in the E-Authentication Partnership or other federations.

At the federal level, not all federal electronic transactions require authentication; however, this guidance applies to all such transactions for which authentication is required, regardless of the constituency (e.g., individual user, business, or government entity). Transactions not covered by this guidance include those that are associated with national security systems as defined in 44 U.S.C. § 3542(b)(2). Private-sector organizations and state, local, and tribal governments whose electronic processes require varying levels of assurance may consider the use of these standards where appropriate.

There are two types of individual authentication:

1. Identity authentication—confirming a person's unique identity.
2. Attribute authentication—confirming that the person belongs to a particular group (such as military veterans or U.S. citizens).

Attribute authentication is the process of establishing an understood level of confidence that an individual possesses a specific attribute. If the attribute does not provide ties to the user's identity, it would be considered an *anonymous credential*. Agencies may accept anonymous credentials.

Federal guidance describes four identity authentication assurance levels for e-government transactions. Each assurance level describes the agency's degree of certainty that the user has presented an identifier (a credential in this context) that refers to his or her identity. In this context, assurance is defined as (1) the degree of confidence in the *vetting process* used to establish the identity of the individual to whom the credential was issued, and (2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.
The four assurance levels are:

- Level 1: Self Assertion—no confidence in the asserted identity's validity. Some confidence that the same person is accessing a resource as previously.
- Level 2: Some confidence in the asserted identity's validity.
- Level 3: High confidence in the asserted identity's validity.
- Level 4: Very high confidence in the asserted identity's validity.

To determine the appropriate level of assurance in the user's asserted identity, agencies must assess the potential risks, and identify measures to minimize their impact. Authentication errors with potentially worse consequences require higher levels of assurance. Business process, policy, and technology may help reduce risk. The risk from an authentication error is a function of two factors:

1. Potential harm or impact.
2. The *likelihood* of such harm or impact.

Categories of harm and impact include:

- Inconvenience, distress, or damage to standing or reputation.
- Financial loss or agency liability.
- Harm to agency programs or public interests.
- Unauthorized release of sensitive information.
- Personal safety.
- Civil or criminal violations.

Required assurance levels for electronic transactions are determined by assessing the potential impact of each of the above categories using the potential impact values described in Federal Information Processing Standard (FIPS) 199, "Standards for Security Categorization of Federal Information and Information Systems." The three potential impact values are (1) low impact, (2) moderate impact and (3) high impact.

Compare the impact profile from the risk assessment to the impact profiles associated with each assurance level, as shown in Table 1 following. To determine the required assurance level, find the lowest level whose impact profile meets or exceeds the potential impact for every category analyzed in the risk assessment (as noted in step 2 following).

Table 1 – Maximum Potential Impacts for Each Assurance Level

Assurance Level Impact Profiles				
Potential Impact Categories for Authentication Errors	**1**	**2**	**3**	**4**
Inconvenience, distress or damage to standing or reputation	Low	Mod	Mod	High
Financial loss or agency liability	Low	Mod	Mod	High
Harm to agency programs or public interests	N/A	Low	Mod	High
Unauthorized release of sensitive information	N/A	Low	Mod	High
Personal Safety	N/A	N/A	Low	Mod High
Civil or criminal violations	N/A	Low	Mod	High

In analyzing potential risks, the agency must consider all of the potential direct and indirect results of an authentication failure, including the possibility that there will be more than one failure, or harms to more than one person. The definitions of potential impacts contain some relative terms, like "serious" or "minor," whose meaning will depend on context. The agency should consider the context and the nature of the persons or entities affected to decide the relative significance of these harms. Over time, the meaning of these terms will become more definite as agencies gain practical experience with these issues. The analysis of harms to agency programs or other public interests depends strongly on the context; the agency should consider these issues with care.

Agencies shall use the following steps to determine the appropriate assurance level:

Step 1: Conduct a risk assessment of the e-government system.

Guidance for agencies in conducting risk assessments is available in A-130, Section 5 of the U.S. Office of Management and Budget's GPEA guidance and existing NIST guidance. The risk assessment will measure the relative severity of the potential harm and likelihood of occurrence of a wide range of impacts (to any party) associated with the e-government system in the event of an identity authentication error.

Note: An e-government system may have multiple categories or types of transactions, which may require separate analysis within the overall risk assessment. An e-government system may also span multiple agencies whose activities may require separate consideration.

Step 2: Map identified risks to the required assurance level.

The risk assessment should be summarized in terms of the potential impact categories in Table 1. To determine the required assurance level, agencies should initially identify risks inherent in the transaction process, regardless of its authentication technology. Agencies should then tie the potential impact category outcomes to the authentication level, choosing the lowest level of authentication that will cover all of potential impacts identified. Thus, if five categories of potential impact are appropriate for Level 1, and one category of potential impact is appropriate for Level 2, the transaction would require a Level 2 authentication. For example, if the misuse of a user's electronic identity/credentials during a medical procedure presents a risk of serious injury or death, map to the risk profile identified under Level 4, even if other consequences are minimal.

Step 3: Select technology based on the NIST e-authentication technical guidance.

After determining the assurance level, the agency should refer to the NIST e-authentication technical guidance to identify and implement the appropriate technical requirements.

Step 4: After implementation, validate that the information system has operationally achieved the required assurance level.

Because some implementations may create or compound particular risks, conduct a final validation to confirm that the system achieves the required assurance level for the user-to-agency process. The agency should validate that the authentication process satisfies the system's authentication requirements as part of required security procedures (e.g., certification and accreditation).

Step 5: Periodically reassess the information system to determine technology refresh requirements.

The agency must periodically reassess the information system to ensure that the identity authentication requirements continue to be valid as a result of technology changes or changes to the agency's business processes. Annual information security assessment requirements provide an excellent opportunity for this. Agencies may adjust the identity credential's level of assurance using additional risk mitigation measures. Easing identity credential assurance level requirements may increase the size of the enabled customer pool, but agencies must ensure that this does not corrupt the system's choice of the appropriate assurance level.

Legislation

OMB's Government Paperwork Elimination Act (GPEA) guidance states that properly implemented technologies can offer degrees of confidence in authenticating identity that are greater than a handwritten signature can offer. Conversely, electronic transactions may increase the risk and harm (and complicate redress) associated with criminal and civil violations. The Department of Justice's "Guide for Federal

Agencies on Implementing Electronic Processes" discusses the legal issues surrounding electronic government. Legal and enforcement needs may affect the design of an e-authentication system and may also entail generation and maintenance of certain system management documentation.

Legal issues can present significant policy challenges for agencies. Agencies should consider these issues when assigning transactions to assurance levels. Risk assessments should include the potential effects of illegal activities and process failures with respect to agency enforcement priorities, agency programmatic interests, broader public interests such as national security, the environment, and economic markets.

The risk analysis incorporates this by discussing the risks associated with criminal and civil violations, and harm to agency programs or the public interest. Agencies should remember to consult appropriately with their counsel's office in their determination of this impact. For example, if sensitive information is available from an agency Web site, the agency should consider the effects of single acts and possible patterns of such activity when assessing risk levels. (18 U.S.C. 1029, 1030)

Agencies may also decrease reliance on identity credentials through increased risk-mitigation controls. For example, an agency business process rated for Level 3 identity assertion assurance may lower its profile to accept Level 2 credentials by increasing system controls or "second level authentication" activities.

Agencies are expected to follow all relevant guidance issued by the National Achieves and Records Administration (NARA) regarding the handling of electronic records.

Most e-authentication processes capture the following information:

- Information regarding the individuals/ businesses/governments using the e-government service.
- Electronic user credentials (i.e., some combination of public key certificates, user identifiers, passwords, and Personal Identification Numbers).
- Transaction information associated with user authentication, including credential validation method.
- Audit log/decurity information.

To the extent that the authentication process captures information that is protected by the Privacy Act (because it is information about an individual that the agency retrieves by an individual's name or other identifier and thus is maintained in an agency Privacy Act system of records), the agency needs to comply with the Privacy Act with respect to such information. Authentication data must be protected from

unauthorized disclosure or modification. The Privacy Act generally requires that registered users be allowed to have access to and request amendment to information about them maintained in a system of records. Information from the system of records should not be shared, except in accordance with the Privacy Act and other applicable laws.

User Acceptance

Will users accept identity federation? It should not be taken as a given that a new model that gives a user a single point of authentication for access to multiple applications will be favored by the user. Many organizations' users trust existing systems. This established history may create resistance when new practices are implemented. Some users may find they are uncomfortable providing the required personally identifiable information for certain authentication assurance levels. Education can play an important role, particularly when it comes to providing feedback to users on risk mitigation for privacy concerns.

A thorough assessment and implementation process must be deployed to ensure user confidence in the third-party Credential Service Providers, or CSPs. Since identity credentials are used to represent one's identity in electronic transactions, it is important to assess the level of confidence in the credential. CSPs are governmental and non-governmental organizations that issue and sometimes maintain electronic credentials. These organizations must have completed a formal assessment against the assurance levels described in this guidance.

The CSP's issuance and maintenance policy influences its e-authentication process trustworthiness. The E-Authentication Initiative will therefore develop an assessment process for the government to determine the maximum assurance level merited by the CSP. For example, if a CSP follows all process/technology requirements for assurance Level 3, a user may use a credential provided by the CSP to authenticate himself for a transaction requiring assurance Levels 1, 2, or 3.

When developing authentication processes, agencies must satisfy the requirements for managing security in the collection and storage of information associated with validating user identities. The E-Government Act of 2002, Section 208, requires agencies to conduct privacy impact assessments for electronic information systems and collections. This includes performing an assessment when authentication technology is added to an electronic information system accessed by members of the public. For additional information on privacy impact assessments, consult OMB further guidance.

Security and Safety

The U.S. Federal Trade Commission has highlighted identity theft as the fastest growing white collar crime in America with over 10 million Americans reporting becoming victims per year since 2001. While considered to be an "insider" threat, criminal activities committed by people internal to an organization, was the most common problem before 2001. Since 2003, however, the primary manner of compromise has been external compromise of federated data by coordinated criminal attack.

Allowing access by federation participants to secure databases, federated access increases the likelihood that a penetration by unwanted users or miscreants into one section of the federation will widen and create damage or loss in other areas of the federation.

The following databases that allow federated access have been documented as sources of identity and credit information theft in 2004 and 2005.

- Reporting files of drug sales to confirm "doctor shopping" compliance
- Boating registrations
- Credit scoring agencies
- City government tax, home sale, title and animal registrations
- County real estate estimations
- College records
- College alumni organizations
- Merchant credit card validations
- Marketing records
- Frequent flight point clubs

The Bugbear Trojan Threat

The Bugbear worm illustrates the Trojan phenomenon. In late May of 2003, a blended threat (a threat that uses several different techniques to attack a system) from eastern Europe was unleashed on the net by the name of Bugbear.B. Within one hour it was sighted in 115 countries as reported by www.MSNBC.com.

Bugbear.B focused on computers linked to certain Internet domains owned by over 1,200 financial institutions. It appended itself to more than 30 different programs and executed when those applications began running. Any hard drives sharing data with infected systems were also in danger from the worm.

Bugbear.B is a sophisticated and targeted worm, a malicious program called a "key logger." It stores a user's keystrokes and uses this information to enter areas under the guise of someone else's identity. It also attempts to shut down any antivirus software and related security programs running on a victim's computer. It then transmits the stolen passwords to 10 drop sites located in the former Soviet Bloc.

There is evidence that several targeted attacks using the Bugbear.B have been launched in 2003 and 2004 against local governments lacking the expertise to detect or remove the worm.

In most instances authentication theft is perpetuated by the over-reliance on passwords, the weakest of authentication options. Passwords are easily compromised, easily circumvented, and often can be stolen in batches.

The preferred modus operandi of sophisticated hacker criminal syndicates is to steal authentication/access controls to facilitate widespread identity theft in order to duplicate the credit history and identity of the victims. Most computer intrusions are perpetuated as a

result of insufficient access controls and weak authentication mechanisms. In 2003, a World Bank report entitled “Electronic Safety and Soundness: Securing Finance in a New Age”[8] cited the exponential growth in identity and authentication theft. The report highlighted the stark reality that more than 57% of all hack attacks last year were initiated in the financial sector (Glaessner, Kellermann, & McNevin, 2003). The FBI has corroborated this statistic. With the growing amount of financial data stored and transmitted online, the ease of computer intrusions add to the severity of traditional crimes such as identity theft; to put this in perspective for the digital age, over USD$222 billion in losses were sustained to the global economy as a result of identity theft.

Whereas many have focused on the insider threat, it should be noted that according to OECD estimates in 2004, one out of every three PCs (clients) was hijacked, or “zombied”, by an outsider. Additionally, the OECD study cited that every virus and worm released last year contained a Remote Access Trojan (R.A.T.). These remote access Trojans allowed for cyber bandits to infiltrate clients through executable backdoors. While Trojans may have surveillance capabilities, to be effective, communications channels must exist through which Trojans inside the infected machine and remote hackers/crackers send and receive data. Quite possibly the biggest threat posed by a Trojan infection is its ability to open “back doors” in a compromised system, allowing a malevolent user(s) to remotely control the infected computer and subsequently have access to the computer’s network.

This threat is far more massive than is appreciated by nearly all users of systems today. Processing power has become so large in most systems that the additional “trickle” of processor time used by sophisticated thieves is virtually undetectable without active monitoring tools deployed by trained IT professionals. Once a Trojan horse has been introduced into a user’s computer system it plants a program that searches for vulnerable, open ports. When it locates a target, the Trojan uses this open port as a communications channel. Through these backdoors, remote crackers launch code to vandalize, alter, move, or delete files on the infected computer. They may also harvest sensitive user information such as financial account numbers and passwords from the victim’s locally stored data files, and then transmit this information through the backdoors. The Sysbug Trojan is a recent example. Symantec has seen a 50% rise in compromised back doors.[9]

The global financial regulatory community has advised banks on multiple occasions for the need to transition to “two-factor” authentication. (FDIC: FIL-132-2004: Study on "Account-Hijacking" Identity Theft and Suggestions for Reducing Online Fraud; FDIC: Press Releases - PR-125-2004 12-14-2004)

[8] See Glaessner, Kellermann & Mcnevin 2003. Electronic Safety and Soundness, World Bank. http://wbln0018.worldbank.org/html/FinancialSectorWeb.nsf/(attachmentweb)/E-safetyandSoundness/$FILE/E-safety+and+Soundness.pdf.
[9] Krebs, Brian, “Computer Worms Breeding More ‘DDoS’ Attacks,” washingtonpost.com, 4 Nov 2003, The Washington Post, accessed on 4 Nov 2003 at: <http://www.washingtonpost.com/ac2/wp-dyn/A61786-2003Nov4?language=printer>.

A simple authentication taxonomy should be noted; there are three factors of authentication:

1. Something you have (e.g., hardware token or smart card).
2. Something you know (either shared-secret or non-shared secret).
3. Something you are (biometrics, such as fingerprint or retina scans).

In the evolving electronic world that has been based on secrets, shared-secrets are becoming a larger and larger problem. Federated data is extremely vulnerable to attacks of this nature and it is recommended that any organization participating in a federation with sensitive data consider implementing "multi-factor" authentication, or, combining password access with "something you have" or "something you are." Government federated environments, such as those mandated by HSPD-12 (Homeland Security Policy Directive-12) in 2004, direct the use of "smart card" access to both the physical facility as well as with logical access to government computer systems in combination with strong passwords.

Decision Points

An organization's decision to join an identity federation is not made casually or randomly, simply because it is the new technology buzzword. Such a decision would be made based on the acknowledgement of a need for successful deployment of "Web services"[10] as part of an organization's strategic initiative involving electronic service delivery. Most significantly, participation in an identity federation requires the implementation of a service oriented architecture (SOA), and an acknowledgement that the management of user identities between corporate and/or government enterprise boundaries is vital for both security and the successful deployment of those Web services.

Organizations are currently faced with significant challenges as they deploy Web services. The business, technical and legal requirements for seamless access to services that cross enterprise boundaries, need to be addressed in ways that map to the corresponding bricks and mortar processes in those enterprises. One of the outstanding issues is the management of users that are both internal and external to the

[10] The term *Web services* describes a standardized way of integrating Web-based applications using the XML, SOAP, WSDL and UDDI open standards over an Internet protocol backbone. XML is used to tag the data, SOAP is used to transfer the data, WSDL is used for describing the services available and UDDI is used for listing what services are available. Used primarily as a means for businesses to communicate with each other and with clients, Web services allow organizations to communicate data without intimate knowledge of each other's IT systems behind the firewall. Unlike traditional client/server models, such as a Web server/Web page system, Web services do not provide the user with a GUI. Web services instead share business logic, data and processes through a programmatic interface across a network. The applications interface, not the users. Developers can then add the Web service to a GUI (such as a Web page or an executable program) to offer specific functionality to users. Web services allow different applications from different sources to communicate with each other without time-consuming custom coding, and because all communication is in XML, Web services are not tied to any one operating system or programming language. For example, Java can talk with Perl, Windows applications can talk with UNIX applications. Web services do not require the use of browsers or HTML. Web services are sometimes called *application services*. WEBOPEDIA

organization. All users become a shared responsibility. The functionality of federated identity supports a distributed computing model such as Web services that span enterprise domains. Its processes and procedures allow organizations to share user authentication. However, liability risks along with the costs associated with establishing a trust framework for sharing user authentication is part of the picture as well. Along with any technical requirements, formal agreements between all participants need to be established that specify operating rules for exchanging authentication information. These rules include privacy compliance requirements, dispute resolution and any liability provisions.

In addition to business and legal interoperability, technical interoperability must be addressed as well. An SOA must be in place, and online services must be developed which leverages that architecture in order to achieve federation. The use of standards such as SAML[11] must be part of the application design in order to share identity information across organizational boundaries. The use of SOA, along with these standards, provides mechanisms for security that are necessary along with the disappearing perimeter of an organization that is the result of cross boundary integration.

The examples cited in this paper of identity federations serve as evidence that this model is increasingly becoming a favored approach to identity management for many organizations. As suggested throughout, there are multiple drivers moving the public and private sector toward federation including the threat of terrorism, the explosive growth in identity theft, market pressures for efficiency and an increased focus on end-user satisfaction. Yet even with the rise in popularity of federated identity architectures, this paper also points out that there are costs to consider, tradeoffs that may be required, and a number of issues which are likely to arise. With that in mind, organizations are encouraged to become actively engaged during the process of deciding whether to join or initiate an identity federation. There are a number of factors to consider when weighing the decision and for some organizations a federation may not be the appropriate framework for identity authentication.

Organizational Compatibility

Organizations that decide to share credentialing services across applications may find that a number of factors frustrate their efforts to work together toward this common goal. Preeminent among these is the matter of trust. The federation must be able to trust that members will not serve as a weak link and that a minimum standard for privacy and security can be met as a credential is authenticated and passed from application to application.

---

[11] Security Assertion Markup Language (SAML) is an XML standard for exchanging authentication and authorization data between security domains, that is, between an *identity provider* and a *service provider*. SAML is a product of the OASIS Security Services Technical Committee. Wikipedia.

Trust is essential when organizations which may have vastly different missions, cultures, structures and management styles have to work together to organize a federation. Seemingly straight forward questions about the type of federation, the credentialing model, data ownership, levels of assurance and impact, risk mitigation plans may unravel the best laid plans for a federation if organizations lack a sense of being able to rely on one another. This is especially true when the rash of security breaches reported on over the past twelve months demonstrate that breakdowns can lead to financial, civil or criminal liabilities.

Technical Considerations

Technology plays an important role in the success or failure of a federation. Member organizations which likely employ vastly disparate technologies now must find ways to reach adequate levels of interoperability. Although reliance on a variety of technologies is beneficial in that it increases flexibility, it often drives up integration costs, particularly if Commercial Off The Shelf (COTS) products are not used. Furthermore, each member must have the appropriate technical competence if the integration is to be deployed across the entire membership without creating a weak link.

External Dependencies

If membership is geographically diverse, organizations both in the public and private sector may find that policies and regulations impact their participation within a federation. This may vary across the federation depending on the locale of different members. For instance, as mentioned previously, privacy laws show great variance across states. A provision for the management of personal data required of one member may have ramifications for the group that other organizations are not prepared to address. In the public sector, an agency's movement into a federation may be dependent on the actions of a legislative body (e.g., appropriations of funds), something which could impact the entire group's effort.

Organizations that decide to work through these and other potential issues will find participation in a federated environment brings a plethora of benefits to members. When loosely formed relationships are transformed through the structure of a federation, there can be significant improvement in the management and enforceability of standards, policies and protocols for shared credentialing. This can enhance cross-boundary communications, facilitate resolution of intra-federation issues and lead to greater participation and relationships among members.

Standards for a federation which may be defined by initiatives such as the Liberty Alliance Project or outlined through publications such NIST SP 800-63 support greater interoperability among members. The result can be operational efficiencies such as lower software development and maintenance costs, faster transactions and other cost economies.

Managed properly, a federated environment provides robust security. Improved management of security policies can lead to greater control of identity across organizations. Members will find greater ease with identity revocation, enhanced levels of non-repudiation and augmented information sharing regarding security threats. Furthermore, interoperable but distinct technologies found within the federation reduce the risk of breaches across the shared enterprise.

Customer satisfaction is a driving factor in the adoption of federated identity management and the benefits for end users shouldn't be underestimated. A federation offers an individual the opportunity for more control over their personally identifiable information, improved access especially with cross certification across multiple federations and overall better service when compared to models with multiple points of authentication.

Cases

The following cases are demonstrative of the universe of existing federations or those in development. The cases were chosen to provide examples of the range of choices made in creating and implementing identity federations.

ComCare Case Study

An Overview of Some Issues of Federations for EMS Inter-Agency Communication to Create an Inter-Agency, All-Hazards Alert System.

The ComCare Alliance, with a study grant for DHS, launched an initiative to create a federation of databases of skilled EMS and related service providers to address the needs of alerting and reporting of relevant issues.

The Components of the ComCare Challenge

The issues of federation in the area of emergency management and services (EMS) communication are extremely complex. The challenges of credentials include:

- Who gains entry?
- What multiple layers of access should exist?
- How to reconcile non-parallel nomenclatures used for communications.

- Once a member, what is the “too much information” result?
- Classified and unclassified information may intermix.

The task force assembled by ComCare has worked to address the credentialing issue while looking at the nature of the alert information separately. The alert information was looked examined along five “Axis of Information”:

1. “Common” information alerts through highly classified alerts.
2. All agency, some agency, intra-agency, partial agency or domain expertise alerts.
3. Specific roles or ranks both for inter and intra agency alerts.
4. Variable rules for role based on type of incident – talk vs. listen only.
5. Transfer of incident command as events during scale up and down.

Working out which type of EMS agency, what roles and which members of each EMS agency have jurisdiction must address extremely complex issues that are technical, factual and historical. A fire chief announcing “This is my Incident Command Now” when smoke comes out of a building the police have surrounded is common, already difficult and made more complex when interagency communication and alert systems are built.

In addition “call fatigue,” “too much information,” or “that’s not the information my team needs” issues can be a problem making EMS responses less effective by making information too abundant but less specific to a teams task. Fire crews do not need to know about every incident effecting power lines. But they do need to know about those with a high likelihood of creating fire. In this case the “filter” has traditionally been the “intelligent phone tree” that the power company dispatch would call 911 only if they needed them. All other power line issues were dealt with by the utility.

The Business Case of ComCare “All Hazard Alert” System

In Sum:

- EMS providers often do not know what situation they are being dispatched to.
- Experts in rare and dangerous events are often alerted well after the event begins.
- Interagency response “who has command” is often hard to determine.
- Tabletop drills consistently show this concern is largest threat in many situations.

Every EMS responder of any kind can provide an exhaustive list of examples of arriving at a scene with “no clue” of what they were arriving to do, why or who else would be there. This failure to get good information en route has been the root cause of many tragedies when responding to emergencies of a

non-malicious nature. In the very foreseeable situation of an event created with malicious intent, this failure to know often results in catastrophic losses in tabletop exercises.

There is a compelling need to allow first responders to know what they will address, to coordinate multiple agencies in response, and finally to alert and mobilize key specialists from remote locations. This alert must be timely, preplanned and have a clear chain of command.

Unfortunately, by placing vast amounts of sensitive data in one place, the chance of it being compromised, or used itself for malicious intent can not be ignored.

Role identification for who needs, who wants, and who may activate certain alerts make the problem not only one of getting information, but who can start information.

Rules for who has authority to start an alert are, when examined, equally complex as who receives an alert, but they also create an obvious starting point to develop the federation.

Once ComCare has created an All Hazard alert system, it will to some extent, bypass the traditional role of dispatch and be able to directly inform elements of EMS issues of a situation initiated from the system.

If the ComCare Alert does not involve and match with information coming from local and trusted dispatch systems, it can both become untrusted, or worse, a confusing element.

The traditional manners of communication in emergency responder communities have been trust-based with historically high barriers to entry both technically and procedurally. Local fire, hazmat, local police, state police, forest service, coast guard, border patrol, customs, military branches, FAA, hospitals, ambulance services, EMTs, chemical plants, utilities and road crews are all examples of entities with:

- Communications and alert needs within their role and jurisdiction.
- Needs for cross-agency alerts in some situations.
- Information needed by other entities before and during some incidents.
- Internal structures, communications and nomenclatures unique to them.
- Historical power centers and rivalries that may be difficult to overcome.

Nearly every local jurisdiction has public and private agencies who have separate, discrete systems of communication, recall, alert and stand-down. It is equally true to have very different methods of credentialing, and usage rights. It is also true that for 90% of all EMS communications and alerts there is

no need at all for interagency communication and the very process of making such information interagency may complicate problems legally, physically and procedurally.

Of equal importance is that very few of these “historical trust” or esprit de corps based systems have any formal credentialing process. Only “known” members of the organization exist in the Circle of Trust making the credential process highly accurate but often completely undocumented. “I know he’s got my back, and he knows I’ve got his” dominates this space. In addition, in all interagency responses conflicts between agency procedures, nomenclatures and operations are common and often highly charged. “We have always done it this way and the other guys should change” is a large issue in EMS communications.

ComCare asked for the dispatchers who manage local information to be the primary gatekeepers to validate credentialing in the system. A local EMS agency signs up leadership on the ComCare All Hazard System, and ComCare administration then turns to local dispatch organizations to gain a level of trust of “Do you know them?” “Do they have these skills?” “Who do you call first among this group?”

Issues and Challenges Going Forward

In the spring of 2005, a tabletop drill was coupled with a beta test of the system, involving participants from over 100 EMS agencies and seven technology providing companies.

Three hundred and forty self-selected EMS responders were assigned to roles matching their skill sets in an area of Anytown, Kentucky, and treated to the string of alerts the ComCare System would send out for an event in which a rail tank car derailed and exploded.

The issues and challenges arising from this event fall into three categories.

1. Information overload.
2. Information compromise.
3. Contradictions between local command, local dispatch and ComCare notifications.

The events tiered roughly as follows:

1. Reported explosion(s), possibly involving a train(s) or train-side building(s), this alert primarily went to the “standard” set of local responders (fire, police, EMTs, hospital, and city officials).
2. Reports of the explosions involving a tank car carrying HazMat went the same suite of local responders, but expanded to regional hospitals, rail experts and state and federal enforcement.

3. A series of increasingly detailed alerts about the Chlorine-based material in the tank car, the nature of injuries, the nature of the search and rescue, the nature of casualties, the nature of the triage and the movement of the chlorine cloud went out.
4. A stand down that the situation would need no further assets.

Examining information overload issues.

Many of the 340 participants had checked off areas they wanted to receive information that in retrospect they did not need. One example was ambulance location, movement and dispatch. This is area was the domain expertise of only five members of the demonstration, but was an area in which over the majority of participants checked off "yes" in the desire to get notification related to the issue. Thus, as the drill went along, more than 100 participants were constantly distracted by the nearly endless stream of information coming from the needs of getting numerous ambulances to locations in which victims of the chlorine gas were found.

In the after action, no participating member of the event felt they had gotten the correct information, and most reported a response along the lines of "I got so much information about what was happening I couldn't do my job, and had no idea what was relevant for me."

This problem was a predictable result of the "self-selecting what information I need" that the ComCare Federation has followed. All IT experts involved with the drill had warned that this was a concern. It remains a concern for all federations of EMS information.

Examining information compromise issues.

ComCare's All Hazard Alert System directly alerts relevant dispatch centers, but it does not directly alert non-dispatch EMS personnel or groups of assets, they are alerted by commercial providers who echo the ComCare alert. The alert sent out by ComCare is an E-XTML message. It arrives at commercial and public notification tool suites. PSAPs, 911 commercial sites and commercial notifiers like First Alert, All Alert, National Notification Networks, OneCall, and Send Word Now all participated. They repackaged the messages for delivery to land-lines, cell-phones and PDAs.

The after action evaluation pointed out none of these organizations had clearance to carry EMS data required to comply with HIPPA and in some cases sensitive data delivery, but did so in this drill.

All of the secondary commercial providers, the ISPs, common carriers and other various POPs both had the information themselves and could easily have provided to unwanted sources. A best case is they would use the information themselves, become a source for the media, or worse, perpetrators of malicious intent could have either had access to the response and created countermeasures on the

ground, or hacked into the commercial providers and sent a false message, introducing into the system a compromise via one of these vendors. A false instruction, indistinguishable from a true one could have instructed responders to go into the chlorine gas cloud rather than retreating from its path.

In addition, all 340 of the participants reported the enormous distraction that once they had been alerted and joined the process, their common carrier devices continued to give the same information they were getting from their proprietary EMS networks. And in most cases their cell phones and PDAs became overwhelmed with calls making them un-unusable as back up devices.

It should be a consideration of any federation of EMS providers that once an EMS responder has been recalled and joined the proprietary networks, their personal commercial devices should be dropped from the alert network. This may be a process of creating an entry code from the device itself to be excluded from future alerts.

Finally the tabletop experienced a limited number of contradictions between local command decisions and instructions sent out on general alerts. While in this incident it did not cause a noted problem, the possibility a problem could occur was obvious to trained observers.

Decision Points

Uniform agreement exists that large area disasters need methods and planning for interaction and alert. However, the risk/reward evaluation of the ComCare effort makes it unclear if a self-selecting federation of EMS providers of an all-hazards system will improve the reaction to EMS situations.

Strong thought needs to be places on who needs to be alerted, what they need to be told and when, who should stay in the all-alert network and who should be dropped out and placed into proprietary responder systems so they can do their jobs.

How the decision will be made going forward is unclear at this time. But the lessons learned from the ComCare effort are:

1. Alerting all EMS impacted by an event via a federated alert system is valuable.
2. After the initial alert, most EMS communication is best done outside this system.

Case Study of the Capitol Corridor Train Mobile Environment

The Capitol Corridor Inter-City trains travel from Auburn, Sacramento, Santa Clara and San Jose in California's Silicon Valley. The trains are running trials that will evaluate technology and business models for trial WiFi and mobile Internet, working with the State of California, Department of Transportation, Rail Division, which has made arrangements with the California Center for Innovative Transportation (CCIT), an applied transportation technology research institution affiliated with the University of California Berkeley. The project is a collaboration between the French technology center of excellence, INRETS, GLOCOL, and the University of California at Berkeley.

The effort is to lead trials to provide secure wireless Internet services on a long-term exclusive basis. The example helps establish a protocol for sharing data and survey results with each vendor that respects the sensitivities of each vendor.

Mobile IP and WiFi on Train and Berkeley Mobile Environment Simulation

Wireless fidelity or Wi-Fi communication and mobile IP is being used for trials for commuter Internet services for mobile environments. Research Framework by Glocol introduces mobile IP, an open standard, defined by the Internet Engineering Task Force (IETF), which is becoming dominant today as it allows a user to keep the same IP address, stay connected, and maintain ongoing applications while roaming between IP networks. Mobile IP is scalable for the Internet because it is based on IP; any media that can support IP can support mobile IP. Mobility and networks while-in-motion are becoming dominant themes for the mobile Industry.

In IP networks, routing is based on stationary IP addresses. A payment device on a network is reachable through normal IP routing by the IP address it is assigned on the network. A payment device sitting on a network inside a moving medium such as an automobile, bus or train, as it roams away from its home network, is no longer reachable by using normal IP routing. This results in the active sessions of the payment device being terminated. Mobile IP enables users to keep the same IP address while traveling to a different network, ensuring that a roaming individual can continue communication without sessions or connections being dropped.

The security of transportation systems has taken on new dimensions since 9/11. New threats on the security and the safety of transportation systems, particularly trains and their users have come to light in recent years and present tremendous technical and operational challenges to wide open and expansive systems such as railroads. But new advances in information technology, particularly in the areas of sensing, data management and computing, and communications offer many opportunities to meet these

challenges. One such opportunity is the growing interest in and market for the use of wireless technologies such as WiFi to provide Internet access on the various elements of the railroad system.

The objective of this scenario and simulation is to create a plan of pilot deployment to utilize wireless technologies while creating a trusted environment for secure transit operators:

- Capture the scene of security violation for post-incident investigation.
- Prevent wireless theft of data, wireless and radio-based hacking (e.g., wireless access security).
- Evaluate the wireless technologies as part of the viable communication mechanism for emergency response where land phone is inoperable.
- Implement a viable mechanism to alert train conductor of any adverse safety/security violation
- Improve passenger safety and make precautionary measures for any kind of fraud on train.

The simulation scenario describes an exercise to model and create a mobile network environment simulation within the Berkeley campus to demonstrate mobile networks using mobile IP protocol on mobile router and provide a platform to simulate trackside/wayside research tests before undertaking the test demonstrations at actual rail environment for physical testing on trains. The simulation tests also helped to demonstrate various mobility issues, especially identity federation issues, inside a mobile network and protocols for route optimization and to prepare a reference architecture for future trackside/wayside and terrestrial networks for rail and road, while demonstrating basic core requirements for real-time homeland security infrastructure deployment needs such as video surveillance. Currently, a vendor, Opti-Fi, managed by Parsons and Pointshot Wireless, is running trials on four train sets using satellite download and cellular upload. However, the bandwidth and speeds with such techniques are low.

Sharing Information and Fundamental Trusted Performance Attributes

The effort is intended to provide secure wireless Internet services on a long term exclusive basis. The example helps establish a protocol for sharing data and survey results with each vendor that respects the sensitivities of each vendor. Following are fundamental trusted performance attributes identified as core features of any wireless Internet service provider requirements:

Protected Commuter Communications

- E-mail, instant messaging, voice/fax

Protected E-Payment

- Online purchasing and e-payment
- Pay-for-content

- Pay-for-service
- Electronic ticketing

Information Protection

- Privacy
- Digital rights management
- LOB database locator

Network Access

- VPN and wireless access to home network
- Client integrity checking
- Protected logon

Information Access Control

- Documents and records
- Rail application information access
- Secure Web access for trusted operations like e-payment

Obtaining Identity of Users: An Online Evaluation Process

1. Performance Evaluation from End to End (How users feel its speed)

   1.1 Purpose

   The measurement of the throughput between the Web site the user is visiting, e-mail service and users' PCs (This is the throughput users feel when they use their PC.)

   1.2 Method

   Measure elements in section 1.3 through the users' logs

   1.3 Roles of Vendors

   The vendors capture the Following from users' logs and submit it to CCIT every two weeks. The data format will be shown by CCIT.

#	Elements	Purpose
1	Common ID over vendors*	Recognize the same user who may log in more than one Vendor
2	Timestamp at login/out	Calculate average throughput by (Volume of data) / (logout time – login time)
3	Volume of data transferred during the session	
4	Location at login/out	
5	SMTP and POP	Check whether users use e-mail or not

The preferable way to recognize the same user who may log in more than one vendor is that every vendor shares the unique and common login ID. In order to do so, one of three vendors has to establish and maintain the data base and each vendor has to roam to each other.
The second way is that each vendor gets information which can identify users uniquely, for instance, MAC address of WLAN card or e-mail address may be used.

1.4 Roles of CCIT

CCIT analyzes the data (checks the number of users, calculates throughput, etc).

2. Evaluation of the Service Availability

2.1 Purpose

The measurement of the availability (stability) of the service and the rectification of the throughput measured in section 1

2.2 Method

Measure the number and duration of disconnection during the service

2.3 Roles of Vendors

The vendors check the availability of the network between the gateway to the internet and the wireless interfaces. If they found the disconnection more than one minute in any part of their system, they have to inform CCIT.

2.4 Roles of CCIT

CCIT analyzes the availability of the system and takes considers it calculating the throughput.

3. Performance Evaluation within the vendors' system

3.1 Purpose

The measurement of the throughput and/or the round trip time between the closest point to the gateway to the internet and the wireless interfaces (This is the throughput or round trip time within the vendors' system)

3.2 Method

Some CCIT agents aboard trains will send "ftp", "ping", or "traceroute" command(s) to the FTP server which should be set up at the closest point to the gateway to the internet in the vendors' system.

3.3 Roles of Vendors

Each vendor sets up their FTP server where CCIT designates.

3.4 Roles of CCIT

CCIT makes experiments at least one round trip (Sacramento – San Jose) for each vendor.

4. Others

Vendors have to link the every element in section 1 to 3.

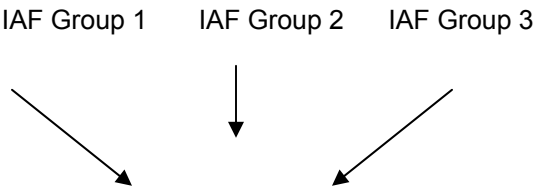
Risk Areas and Challenges

- Open access login
- Local registry – acceptance and session close after user leaves
- Handoff deals with the local registry
- Backend compatibility
- Process used for validation
- Individual authentication and device authentication
- Repeated authentication
- Identity management system under a single authority

Common Situations for Federation Needs:

- Commuter running late, reaches the train at the last minute, jumps on the train and need a ticket.
- Regular commuters want to automatically reload payment and use some common applications maybe, like payment for on-air-TV, e-ticketing, payment for food services etc.

Draft Experimental Design for Trial Evaluation



1st connection

- User profile : frequent traveler : yes , no
    - **Unique USER ID given by the vendor for the entire duration of the trial**
    - Login time stamp
    - Train number, origin/destination (if applicable)
    - Volume of data uploaded
    - Volume of data downloaded
    - Average transmission rate
- User evaluation: 1) quality of the session: poor, average, good excellent 2) willingness to pay for the session (in the absence of any monthly plan):
    - Logout time stamp

2nd connection

- enter User ID

If the user evaluation questions were not answered at the end of the previous connection ask again

Then →

- Login time stamp
- Volume of data uploaded
- Volume of data downloaded
- Average transmission rate

- User evaluation : (1) quality of the session : poor, average, good excellent, (2) reasons, (3) willingness to pay for the session (in the absence of any monthly plan)
    - Logout time stamp

Nth connection

Methodology for Data Collection for Trial Deployment and Evaluation

The same user who may log in more than one vendor must be recognized as the same person. It will not be so easy. The methodology for this is described below.

Alternative 1

The first proposed alternative for data collection for evaluations is to collect data into a common database of commuters/users, if agreed upon by all vendors participating in the trial, such that a common ID used for registering with Vendor 1 could also be available for logging in with the other vendors. This would require use of a common database as a user pool. In this option, every vendor shares the unique and common login ID either in real-time or by FTPing to CCIT at midnight and then this data becomes available to other vendors as well. Thus the user can "roam" with each vendor. This is illustrated in the ID Allocation Model 1 in Figure 1.

The difficult part in this option is to have the vendors agree to sharing their trials information and customer database and also to have a provision for consolidation and settlement process amongst the vendors. The advantage this option could present to CCJPA and CCIT is to have a common database for more level evaluations and easier comparison of feedback from the users.

Alternative 2

It is perceived that the vendors may not agree to share their database amongst each other, and hence the other alternative proposed is for each vendor to provide some unique information which can identify users uniquely in their data base, when FTPing the user information to CCIT, for instance, MAC address of WLAN card or e-mail address may be used. The unique key provided by the vendor for the session data, for identifying a user without any customer-specific profile information, would be used as a means for matching user access and response by the specific person while traveling on different trains equipped by different vendors. This is illustrated in the ID Allocation Model 2 in Figure 2.

Again, as with alternative 1, vendors have the option to FTP their information to CCIT either in real-time, at midnight or at bi-weekly intervals, as decided upon discussions with vendors. The data provided by each vendor shall remain confidential to each vendor and CCIT when provided to CCIT and the evaluations generated from this data would be shared for analysis only, either with the specific vendor or commonly, as may be decided, after discussions with vendors.

The difficult part is to have a uniqueness of information which could be provided by the use of MAC address, though limiting the use of that specific device for the user for trial participation. If MAC address is

not used and vendors do not wish to share e-mail addresses of their users, and a user ID or additional password (say Gamma) is used, there is a possibility even though quite low, that different users on different trains may have generated the same user ID or matching password. These issues can be ironed out during discussions with vendors.

Tools for the evaluation and based on vendor's agreement

- Allocation of a unique customer ID that allows the evaluation agent to track all sessions of same individuals over time and over different vendors. The unique user ID number can be attributed following model 1 or model 2.
- Definition of an online procedure for logout that allows the vendor to send the two final session questions to the users and collect the answers associated to the session.
- Format of the data transmitted every two weeks or midnight by each vendor to the evaluation agent at CCIT as per mutual agreement
- Online monitoring tool for CCIT staff/evaluation agent aboard trains for user count summary statistics.

Figure 3 gives a hi-level picture of the system work packages. Some work packages are to be prepared for a quantitative analysis.

The results will be disseminated through different vendors following the agreements that will be discussed and established between all partners before the trials.

Figure 1 –
ID Allocation Model 1

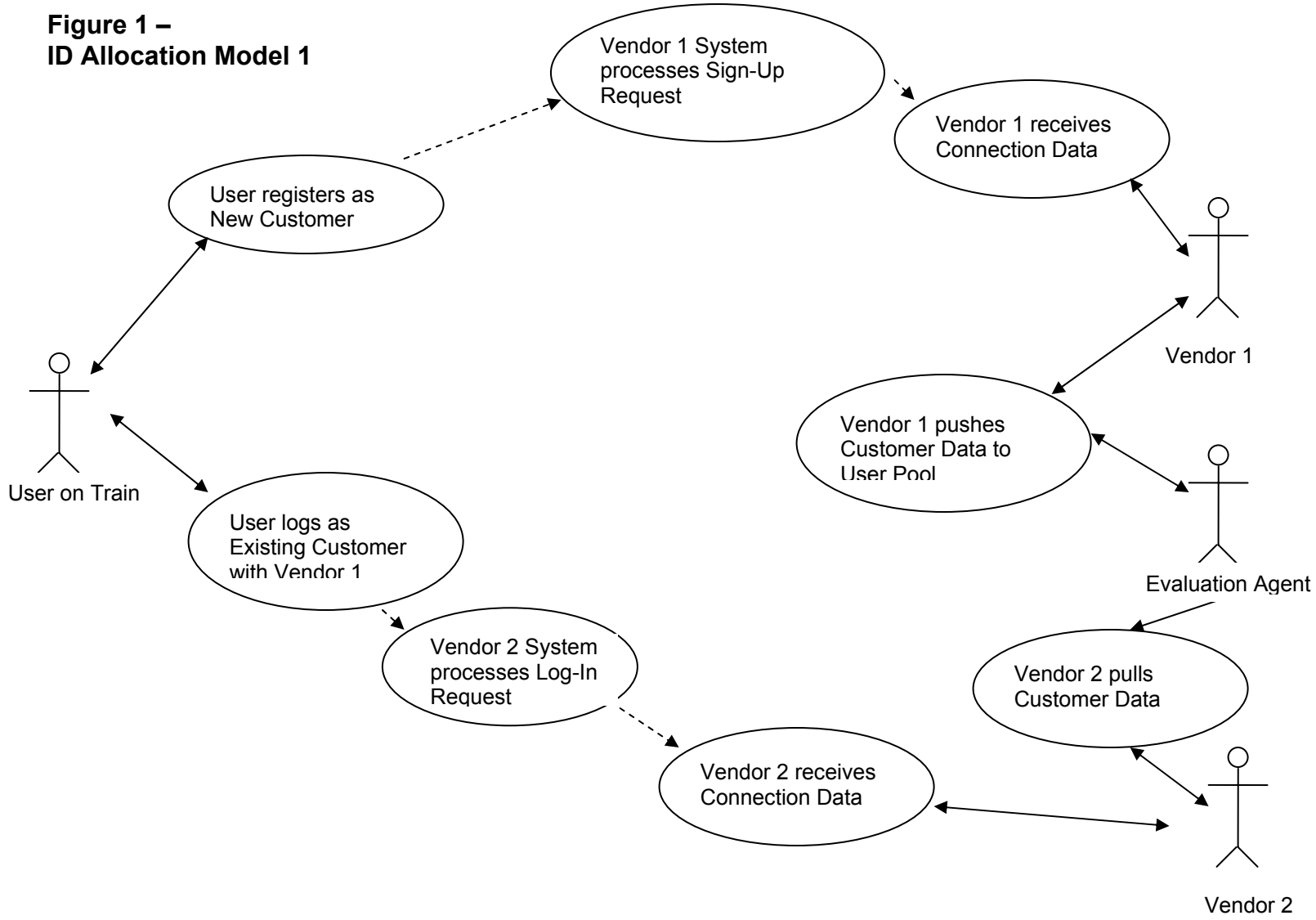


Figure 2 –
ID Allocation Model 2

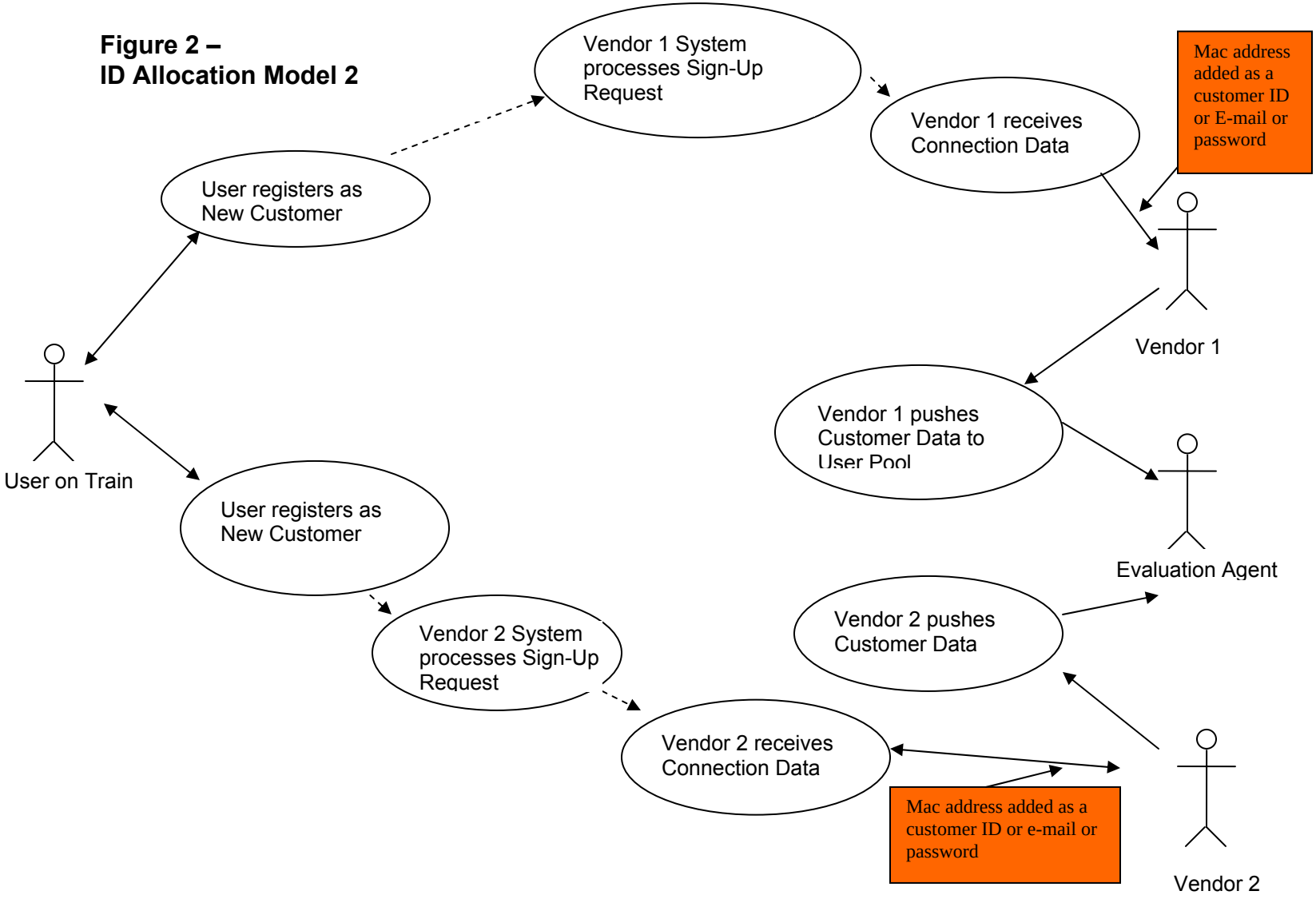
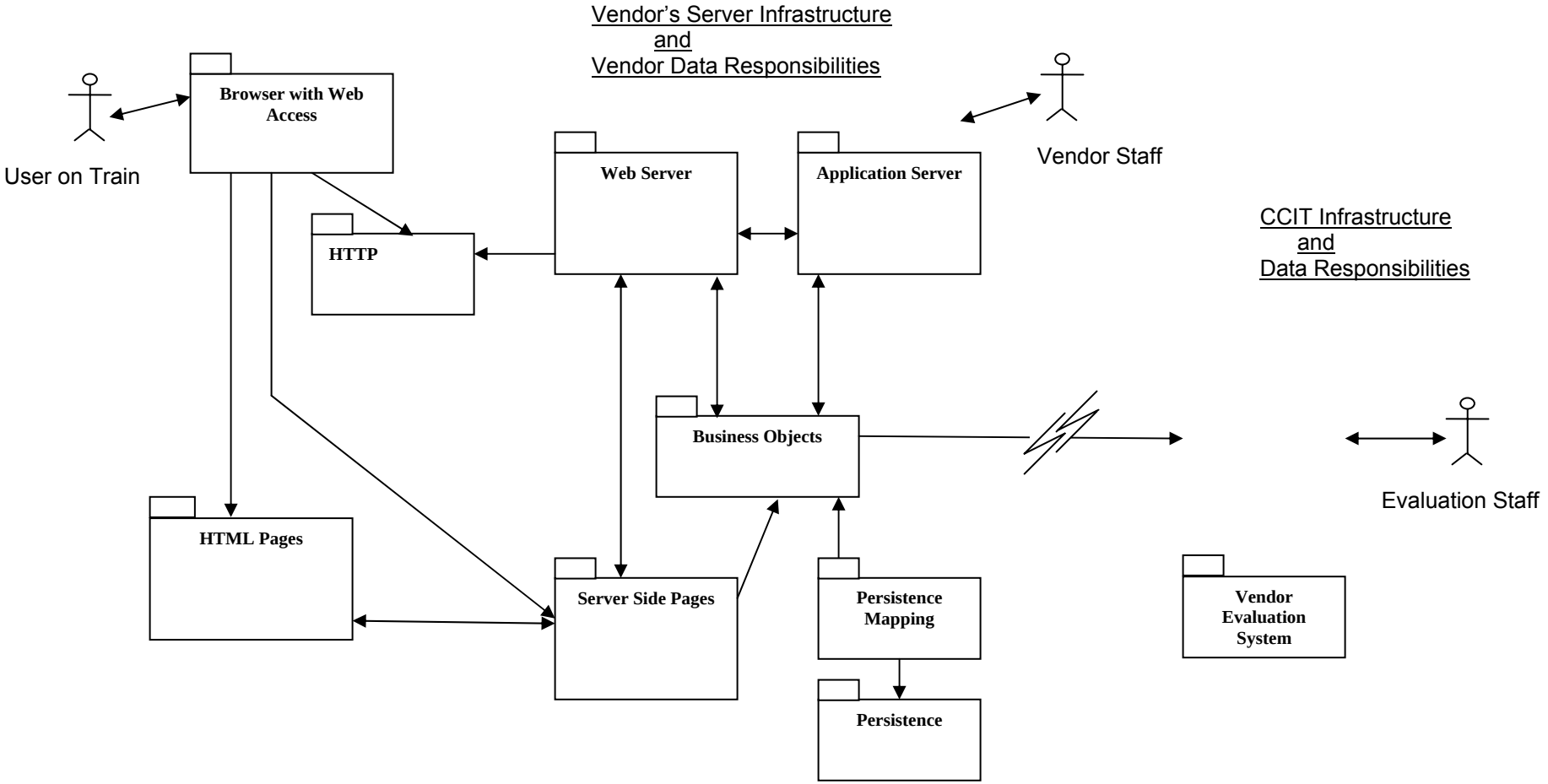


Figure 3: Multi-Vendor Trials Evaluation System Work Package Diagram (CCJPA)



References

1. Process of Capitol Corridor Joint Powers Authority (CCJPA) Commercial Evaluation of Wireless Internet Trials, Jim Allison, Senior Planner, CCJPA.
2. Guidelines for WiFi "Trains Connected" CCJPA Evaluation Project, J.L. Ygnace, Harsh Verma, Kazuhiro Yamada, Doug Cooper.
3. Trains Connected Project, 11th World ITS Congress, Nagoya Aichi, Japan, Harsh Verma, Jean-Luc Ygnace, Hamed Benouar.

Shibboleth-Based Federation(s)

Federations: Sharing Resources Across Domains

When a number of organizations join together to use Shibboleth software to share access to resources in a common way, this is called a federation. The Shibboleth system supports federations by providing scalable methods to manage and distribute configuration and security information among a large number of organizations, and a common vocabulary for user attributes. Internet2 is establishing federations in support of the needs of U.S. higher education, and other federations are emerging in other communities.[12]

A General Introduction

When you want to share secured online services or access restricted digital content, the Shibboleth system offers a powerful, scalable, and easy-to-use solution. It leverages campus identity and access management infrastructures to authenticate individuals and then sends information about them to the resource site, enabling the resource provider to make an informed authorization decision. Shibboleth software is at work today providing this capability—it's a powerful, secure, standards-based and user friendly, inter-realm access-control solution for research and education.

The Shibboleth system provides a standards-based link between existing campus authentication systems and resource providers of all kinds. For example, when a student requests access to a protected video clip, her home organization (origin site) requests her to authenticate (if she has not done so already) and then passes on the information that she is enrolled in Biology 562 to the site housing the video. The provider (target site) uses the fact that she is enrolled in this course to determine her eligibility to access the video.

[12] http://shibboleth.internet2.edu/shibboleth-brochure01.html.

A Solution for the Campus and the User

Because only information (attributes about the person requesting authentication) is exchanged, the Shibboleth system allows institutions with different technology architectures and security systems to easily collaborate without using proxies or managing thousands of external or transitory accounts. It also simplifies the process of integrating a service, such as access to a licensed library resource with campus-based authentication systems. The Shibboleth system can:

- Leverage existing infrastructure (once it's installed, other Shibboleth software-enabled sites can be easily added).
- Facilitate collaboration with other campuses, organizations, and off-campus vendor systems.
- Operate without releasing identity, where appropriate.

From anywhere in the world, users authenticate at their home campuses and those institutions pass information (attributes) on each user's behalf to the resource provider. Users don't need to remember multiple passwords for each restricted site to which they have access.

Below are typical scenarios that the Shibboleth system addresses:

- Enabling anonymous access (and thereby protecting personal privacy) by a member of the campus community to a licensed information resource available to "active members of the community."
- Ensuring anonymous access to a remote information resource where access is limited to "people associated with Course X at the origin site."
- Providing access to a restricted service using an attribute such as a person's name to determine authorization. For example, a team of researchers forming a multi-institutional workgroup can control the release of their attribute information to the workgroup site. In this scenario, access would be denied if an individual chose not to provide the required information.

Who is Using Shibboleth?

Internet2 and a group of leading campus middleware architects from Internet2 member schools and corporate partners constitute the project and implementation team for the Shibboleth initiative. Organizations collaborating in its development include national and international higher education institutions, their partners, content providers, and government agencies.

At The Pennsylvania State University during fall semester of 2002, Information Technology Services and

the Department of Physics piloted the Shibboleth system. Now in production for more than a year, the Shibboleth system has successfully enabled 1,200 Penn State students enrolled in three physics courses to access resources at North Carolina State University to complete their course assignments.

The National Science Digital Library (NSDL), funded by the National Science Foundation, uses the Shibboleth system to facilitate seamless access for its patrons and community participants. David Millman, the director of research and development at Academic Information Systems at Columbia University and a member of the NSDL Core Integration Team said, "The NSDL has long been committed to the Shibboleth technology because of its scalable, distributed architecture and its privacy protections, both critical goals of the NSDL itself."

During 2003, 20 university campuses and higher education service providers, along with six digital content providers/publishers and three course management vendors/publishers, participated in the Shibboleth Pilot Project. Numerous campuses and higher education associations as well as content, service, and learning management system vendors are working on improvements and enhancements to the Shibboleth system.[13]

Components

Shibboleth® Project

When you want to share secured online services or access restricted digital content, the Shibboleth system offers a powerful, scalable, and easy-to-use solution. It leverages campus identity and access management infrastructures to authenticate individuals and then sends information about them to the resource site, enabling the resource provider to make an informed authorization decision.

For example, when a student requests access to a protected video clip, her home organization requests her to authenticate (if she has not done so already) and then passes on the information that she is enrolled in Biology 562 to the site housing the video. The video provider uses the fact that she is enrolled in this course to determine her eligibility to access the video.

Shibboleth, a project of Internet2/MACE, is developing architectures, policy structures, practical technologies, and an open source implementation to support inter-institutional sharing of web resources subject to access controls. In addition, Shibboleth will develop a policy framework that will allow inter-operation within the higher education community. Key concepts within Shibboleth include:

[13] http://shibboleth.internet2.edu/shibboleth-brochure01.html.

- Federated Administration. The identity provider (origin) campus (home to the browser user) provides attribute assertions about that user to the service provider (target) site. A trust fabric exists between campuses, allowing each site to identify the other speaker, and assign a trust level. Identity provider sites are responsible for authenticating their users, but can use any reliable means to do this.
- Access Control Based On Attributes. Access control decisions are made using those assertions. The collection of assertions might include Identity, but many situations will not require this (e.g., accessing a resource licensed for use by all active members of the campus community, accessing a resource available to students in a particular course).
- Active Management of Privacy. The Identity provider (origin) site and the browser user control what information is released to the service provider (target). A typical default is merely "member of community". Individuals can manage attribute release via a web-based user interface. Users are no longer at the mercy of the target's privacy policy.
- Standards Based. Shibboleth will use OpenSAML (www.opensaml.org) for the message and assertion formats and protocol bindings, which are based on Security Assertion Markup Language (SAML, www.oasis-open.org/committees/tc_home.php?wg_abbrev=security) developed by the Oasis Security Services Technical Committee.
- A Framework for Multiple, Scaleable Trust and Policy Sets (Federations). Shibboleth uses federations to specify a set of parties who have agreed to a common set of policies. (A site can be in multiple federations, though.) This moves the trust framework beyond bi-lateral agreements, while providing flexibility when different situations require different policy sets.
- A Standard (yet extensible) Attribute Value Vocabulary. Shibboleth has defined a standard set of attributes; the first set is based on the eduPerson (www.oasis-open.org/committees/tc_home.php?wg_abbrev=security) object class that includes widely-used person attributes in higher education.[14]

The Shibboleth Advantage[15]

Rev. 8-Sep-2003

Contact: <info-shib@internet2.edu>

Shibboleth offers a compelling alternative for providers of services and content to higher ed, by eliminating the need to build extensive custom front-ends and interfaces to deal with the variety of systems customer sites use for controlling access to resources and services. Shibboleth is freely available open source software, available for Solaris, Linux, and Windows 2000/XP. Detailed information is available at http://shibboleth.internet2.edu/.The following is a brief high-level overview of some of the advantages Shibboleth offers:

[14] http://shibboleth.internet2.edu/about-shibboleth.html.
[15] http://shibboleth.internet2.edu/docs/internet2-mace-shibboleth-advantage-200309.html.

Issue	Without Shibboleth	With Shibboleth
End User Authentication	Most content and service providers, if they want to offer services to end users on campuses, generally have had only two options: 1. provide and manage individual accounts for each user, with the high level of support and insecurity this entails. 2. integrate with each customer campus SSO.	Unified authentication mechanism from the vendor perspective, much more scalable, and much less integration work required to bring a new customer online.
Access Control	Fine-grained access control impractical, usually defaults to access decisions based on IP address (or range of addresses), possibly combined with time of day.	Ability to implement fine-grained access control (e.g. access by role), allowing customer sites to effectively control access by attributes and thus control usage costs, by not granting access unnecessarily – compelling marketing message for vendor.
Competitive Advantage: Leading Edge		Ability to market yourself as being at the forefront of compelling new technology adoption. E.g., as Shibboleth enables role based access control (RBAC); vendors are able to offer new service offerings.
ROI - Vendor	Variable and potentially significant costs associated with bringing new customer sites online.	Once the initial Shibboleth integration work has been completed on the vendor's systems, the incremental cost of adding new customers is relatively minimal, in contrast.
ROI - Customer		Many campuses are already implementing Shibboleth as core infrastructure, to support inter-institutional applications, thus they would be leveraging something already in place. If your customers have Shibboleth implemented, it is a matter of managing attributes. For those who have not yet implemented Shibboleth, the installation is relatively easy.
Competitive Advantage: Joint Procurement (e.g. statewide university systems)	Less feasible to offer joint procurement service opportunities in some cases.	Opportunity to offer joint procurement services through federation membership, providing economies of scale for both vendor and customer.

Conclusions

Shibboleth provides an effective solution for secure multi-organizational access to Web resources. IT managers might think that this technology sounds complicated and that external access isn't at the top of

the priority list right now. We suggest that the implications of Shibboleth and its adoption by many campuses and service providers has compelling implications even for those not on the bleeding edge:

- *Meeting campus identity management standards*: Federations such as InCommon are establishing a baseline for campus infrastructures to participate in multi-institutional scenarios. This is strong motivation for IT organizations to bring their local services up to standard in the areas of campus-wide user authentication and directory data management. In particular, stating assurance levels regarding how users authenticate (for example, strength of passwords) is important to applications both external and internal.
- *Privacy control*: Shibboleth meets strong requirements from higher-education communities to provide appropriate protection of personal information even when services use access control. Dealing effectively with privacy concerns is particularly complex; technology is only part of the story. Shibboleth provides campuses with controls so that as a community we can determine the balance points. By deploying Shibboleth, campuses can take better part in this discussion.
- *Attribute-based authorization*: Managing authorization in a secure and cost-effective fashion is a major goal for many IT organizations. The handling of attributes in Shibboleth provides a testbed for the use of role- and attribute-based authorization for applications of all kinds, not just multi-organizational ones. IT organizations can benefit from learning about and contributing to this emerging practice.

A large and growing community is using the Shibboleth System to solve problems and enable a new generation of applications and services. We encourage organizations of all kinds to try out the Shibboleth System and participate in the Shibboleth Project.[16]

E-Authentication Federation

The federal government is currently working on two federation efforts. One is the E-Authentication Federation (EAF and formerly the e-authentication initiative) and the other is the E-Authentication Partnership (EAP). The EAF began as one of the e-gov initiatives as reported in *Federal Computer Week* in its online edition at www.fcw.com:

> "The Office of Management and Budget on Oct. 26, 2001, released brief descriptions of 23 e-government initiatives in the Bush administration's plan to use technology to connect with citizens."
>
> E-authentication, with the General Services Administration as lead agency, would, "(e)stablish a core federal public-key infrastructure with which federal employees and the federal community would interoperate and give the public a secure and consistent method of communication with government."[17]

Since that time the e-authentication initiative evolved to meet the advancing experiences and understanding of federal agencies' and citizens' requirements. While still incorporating the use of PKI the EAF has adapted to include the use of other forms of authentication and security access communication. The EAF is being developed to serve the needs of government for internal and external access to government applications.

[16] Educause Quarterly: Volume 27, Number 4, 2004; http://www.educause.edu/apps/eq/eqm04/eqm0442.asp.
[17] http://www.fcw.com/fcw/articles/2001/1029/web-egovlist-10-29-01.asp#e-auth.

The EAP grew from efforts of some of the same people working to develop the e-authentication initiative. A work group was created under the auspices of the Center for Strategic and International Studies to bring together government and private sector participants to build the foundation of an organization that would provide electronic authentication functions for participants.

The EAF is largely a one-way or “hub and spoke” arrangement in which users access Government applications using credentials issued by approved CSPs. The EAP when fully operational will work as a “mesh” in which credentials from any of the participants might be used to access protected resources in any of the participants’ domains, possibly including both physical and virtual environments. At the time of this writing the EAF is further along in its development and inherently simpler, though by no means simple. The developments in the EAF are shared with the EAP for adoption or adaptation as appropriate to the uses of the EAP. This section will deal with the EAF although much of the information contained herein may well be applicable to the EAP.

It is interesting now to read some of the original information on the EAI.

> “The Bush administration last week identified the 23 e-government projects that it hopes will open a new era of cross-agency cooperation to improve services to the public and eliminate redundant systems.
>
> But information technology experts warn that Bush's ambitious e-government plan has numerous obstacles, not the least of which are finding the estimated $400 million to $900 million needed to fund the projects and convincing agencies to give up control of long-held tasks. The Office of Management and Budget divided the 23 initiatives into four customer segments: electronic service to the public, to businesses, to other governments and within the federal government, with one initiative — securing electronic transactions — cutting across all four. OMB did not include the latter initiative in its initial press release.
>
> The list of projects reflects OMB's interest in eliminating redundant e-government systems, reducing the government's costs associated with developing and managing those systems and simplifying interactions with the public and businesses.
>
> But this plan requires agencies to work together like never before, said Mark Forman, associate director for IT and e-government at OMB.
>
> The fact that the President's Management Council (PMC), as well as OMB Director Mitchell Daniels Jr., signed off on the list should garner some support for it, Forman said.”[18]

The e-government projects have met with some severe challenges. There has never been more than a few million dollars budgeted to these projects intended to dramatically alter the federal government (please note the projected cost of $400 million to $900 million). As might be expected from such ambitious projects there has been internal and external resistance and varying degrees of progress. The

[18] http://www.fcw.com/fcw/articles/2001/1029/news-omb-10-29-01.asp.

EAF experienced many of these same challenges but has survived to become established as the E-Authentication Service Component of the Federal Enterprise Architecture[19] which means it has passed a significant milestone for assuring its long-term existence.

There has been significant Executive Office support of the EAF. OMB M-04-04 (www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf), a memorandum issued to the heads of all departments and agencies by Joshua Bolten, director of the Office of Management and Budget of the Executive Office of the President. The memorandum provides e-authentication guidance for federal agencies covering assurance levels and risk assessments, assessing confidence in credential service providers, implementing an authentication process and the effective dates of the guidance. On August 27, 2004 President Bush issued HSPD-12 initiating a process to create a policy and implement a standard for common identification for federal workers.

Homeland Security Presidential Directive/Hspd-12

Subject: Policy for a Common Identification Standard for Federal Employees and Contractors

(1) Wide variations in the quality and security of forms of identification used to gain access to secure Federal and other facilities where there is potential for terrorist attacks need to be eliminated. Therefore, it is the policy of the United States to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees).

(2) To implement the policy set forth in paragraph (1), the Secretary of Commerce shall promulgate in accordance with applicable law a Federal standard for secure and reliable forms of identification (the "Standard") not later than 6 months after the date of this directive in consultation with the Secretary of State, the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, the Director of the Office of Management and Budget (OMB), and the Director of the Office of Science and Technology Policy. The Secretary of Commerce shall periodically review the Standard and update the Standard as appropriate in consultation with the affected agencies.

(3) "Secure and reliable forms of identification" for purposes of this directive means identification that (a) is issued based on sound criteria for verifying an individual employee's identity; (b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; (c) can be rapidly authenticated electronically; and (d) is issued only by providers whose reliability has been established by an official accreditation process. The Standard will include graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appropriate level of security for each application. The Standard shall not apply to identification associated with national security systems as defined by 44 U.S.C. 3542(b)(2).

(4) Not later than 4 months following promulgation of the Standard, the heads of executive departments and agencies shall have a program in place to ensure that identification issued by their departments and agencies to Federal employees and contractors meets the Standard. As promptly as possible, but in no case later than 8 months after the date of promulgation of the Standard, the heads of executive departments and agencies shall, to the maximum extent

[19] http://a257.g.akamaitech.net/7/257/2422/01jan20051800/edocket.access.gpo.gov/2005/pdf/05-15515.pdf.

practicable, require the use of identification by Federal employees and contractors that meets the Standard in gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems. Departments and agencies shall implement this directive in a manner consistent with ongoing Government-wide activities, policies and guidance issued by OMB, which shall ensure compliance.

(5) Not later than 6 months following promulgation of the Standard, the heads of executive departments and agencies shall identify to the Assistant to the President for Homeland Security and the Director of OMB those Federally controlled facilities, Federally controlled information systems, and other Federal applications that are important for security and for which use of the Standard in circumstances not covered by this directive should be considered. Not later than 7 months following the promulgation of the Standard, the Assistant to the President for Homeland Security and the Director of OMB shall make recommendations to the President concerning possible use of the Standard for such additional Federal applications.

(6) This directive shall be implemented in a manner consistent with the Constitution and applicable laws, including the Privacy Act (5 U.S.C. 552a) and other statutes protecting the rights of Americans.

(7) Nothing in this directive alters, or impedes the ability to carry out, the authorities of the Federal departments and agencies to perform their responsibilities under law and consistent with applicable legal authorities and presidential guidance. This directive is intended only to improve the internal management of the executive branch of the Federal Government, and it is not intended to, and does not, create any right or benefit enforceable at law or in equity by any party against the United States, its departments, agencies, entities, officers, employees or agents, or any other person.

(8) The Assistant to the President for Homeland Security shall report to me not later than 7 months after the promulgation of the Standard on progress made to implement this directive, and shall thereafter report to me on such progress or any recommended changes from time to time as appropriate.

GEORGE W. BUSH[20]

The issuance of HSPD-12 and the creation of a common identification standard for government workers will provide a significant body of people whose identities will be verified according to a common set of criteria with credentials for physical facilities and logical and systems access. This is a large “anchor tenant” ready to use the EAF.

Components

The components of the EAF include the Business Rules included in the Appendix, the EA technical architecture, the risk assessment tool, the trusted credential provider list, the EA laboratory, the approved technology provider list, and a large body of documentation including implementation guides, technical documentation, certificate policy, certification requirements and other related documents.

[20] http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html.

07/13/04

Final E-Authentication architecture approved

By William Jackson and Jason Miller
GCN Staff

The General Services Administration yesterday released the final piece to the E-Authentication puzzle.

The Quicksilver project's executive board approved the final architecture for a federated portal. This final guideline ties together the administration policy on authentication levels and National Institute of Standards and Technology technical guidance.

The final architecture addresses authenticating end users to applications through a portal, the agency transaction or the credential service provider. The portal will use Security Assertion Markup Language scheme to verify the identity of remote users accessing government systems.

GSA also released the adopted scheme for the SAML architect (editor's note, this should be artifact) profile and the interface specifications for the SAML profile.

In December, the project team developed an interim architecture plan outlining how the new approach will work. E-Authentication will use credentials from multiple domains and apply common certifications, guidelines, standards and policies (Click for Jan. 12 GCN coverage).

The architecture is based on open standards, using industry accepted protocols, which accommodate personal identification number and password and public-key infrastructure digital certificate authentications.

The project team, working with the Office of Management and Budget's Federal Enterprise Architecture Program Management Office, also decided to incorporate e-authentication into the FEA in the Service Component Reference Model.

E-authentication would join other support services, such as search, security management, systems management and communication, in the bottom layer of the model.[21]

The article included above provides information concerning some of the components of the EAF as of July 2004. The current EA technical architecture documents with descriptions included can be found at www.cio.gov/eauthentication/TechSuite.htm:

E-Authentication Technical Approach
This document provides a description of the technical approach for the E-Authentication Initiative. The approach is based on an architectural framework that allows multiple protocols and federation schemes to be supported over time. The approach is presented in terms of use cases. This document is subject to periodic revision and update.

[21] http://www.gcn.com/vol1_no1/daily-updates/26561-1.html.

SAML Artifact Profile as an Adopted Scheme for E-Authentication
This paper provides an overview of the use of the SAML Artifact Profile in the E-Authentication Initiative. The SAML Artifact Profile is one of the adopted schemes within the E-Authentication architectural framework.

E-Authentication Interface Specifications for the SAML Artifact Profile
This document provides the interface specifications for the SAML Artifact Profile for use with the E-Authentication Initiative.

Federal PKI Requirements for Path Discovery and Validation
This document specifies requirements for PKI clients used in the Federal PKI. Requirements are specified for path validation, path discovery, and auditing.

Following is included the executive summary from the "E-Authentication Technical Approach" document.

Executive Summary

As part of the President's Management Agenda, the E-Authentication Initiative has been established to enable trust and confidence in E-Government transactions via the establishment of integrated policy and technical infrastructure for electronic authentication. After careful analysis and proofs-of-concept, the E-Authentication Program Management Office (PMO) decided to implement E-Authentication infrastructure as a federated architecture called the Authentication Service Component (ASC). The ASC leverages credentials from multiple credential providers through certifications, guidelines, standards adoption and policies. The ASC accommodates assertion-based authentication (i.e., authentication of PIN and Password credentials) and certificate-based authentication (i.e., Public Key Infrastructure (PKI) digital certificates) within the same environment. Over time, the ASC will support multiple schemes such as the Security Assertion Markup Language (SAML) and Liberty Alliance, and therefore is not built around a single scheme or commercial product. In this light, the ASC is more precisely defined as an architectural framework. The ASC is targeted for incorporation into the Federal Enterprise Architecture (FEA), as its government-wide authentication component.

The technical approach presented in this document is aligned with Office of Management and Budget (OMB) M-04-04, which provides policy guidance for identity authentication. It is also aligned with National Institute for Standards and Technology (NIST) SP 800-63, which is the technical companion document to OMB M-04-04. While the ASC architecture addresses authenticating end users to applications, authorization privileges at the application are beyond the scope of the ASC architecture and this document.

Core architectural requirements derived from the E-Authentication Strategic Plan are discussed, including high-level requirements (leverage credentials, single sign-on, privacy, and governance) and design goals (standards based, use of commercial off the shelf products, federation, durability, and flexibility). Key components (agency applications (AAs), credential services (CSs), end users, and the E-Authentication Portal) are defined and discussed, as well as session types within the framework (browser session, authentication session, and agency session). The technical approaches to assertion based authentication and certificate-based authentication are then discussed in separate sessions, recognizing the significant difference between them.

The assertion-based authentication technical approach is discussed in terms of transaction flows of various use cases: (1) end user begins at the E-Authentication Portal, (2) end user starts at an AA, and (3) end user starts at a CS. Transactions flows also highlight single sign-on, which allows end users to move amongst AAs of equal or lesser assurance level without re-authenticating. Support of multiple schemes is shown via a transaction flow that seamlessly includes a Scheme Translator interposed between the different scheme protocols. A methodology for scheme adoption is also detailed.

The certificate-based authentication technical approach is discussed in terms of transaction flows of PKI use cases: (1) an AA uses a certificate validation service, and (2) an AA integrates validation software to perform local certificate validation. Various validation mechanisms are supported including, but not limited to, Online Certificate Status Protocol (OCSP), Simple Certificate Validation Protocol (SCVP), and XML Key Management Specifications (XKMS). The technical approach also supports use of PKI credentials at assertion-based AAs. A transaction flow for this use case is presented, highlighting a special Scheme Translator called a Step Down Translator that facilitates this.

PKI credentials offer considerable advantages for authentication. They can be validated using only public information. Standards for PKI are also more mature and more widely used than the emerging standards for assertion-based authentication of PIN and password credentials. The Federal PKI (FPKI) employs a Bridge Certification Authority (BCA) to harmonize policies and procedures for Certification Authorities (CAs). The E-Authentication Initiative defers assessment and governance of PKI based CSs to the FPKI Policy Authority (PA), the governing body for the Federal Bridge CA (FBCA).

The technical approach addresses exception scenarios. The E-Authentication Portal has a Uniform Resource Locator (URL) that any CS or AA can redirect an end user to in the event of a problem. The URL supports a number of standard error codes that can be passed to it. This approach helps to minimize the usability and exception handling burden on CSs and AAs, and ensures consistent exception processing throughout the architecture.

The technical approach supports secure Email by leveraging the PKI certificate validation techniques available in certificate-based authentication. Any Secure/Multipurpose Internet Mail Extensions (S/MIME) capable email software product can be used to process signed and encrypted email. Four use case transaction flows are discussed: (1) email application requests certificate verification from validation service, (2) email application validates the certificate directly by running certificate validation software on the end user's desktop, (3) email application uses a dedicated validation service for organizations who trust certification authorities that are not trusted government-wide, and (4) a combination of the previous options.

Additionally, the technical approach supports secure submission of electronic forms. Some EGovernment business is performed with electronic form applications rather than web forms. These applications do not have the same characteristics as browser-based applications. Two use case transaction flows are discussed: (1) certificate-based authentication of electronic forms, and (2) pop up an E-Authentication browser window in the electronic form to leverage all E-Authentication CSs and to minimize the need to customize electronic forms applications.[22]

The Electronic Risk and Requirements Assessment (E-RA) was developed to provide a tool for use by owners of prospective participants or agency applications (AAs). The tool was built to be a self-diagnosis to help the user develop informative insights into the risks associated with authenticating users in order to allow access to applications and system resources. Use of the tool will not result in an answer such as Level 2, but will help the user develop information helpful in deciding authentication levels to employ.

Electronic Risk and Requirements Assessment:

In order to provide authentication services that can be used across government, the E-Authentication project must first identify the full range of authentication requirements for the electronic Government Initiatives and projects. The E-Authentication Initiative teamed with the Software Engineering Institute (SEI) at Carnegie Mellon University to develop a risk-based

[22] http://www.cio.gov/eauthentication/documents/TechApproach.pdf, pages ii and iii.

> approach to authentication requirements, called the **E**lectronic **R**isk and **R**equirements **A**ssessment, or **E-RA**. This approach identifies the risks associated with insufficient authentication of users, and it forms the basis for the definition of authentication requirements. This is the tool that the E-Authentication Initiative uses to assess the authentication risks for its customer government IT systems, and it is available through the E-Authentication Initiative to anyone who would like to use it. Click on the appropriate link to download the version of the E-RA tool that will work for you.
> In response to policy changes and feedback from E-RA users and the E-Authentication Program Management Office, the E-RA tool has been improved. This version of the tool is fully aligned with the OMB M-04-04 E-Authentication Guidance, and includes the following modifications:
>
> - Harmonized Authentication Level descriptions
> - Added "Unauthorized release of sensitive information" Impact Area
> - Synchronized harm categories from OMB guidance

The EAF provides valuable service to agencies and users by conducting “investigations” into credential service providers and technology providers. The EA laboratory conducts testing of companies’ commercial off the shelf (COTS) products to ensure that all approved products will successfully interoperate with each other; that they can send, receive and appropriately interpret assertions from all other approved products. This dramatically simplifies the work for agencies to choose products for their use. The EAF also conducts credential assessments to study and if requirements are met, approve credential service providers to issue credentials for use in the EAF. The documentation pertaining to credential assessments can be found at www.cio.gov/eauthentication/CredSuite.htm**.** The assessments are conducted to assure that the CSP’s have in place appropriate policies and procedures to ensure the validity, reliability and security of their systems.

The documentation produced in conjunction with the EAF and other federal government projects is one of its most valuable components and would be difficult to reproduce in another setting. The ability to call upon the resources of the federal government and a variety of educational and private sector institutions to produce this body of work has led to production of a tremendously valuable set of information that are worth referencing whether considering participation in the EAF or almost any other federation.

The National Institute of Standards and Technology through its Computer Security Division: Computer Security Resource Center has produced a series of publications, the 800 Series (csrc.nist.gov/publications/nistpubs/index.html). This set of documents covers a wide range of Information System related topics. One of the key documents for the EAF is NIST 800-63, the E-Authentication Guideline. This document covers the components and processes necessary to conduct secure validation of individual identities and when required authentication of those identities.

> “Electronic authentication (E-authentication) is the process of establishing confidence in user identities electronically presented to an information system. E-authentication presents a technical challenge when this process involves the remote authentication of individual people over a network, for the purpose of electronic government and commerce. This recommendation provides technical guidance to agencies to allow an individual person to remotely authenticate his/her

identity to a Federal IT system. This guidance addresses only traditional, widely implemented methods for remote authentication based on secrets. With these methods, the individual to be authenticated proves that he or she knows or possesses some secret information. NIST expects to explore other means of remote authentication (for example using biometrics, or by extensive knowledge of private, but not truly secret, personal information) and may develop additional guidance on the use of these methods for remote authentication.

This technical guidance supplements OMB guidance, *E-Authentication Guidance for Federal Agencies*, [OMB 04-04] that defines four levels of authentication Levels 1 to 4, in terms of the consequences of the authentication errors and misuse of credentials. Level 1 is the lowest assurance and Level 4 is the highest. The OMB guidance defines the required level of authentication assurance in terms of the likely consequences of an authentication error. As the consequences of an authentication error become more serious, the required level of assurance increases. The OMB guidance provides agencies with the criteria for determining the level of e-authentication assurance required for specific applications and transactions, based on the risks and their likelihood of occurrence of each application or transaction.

After completing a risk assessment and mapping the identified risks to the required assurance level, agencies can select appropriate technology that, at a minimum, meets the technical requirements for the required level of assurance. In particular, the document states specific technical requirements for each of the four levels of assurance in the following areas:

- Tokens (typically a cryptographic key or password) for proving identity,
- Identity proofing, registration and the delivery of credentials which bind an identity to a token,
- Remote authentication mechanisms, that is the combination of credentials, tokens and authentication protocols used to establish that a claimant is in fact the subscriber he or she claims to be,
- Assertion mechanisms used to communicate the results of a remote authentication to other parties."[23]

NIST Special Publication 800-53 covers security recommendations for the systems that store the information and run the applications of the federal government, but is applicable in large part for any other entities needing to operate secure systems.

The purpose of this publication is to provide guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government. The guidelines apply to all components[24] of an information system that process, store, or transmit federal information. The guidelines have been developed to help achieve more secure information systems within the federal government by:

- Facilitating a more consistent, comparable, and repeatable approach for selecting and specifying security controls for information systems;
- Providing a recommendation for minimum security controls for information systems categorized in accordance with Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems;

[23] http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63v6_3_3.pdf , page vi.
[24] Information system components include, but are not limited to, mainframes, servers, workstations, network components, operating systems, middleware, and applications. Network components can include such devices as firewalls, switches, routers, gateways, wireless access points, and network appliances. Servers can include database servers, authentication servers, electronic mail and web servers, proxy servers, domain name servers, and network time servers. Information system components are either purchased commercially off-the-shelve or are custom developed.

- Promoting a dynamic, extensible catalog of security controls for information systems to meet the demands of changing requirements and technologies; and
- Creating a foundation for the development of assessment methods and procedures for determining security control effectiveness. Information system components include, but are not limited to, mainframes, servers, workstations, network components, operating systems, middleware, and applications. Network components can include such devices as firewalls, switches, routers, gateways, wireless access points, and network appliances. Servers can include database servers, authentication servers, electronic mail and web servers, proxy servers, domain name servers, and network time servers. Information system components are either purchased commercially off-the-shelve or are custom developed.

The guidelines provided in this special publication are applicable to all federal information systems other than those systems designated as national security systems as defined in 44 U.S.C., Section 3542.[25] The guidelines have been broadly developed from a technical perspective to complement similar guidelines for national security systems. This publication is intended to provide guidance to federal agencies until the publication of FIPS 200, Minimum Security Requirements for Federal Information and Information Systems (projected for publication December 2005). In addition to the agencies of the federal government, state, local, and tribal governments, and private sector organizations that compose the critical infrastructure of the United States, are encouraged to consider the use of these guidelines, as appropriate.

1.2 TARGET AUDIENCE

This publication is intended to serve a diverse federal audience of information system and information security professionals including: (i) individuals with information system and information security management and oversight responsibilities (e.g., chief information officers, senior agency information security officers, and authorizing officials); (ii) individuals with information system development responsibilities (e.g., program and project managers); (iii) individuals with information security implementation and operational responsibilities (e.g.), information system owners, information owners, information system security officers); and (iv) individuals with information system and information security assessment and monitoring responsibilities (e.g., auditors, inspectors general, evaluators, and certification agents). Commercial companies producing information technology products and systems, creating information security-related technologies, and providing information security services can also benefit from the information in this publication.[26]

NIST Special Publications 800-73, 800-76, 800-78, 800-79 cover Personal Identity Verification and related issues.

Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*, established a policy for all Federal departments and agencies (hereafter “agencies”) to create and use a government-wide secure and reliable form of identification for their Federal employees and contractors. It further specified that this secure and reliable form of identification be issued only by service providers whose reliability has been established by an official accreditation process. Federal Information Processing Standard (FIPS) 201, *Personal Identity Verification of Federal Employees and Contractors*; NIST Special Publication (SP) 800-73, *Interfaces for Personal Identity Verification;* NIST Special Publication 800-76, *Biometric Data Specification for Personal Identity Verification;* and NIST Special Publication 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification* (hereafter collectively called FIPS 201) specify the requirements for an

[25] NIST Special Publication 800-59 provides guidance on identifying an information system as a national security system.
[26] http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf, pages 2-3.

Integrated Circuit Card (i.e., a "Smart Card") to be used as the secure and reliable form (hereafter called a PIV Card) of identification.

The guidelines in this document should be used by Federal agencies issuing, or preparing to issue, Personal Identity Verification (PIV) Cards that comply with FIPS 201 to their Federal employees and/or Federal contractor employees. These guidelines describe a set of attributes that should be exhibited by a PIV Card Issuer (hereafter called a PCI) in order to be accredited. They should be used by each agency for assessing the reliability of any organization providing its PCI services.

These guidelines are patterned closely after those in NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*. SP 800-37 provides guidance for certifying and accrediting the security of information systems. This document, SP 800-79, provides guidance for certifying and accrediting the reliability of a PCI. Note that use of SP 800-79 for accrediting the reliability of a PCI must be done in addition to accrediting the security of computer systems used by the PCI by using SP 800-37 and SP 800-53 as guidance. [27]

There are many more documents so far created, in process or planned to provide guidance and assistance for those participating in and building identity federations.

Business Case

The EAF, still very early in its implementation, cannot provide documented costs versus savings. At this time the business case for the EAF is still being developed and is likely to be published in the spring of 2006 containing projections. It is a very complicated case to fully define and anticipate the full benefits of federation. Participation can change a wide range of functions, relationships and costs and catalyze business process reengineering across an enterprise. Considering one direct change caused by participation in a federation will provide a basis for exploring other benefits.

Password resetting is a costly, time and resource consuming function that bedevils most operators of secured information resources. Various studies of the costs of password resets place the amount at $25 and up per instance and at $100 to several hundred dollars per year for each password maintained. Help desk surveys indicate that 30% to 70% of all calls are for password resets. If a federation controls access to two applications or resources and all users previously had passwords to and accessed both resources then the organization has reduced the total number of passwords required for accessing these systems by half. The more resources participating the greater the reduction in total passwords required. If a further assumption is made that instead of one organization there are two participating organizations, they share a common base of users and they equally share the credentialing of the users, then each organization issues and maintains one half of the previous number of passwords for one half of the previous number of users. There is a theory that relates the value of a network to the number of participants. The value of a Federation is likely similarly related to the number of its participants, but also the costs to each individual participant of operating the Federation decrease in relation to the number of participants.

[27] http://csrc.nist.gov/publications/nistpubs/800-79/sp800-79.pdf, page 1.

Password resetting is just one of the costs of operating secured information resources. Many other related functions identity verification, provisioning and maintenance and the associated costs will be spread or otherwise decrease and benefits expand in similar manner.

Policy

At the federal level, not all electronic transactions require authentication; however, this guidance applies to all such transactions for which authentication is required, regardless of the constituency (e.g. individual user, business, or government entity). Transactions not covered by this guidance include those that are associated with national security systems as defined in 44 U.S.C. § 3542(b)(2). Private-sector organizations and state, local, and tribal governments whose electronic processes require varying levels of assurance may consider the use of these standards where appropriate.

There are two types of individual authentication:

1. Identity authentication—confirming a person's unique identity.
2. Attribute authentication—confirming that the person belongs to a particular group (such as military veterans or U.S. citizens).

Attribute authentication is the process of establishing an understood level of confidence that an individual possesses a specific attribute. If the attribute does not provide ties to the user's identity; it would be considered an *anonymous credential*. Agencies may accept 'anonymous credentials'.

Federal guidance describes four identity authentication assurance levels for e-government transactions. Each assurance level describes the agency's degree of certainty that the user has presented an identifier (a credential in this context) that refers to his or her identity. In this context, assurance is defined as 1) the degree of confidence in the *vetting process* used to establish the identity of the individual to whom the credential was issued, and 2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.

The four assurance levels are:

- Level 1: Little or no confidence in the asserted identity's validity.
- Level 2: Some confidence in the asserted identity's validity.
- Level 3: High confidence in the asserted identity's validity.
- Level 4: Very high confidence in the asserted identity's validity.

To determine the appropriate level of assurance in the user's asserted identity, agencies must assess the potential risks, and identify measures to minimize their impact. Authentication errors with potentially worse consequences require higher levels of assurance. Business process, policy, and technology may help reduce risk. The risk from an authentication error is a function of two factors:

1. Potential harm or impact.
2. The *likelihood* of such harm or impact.

Categories of harm and impact include:

- Inconvenience, distress, or damage to standing or reputation.
- Financial loss or agency liability.
- Harm to agency programs or public interests.
- Unauthorized release of sensitive information.
- Personal safety.
- Civil or criminal violations.

Required assurance levels for electronic transactions are determined by assessing the potential impact of each of the above categories using the potential impact values described in Federal Information Processing Standard (FIPS) 199, "Standards for Security Categorization of Federal Information and Information Systems." The three potential impact values are: low impact, moderate impact and high impact.

Compare the impact profile from the risk assessment to the impact profiles associated with each assurance level, as shown in Table 1 below. To determine the required assurance level, find the lowest level whose impact profile meets or exceeds the potential impact for every category analyzed in the risk assessment (as noted in step 2 as follows).

Table 1: Maximum Potential Impacts for Each Assurance Level

Assurance Level Impact Profiles				
Potential Impact Categories for Authentication Errors	**1**	**2**	**3**	**4**
Inconvenience, distress or damage to standing or reputation	Low	Mod	Mod	High
Financial loss or agency liability	Low	Mod	Mod	High
Harm to agency programs or public interests	N/A	Low	Mod	High
Unauthorized release of sensitive information	N/A	Low	Mod	High
Personal Safety	N/A	N/A	Low	Mod High
Civil or criminal violations	N/A	Low	Mod	High

In analyzing potential risks, the agency must consider all of the potential direct and indirect results of an authentication failure, including the possibility that there will be more than one failure, or harms to more than one person. The definitions of potential impacts contain some relative terms, like "serious" or "minor," whose meaning will depend on context. The agency should consider the context and the nature of the persons or entities affected to decide the relative significance of these harms. Over time, the meaning of these terms will become more definite as agencies gain practical experience with these issues. The analysis of harms to agency programs or other public interests depends strongly on the context; the agency should consider these issues with care.

Agencies shall use the following steps to determine the appropriate assurance level:

Step 1: Conduct a risk assessment of the e-government system. Guidance for agencies in conducting risk assessments is available in A-130, Section 5 of OMB's GPEA guidance and existing NIST guidance. The risk assessment will measure the relative severity of the potential harm and likelihood of occurrence of a wide range of impacts (to any party) associated with the e-government system in the event of an identity authentication error.

Note: An E-government system may have multiple categories or types of transactions, which may require separate analysis within the overall risk assessment. An E-government system may also span multiple agencies whose activities may require separate consideration.

Step 2: Map identified risks to the required assurance level. The risk assessment should be summarized in terms of the potential impact categories in Table 1.

To determine the required assurance level, agencies should initially identify risks inherent in the transaction process, regardless of its authentication technology. Agencies should then tie the potential impact category outcomes to the authentication level, choosing the lowest level of authentication that will cover all of potential impacts identified. Thus, if five categories of potential impact are appropriate for Level 1, and one category of potential impact is appropriate for Level 2, the transaction would require a Level 2 authentication. For example, if the misuse of a user's electronic identity/credentials during a medical procedure presents a risk of serious injury or death, map to the risk profile identified under Level 4, even if other consequences are minimal.

Step 3: Select technology based on the NIST e-authentication technical guidance. After determining the assurance level, the agency should refer to the NIST e-authentication technical guidance to identify and implement the appropriate technical requirements.

Step 4: After implementation, validate that the information system has operationally achieved the required assurance level. Because some implementations may create or compound particular risks, conduct a final validation to confirm that the system achieves the required assurance level for the user-to-agency process. The agency should validate that the authentication process satisfies the systems's authentication requirements as part of required security procedures (e.g., certification and accreditation).

Step 5: Periodically reassess the information system to determine technology refresh requirements. The agency must periodically reassess the information system to ensure that the identity authentication requirements continue to be valid as a result of technology changes or changes to the agency's business processes. Annual information security assessment requirements provide an excellent opportunity for this. Agencies may adjust the identity credential's level of assurance using additional risk mitigation measures. Easing identity credential assurance level requirements may increase the size of the enabled customer pool, but agencies must ensure that this does not corrupt the system's choice of the appropriate assurance level.

Legislation

OMG's Government Paperwork Elimination Act (www.whitehouse.gov/omb/circulars/a130/a130appendix_ii.html) guidance states that properly implemented technologies can offer degrees of confidence in authenticating identity that are greater than a handwritten signature can offer. Conversely, electronic transactions may increase the risk and harm (and complicate redress) associated with criminal and civil violations. The Department of Justice's "Guide for Federal Agencies on Implementing Electronic Processes" (www.usdoj.gov/criminal/cybercrime/ecommerce.html#GFA) discusses the legal issues surrounding electronic government. Legal and enforcement needs may affect the design of an e-

authentication system and may also entail generation and maintenance of certain system management documentation.

Legal issues can present significant policy challenges for agencies. Agencies should consider these issues when assigning transactions to assurance levels. Risk assessments should include the potential effects of illegal activities and process failures with respect to: agency enforcement priorities, agency programmatic interests, broader public interests such as national security, the environment, and economic markets.

The risk analysis incorporates this by discussing the risks associated with criminal and civil violations, and harm to agency programs or the public interest. Agencies should remember to consult appropriately with their counsel's office in their determination of this impact. For example, if sensitive information is available from an agency website, the agency should consider the effects of single acts and possible patterns of such activity when assessing risk levels. (18 U.S.C. 1029, 1030)

Agencies may also decrease reliance on identity credentials through increased risk-mitigation controls. For example, an agency business process rated for Level 3 identity assertion assurance may lower its profile to accept Level 2 credentials by increasing system controls or 'second level authentication' activities.

Agencies are expected to follow all relevant guidance issued by the National Archives and Records Administration (NARA, www.archives.gov) regarding the handling of electronic records.

Most e-authentication processes authenticate or capture the following information:

- Information regarding the individuals/ businesses/governments using the e-gov service.
- Electronic user credentials (i.e., some combination of public key certificates, user identifiers, passwords, and personal identification numbers).
- Transaction information associated with user authentication, including credential validation method.
- Audit log/security information.

To the extent that the authentication process captures information that is protected by the Privacy Act (because it is information about an individual that the agency retrieves by an individual's name or other identifier and thus is maintained in an agency Privacy Act system of records), the agency needs to comply with the Privacy Act with respect to such information. Authentication data must be protected from unauthorized disclosure or modification. The Privacy Act generally requires that registered users be

allowed to have access to and request amendment to information about them maintained in a system of records. Information from the system of records should not be shared, except in accordance with the Privacy Act and other applicable laws.

Appendix

Included in the following pages is the current draft of the E-Authentication Federation's "Business Rules: E-Authentication Federation."

Version 1.0

November 23, 2004

FINAL DRAFT

Written by Daniel Greenwood, Esq., with Input from Linda Elliott and RJ Schlecht

E-Authentication Business Rules Table of Contents

Drafting Notes:
This document complies with the following drafting conventions. Where another document is referenced within this document, an endnote is provided with additional information about that document such as the citation, full formal name or a URL where it can be found. Where another section of the Business Rules is referenced from within the Business Rules, the title is capitalized (for example, when the remedies of section 5.3 are referenced, the term "Recourse" is used). Defined terms are also capitalized when used throughout the document. The definitions of such terms are contained in Appendix 5, the glossary. Defined terms include other parts of speech of the same word when that word has been capitalized in this document (for example, the words"Approved" and "Approve").

It is expected that this document will be used as a "template", meaning it will serve as an initial version that can be amended as the E-Authentication Federation evolves. To achieve clarity and ease of use, only the minimum necessary overlay of legal and contextual verbiage was included. Where possible, other documents containing additional more specific language have been included by reference. In addition, commercial terms and conditions customary in GSA contracts are expected to result from a future solicitation and procurement process in connection with the E-Authentication Federation.

The E-Authentication Federation Business Rules and Participation Agreements were prepared for the General Services Administration and drafted by Daniel J. Greenwood, Esq. with input from Linda Elliott and RJ Schlecht.

Business Rules
E-Authentication Federation
Version 1.0, 2004-NOV-23

1. Title
This document shall be known and may be cited as the “E-Authentication Federation Business Rules”, or, as referenced herein, as “Business Rules”.

2. Scope

2.1. Scope of Rules
Signatories to these Business Rules agree that these Business Rules govern participation in the E-Authentication Federation, administered by the General Services Administration of the U.S. Federal Government (GSA). The GSA, or its authorized agent, shall Certify Credential Services of a Credential Service Provider (CSP). Certified Credentials of a GSA Approved CSP may be accepted, validated and relied upon by GSA Approved Relying Parties. Such acceptance, validation or reliance need not require the use of any additional contract between an Approved CSP and an Approved Relying Party.

2.2. Agreements and Conduct Outside Scope of Rules
Nothing in these Rules shall be construed to prevent Approved CSPs and Relying Parties from executing such additional agreements among themselves as they see fit, including agreements covering the use of services, transactions or Credentials, including identity assertions or parts of such assertions. However, nothing in such additional agreement or services, transactions or Credentials covered by such agreement may conflict with any part of the Rules, processes or technologies specified or referenced in these Business Rules. Any activity covered by an addenda to the Participation Agreement, an addenda to these Business Rules or by any other contract or agreement other than the Participation Agreement or these Business Rules, is subject to the terms of that other agreement and is outside the scope of these Business Rules.

2.3. Rules Appearing in Multiple Documents
Any provision of these Business Rules that duplicates or emphasizes identical or similar provisions of other normative documents governing the E-Authentication Federation shall not be construed as to lessen the enforceability of any other provisions that have not been duplicated or emphasized.

3. Participation

3.1. Eligibility
The United States Federal Government or any State or Local government of the United States is eligible to become a CSP or a Relying Party under these Rules, provided it is a legal entity and the other requirements set forth in these Rules are satisfied. In addition, any legal entity, including a non-governmental organization, is eligible to become a CSP under these Rules, provided the other requirements set forth in these Rules are
satisfied.

3.2. Participation Requirements

3.2.1. Relying Parties
Approval by the GSA is necessary for a Relying Party to participate in the EAuthentication Federation. A Relying Party must be a signatory to these Business Rules as a prerequisite to approval by the GSA. A party becomes a signatory Relying Party by executing the Relying Party Participation Agreement with GSA. Each such Relying Party Participation Agreement includes obligations whereby these Business Rules, asperiodically amended, are incorporated by reference and consented to.

3.2.2. CSPs
Approval by the GSA is necessary for a CSP to participate in the E-Authentication Federation. A CSP must be a signatory to these Business Rules as a prerequisite to approval by the GSA. A party becomes

a signatory CSP by executing the CSP Participation Agreement with GSA. A CSP Participation Agreement may be executed directly with the GSA, or as part of a formal solicitation and procurement process the GSA may require. Each such CSP Participation Agreement includes obligations whereby these Business Rules, as periodically amended, are incorporated by reference and consented to.

A signatory CSP must also have one or more Credential Services Certified according to the applicable requirements of GSA, including the Credential Assessment Framework Suite (CAF)[1], and be added to the E-Authentication Federation Trusted Credential Service Provider List[2] as a prerequisite for Approval by GSA to participate in the EAuthentication Federation.

3.2.3. End-Users

Any party participating in the E-Authentication Federation as an End-User must have an agreement with an Approved CSP. Such agreement must contain such minimum terms as are required under these Business Rules and the CSP Participation Agreement. End-Users are considered participants in the E-Authentication Federation, but are not direct signatories to these Business Rules.

4. Roles and Obligations

4.1. GSA Role and Obligations

The General Services Administration of the United States Federal Government (GSA) is the party responsible for policy and operations related to the E-Authentication Federation. The GSA is responsible for defining and managing the roles, relationships and mutual obligations among parties operating in the E-Authentication Federation. The GSA uses Business Rules and Participation Agreements as a method of defining these roles, relationships and obligations in a formal and, as needed, enforceable manner. The GSA shall provide processes for determining qualification of any party in the E-Authentication Federation. In the course of such activities, as well as ongoing oversight of participant and system performance, the GSA shall act as coordinator and policy enforcement body for the E-Authentication Federation. The GSA may designate offices, departments or other organizational units within the GSA or otherwise within the United States Federal Government to exercise such rights or obligations defined under these Business Rules.

4.1.1. Operating Authorization

GSA actions in administering the E-Authentication Federation support the authentication component of the U.S. Federal Enterprise Architecture[3]. The President's Management Agenda of 2001[4] directed GSA to lead the operation of the E-Authentication Federation, which implements OMB- M04-04[5] and NIST SP 800-63[6].

4.1.2. Promulgation and Amendment of Business Rules and Other Documents

GSA shall formalize and may amend these Business Rules pursuant to its duty to administer and manage the E-Authentication Federation. Amendments to these Business Rules must comply with the E-Authentication Federation Business Rules Amendment Process[7]. In addition to these Business Rules, the following materials are also formal normative documents defining rights, obligations, processes and other binding statements relative to the E-Authentication Federation: the CSP Participation Agreement, the Relying Party Participation Agreement, the Credential Assessment Framework[8], the Technical Architecture[9], the Interface Specification[10] and the Relying Party Requirements Document.

4.1.3. Relying Party and CSP Approval

The GSA is responsible for determining whether to Approve a Relying Party for participation in the E-Authentication Federation. The GSA shall formalize and may amend periodically requirements for CSP Certification and is responsible for making approval decisions for participation in the E-Authentication Federation by Certified CSPs. The GSA shall formalize, maintain and update as needed a Trusted Credential Service Provider List[11] of Approved and Certified CSPs participating in the E-Authentication Federation. This list shall be a public document and include, at a minimum, the names of each CSP that has been successfully Certified, and the Level of Assurance of each Certified Credential Service of that CSP. The GSA shall determine what continuing audit and other compliance requirements shall satisfy maintenance of Certification and the terms of these Business Rules.

4.1.4. Service Offerings
To facilitate use of the E-Authentication Federation, the GSA will provide policies, various Architectural Components, business relationship management, Business Rules and Participation Agreements and other offerings.

4.1.4.1. Architectural Components
GSA may implement and make available to Approved Parties Architectural Components to facilitate use of the E-Authentication Federation, including the EAuthentication Portal identified in the Technical Architecture[12], Step-Down Translator(s), Schema Translator(s) and Validation Services. The GSA may incorporate additional components.

4.1.4.2. Interoperability Requirements
The GSA shall operate an interoperability laboratory for the purpose of testing interoperability of products, software, communication specifications and other relevant aspects of current and potential future enhancements to the EAuthentication Federation.

4.1.5. Contact Information
For current information related to the E-Authentication Federation and these Business Rules, contact the contact E-Authentication Program Director of the General Services Administration of the U.S. Federal Government or see http://cio.gov/eauthentication/.

4.2. Relying Party Role and Obligations

4.2.1. Relying Party Participation Agreement
A Relying Party is obliged to execute a Relying Party Participation Agreement as a prerequisite to approval for participation in the E-Authentication Federation. The current Relying Party Participation Agreement is included as Appendix 2.

4.2.2. Interface Specification, Approved Software Use and Upgrade
A Relying Party is obliged to comply with and use the E-Authentication Interface Specification[13] to participate in, communicate through or connect with the EAuthentication Federation. A Relying Party is obliged to use software on the Approved Communications Software[14] list or interface software otherwise approved by GSA. In order to maintain Approval to participate in the Federation, each Relying Party is obliged to follow requirements set by GSA to stay current with Approved Communications Software[15].

4.2.3. Security and Privacy Compliance
The following Rules apply to any information system supporting the Agency Application of the Relying Party that is part of the U.S. Federal Government. An Approved Relying Party is obliged to comply with OMB Circular No. A-130[16] including Appendix III to OMB Circular No. A-130[17], with respect to any information technology system of the Relying Party.

An Approved Relying Party is obliged to comply with the Privacy Act of 1974[18] and OMB Memorandum M-03-22[19], including where required, performing a Privacy Impact Assessment with respect to the handling of personally identifiable information of an End-User.

An Approved Relying Party that is not part of the U.S. Federal Government must certify to the GSA that it is in compliance with equivalent safeguards and relevant requirements. GSA, in its discretion, shall determine whether such certification is sufficient.

4.2.4. Reasonable Reliance and Level of Assurance
A Relying Party is obliged to determine for itself whether to rely on the authentication status of an End-User and whether to authorize usage of the Agency Application. In order to determine the authentication status of an End-User, a Relying Party must:
- Determine for itself the level of Agency Application risk, and therefore the needed Level of Assurance, as per the guidance in OMB M-04-04[20] and NIST SP 800-63[21], using the GSA-provided ERA tool or any other method it deems acceptable;

- Determine communications or other interactions through the Federation are with Approved CSPs, in accordance with the Approved Party Authentication requirements in Section 4.4.5 of these Rules;
- Determine that the Level of Assurance of an Approved Credential is not less than the Relying Party required Level of Assurance for its Agency Application; and
- Determine that the credential is currently valid as per the E-Authentication Technical Architecture[22], including, as relevant, the Interface Specification[23].

Communications and other interactions with a CSP or End-User by a Relying Party must comply with the requirements in this Section in order to be within the scope of the EAuthentication Federation and governed by these Business Rules.

4.3. CSP Role and Obligations

4.3.1. CSP Certification
An Approved CSP is obliged to achieve Certification and be added to the Trusted Credential Service Provider List[24]. Certification is achieved upon successful completion of policy mapping, assessment of the CSP according to the CAFs[25] and operational testing.

4.3.2. CSP Participation Agreement
A CSP is obliged to execute a CSP Participation Agreement as a prerequisite to approval for participation in the E-Authentication Federation, thereby agreeing to abide by these Business Rules. The current CSP Participation Agreement is included as Appendix 1.

4.3.3. CSP Continuing Audit Requirement
An Approved CSP is obliged to undergo an audit, no less than annually, confirming compliance with continuing requirements arising out of Certification and with the obligations and other relevant terms of these Business Rules and the CAF[26]. An audit planned or undergone by a CSP unrelated to the E-Authentication Federation may be sufficient to meet this requirement in whole or in part, in the discretion of the GSA.

4.3.4. Material Change to CSP, Credential Services or Credential
An Approved CSP may be required by the GSA to undergo an additional Certification in whole or in part, to re-Certify one or more Credential Services at the same or different Levels of Assurance or to accept Suspension or Termination of Certification and Participation in the E-Authentication Federation when audit results indicate material changes in the CSP, the Certified Credential Services or in the Credentials it issues or other relevant changes that bring the CSP out of compliance with continuing requirements.

4.3.5. Interface Specification
A CSP is obliged to comply with and use the E-Authentication Technical Architecture[27] to participate in, communicate through or connect with the E-Authentication Federation.

4.3.6. End-User Notice Terms
E-Authentication Federation End-User notice terms include agreement to maintain the security of each Approved Credential, including any Token housing each Credential, and to report to the appropriate authorities of the CSP or otherwise any known or reasonably suspected compromise of such Credential or Token.

Every Approved CSP is encouraged to assure the affirmative manifestation of assent by each End-User to E-Authentication Federation notice terms. Every Approved CSP is obliged to assure that each End-User has, at least, been given notice of and the opportunity to review E-Authentication Federation End-User notice terms

4.4. General Obligations
Every Approved Relying Party and Approved CSP (Approved Party) is obliged to comply with the following Rules.

4.4.1. Record Keeping

Any Approved Party may be requested to transmit to GSA transaction information for the purpose of investigating and correcting interoperability issues that may arise between parties operating in the E-Authentication Federation. In addition, every Approved Party, in order to facilitate GSA resolution of disputes under Section 5 of these Business Rules, is obliged to keep records sufficient to preserve relevant evidence of the facts related to the dispute in question. To the extent that information identified in this Section constitutes Personally Identifiable Information within a System of Records under the Privacy Act of 1974[28], nothing in this section shall be construed to authorize or permit the communication of such information about an End-User without that End-User's informed consent.

4.4.2. Federation Security and Reliability

Every Approved Party agrees to coordinate with the GSA in safeguarding the security and reliability of the E-Authentication Federation. GSA may render inaccessible any Architectural Component of the E-Authentication Federation to prevent or cease serious harm to the Federation. Every Approved Party agrees the GSA reserves the right to suspend participation by any Participant in the E-Authentication Federation in accordance with the E-Authentication Federation Participation Suspension Policy[29], and only under extraordinary circumstances necessary to prevent or cease serious harm to the EAuthentication Federation.

To assure the reliable operation of the E-Authentication Federation, every Approved Party must inform GSA through appropriate channels of any material change in a web site, use of an Architectural Component or other technology or business modification that can reasonably be expected to disrupt, significantly delay or prevent communications through the Federation. This notice must occur in a timely manner prior to the date of any such planned modification.

4.4.3. Federation Interoperability

To assure the efficacy and operation of the E-Authentication Federation, every Approved Party must demonstrate to the GSA that its interactions and communications through the Federation comply with the E-Authentication Technical Architecture[30] and will interoperate with the architectural components of the Federation. To this end, every Approved Party must conduct tests of its planned Federation interactions and
communications in the Interoperability Lab, or through such other process GSA may designate, to demonstrate compliance and interoperability requirements for the Federation have been met.

4.4.4. Operational and Ongoing Requirements

Every Approved Party is obliged to comply with application, testing, piloting, production and continuing maintenance requirements set forth by the GSA. These ongoing requirements include continued compliance with the provisions of the CAF[31] and with applicable requirements documents defining operational sufficiency for participation in the E-Authentication Federation. Nothing in this section, however, shall be construed to
prevent any Approved Party from extending, adding to or otherwise applying other technologies or services in accordance with Section 2.2 of these Rules.

4.4.5. Authentication of Approved Parties

Communications through the E-Authentication Federation are subject to mandatory authentication by the communicating Approved Parties to prevent participation in the Federation by non-Approved Relying Parties or CSPs. To this end, Approved Parties must implement and comply with the E-Authentication Federation Technical Architecture[32] specifications for authenticating approved parties.

4.4.6. End-User Privacy

Every Approved Party is obliged to assure that each End-User has provided Informed Consent to the sharing of any personally identifiable information related to the End-User by the Approved Party with any other party operating within the E-Authentication Federation, including any personally identifiable information contained in a certificate or other identity assertion as included in the Interface Specification. Under these Business Rules, no Approved CSP or Approved Relying Party is permitted to share

personally identifiable information about an End-User beyond the information provided for in the Interface Specification.

5. Enforcement

5.1. Dispute Resolution
Every Approved Party agrees to attempt in a timely manner to resolve any dispute arising out of or related to the application of these Business Rules or the Participation Agreement executed by that Approved Party in good faith with the other disputants and parties related to the dispute. Each such dispute, the date and successful or attempted resolutions, including changes in policy, practices or technology implementation, shall be reported to the GSA in a timely manner.

To the extent that information identified in this Section constitutes Personally Identifiable Information within a System of Records under the Privacy Act of 1974[33], nothing in this section or any sub-section shall be construed to authorize or permit the communication of such information about an End-User without that End-User's informed consent.

In the event parties to a dispute are unable, despite their best good faith efforts, to resolve a dispute among themselves, any party may request GSA investigate the dispute potentially leading to Recourse for the aggrieved party.

5.2. GSA Investigation
GSA shall respond to every request to investigate a dispute in a timely manner. GSA may request additional information from one or more parties to the dispute.

5.2.1. Federation Participant Request for Investigation
In the event good faith efforts to resolve a dispute are not successful among the disputants and other parties, any Participant in the E-Authentication Federation may request that GSA investigate the matter, propose a resolution and, if necessary arbitrate a resolution of the matter. Each such request must be accompanied by a full report of all the relevant information related to the dispute.

5.2.2. GSA Initiated Investigation
GSA may initiate an investigation based upon the request of any Participant in the EAuthentication Federation, or may initiate an investigation whenever it deems appropriate based on any information it regards as relevant and credible. Without limitation, such information may include reasonable suspicion that an Approved Party is not in compliance with continuing obligations required under these Business Rules.

5.3. Recourse
Based upon the results of its investigation and in accordance with the E-Authentication Federation Participation Suspension Policy[34], and only under extraordinary circumstances necessary to prevent or cease serious harm to the E-Authentication Federation, the GSA may suspend participation of any Participant in the E-Authentication Federation or render inaccessible any Architectural Component of the Federation by one or more Participants. If the result of an Investigation indicates that an Approved Party is not in compliance with any requirement included directly or by reference under these Business Rules, GSA may require such additional audit, re-Certification or Certification at different Levels of Assurance, to the extent necessary to prevent or cease serious harm to the Federation.

6. General Legal Terms

6.1. Limitation Of Liability
Recourse against the United States for damage caused by negligence of a government employee is controlled by the Federal Tort Claims Act[35], 28 USC Section 1346 et seq. A non-governmental Approved CSP operating in accordance with the terms of the CSP Participation Agreement and these Business Rules may assert the government contractor defense to tort claims arising under the CSP Participation Agreement and these Business Rules.

There shall be no Recourse for any claim arising out of or in relation to use of or reliance upon an Approved Credential or the E-Authentication Federation against any Approved Party under any theory of liability, beyond the Recourse available under the Federal Tort Claims Act[36], unless agreed by contract among the relevant parties.

6.2. Governing Law
These Business Rules and any related materials governing the E-Authentication Federation shall be construed and adjudicated according to the laws of the United States of America.

6.3. Order of Precedence
In the event of a conflict between the terms of various E-Authentication Federation related documents, each such document shall be accorded the following order of priority: the Participation Agreement shall be construed to prevail over conflicting terms of any other E-Authentication Federation document, followed in order of precedence by the terms of these Business Rules, followed by the terms of any normative document listed in Section 4.1.2 of these Rules, followed by the terms of any other policies, agreements or other materials formally promulgated for the purpose of documenting legal terms governing participation in the E-Authentication Federation.

6.4. Assignment, Succession and Bankruptcy
No Approved Party may sell, rent, lease, sublicense, assign, grant a security interest in or otherwise transfer any right and/or obligation contained in these Business Rules or the Participation Agreement executed by that Approved Party, except as permitted herein. Any Approved Party may request of GSA permission for assignment or succession to a different party, including a creditor of the Approved Party, of part or all of the rights and/or obligations contained in these Business Rules or the Participation Agreement executed by that Approved Party.

6.5. Severability
If any provision, set of provisions or part of a provision of these Business Rules is held to be unenforceable or otherwise invalid in whole or in part, the remaining provisions shall remain in full force and effect and shall be construed to the maximum extent practicable as a consistent and reasonable entire agreement.

6.6. Counterparts
These Business Rules may be executed as an agreement simultaneously in one or more counterparts, each of which shall be deemed to be an original, but all of which together shall constitute one and the same instrument.

6.7. Waiver
Neither party's failure to enforce strict performance of any provision of these Business Rules will constitute a waiver of a right to subsequently enforce such a provision. No written waiver shall constitute, or be construed as, a waiver of any other obligation or condition of these Business Rules.

6.8. Responsibility For Taxes, Expenses
Each Approved Party agrees that it is solely responsible for the payment of taxes or expenses incurred by that Approved Party arising out of or related to participation in the EAuthentication Federation.

7. Interpretation and Amendment
The terms of these Business Rules shall be interpreted by the GSA so as to avoid conflict or inconsistencies between the various provisions and between these Business Rules, applicable Participation Agreements and other relevant E-Authentication Federation materials. These Business Rules may be amended according to the E-Authentication Federation Business Rules Amendment Process[37], however no such amendment shall go into legal effect earlier that 90 days from the time notice is afforded to Approved Relying Parties and Approved CSPs. Notice may be provided of amendment to these Business Rules and other matters related to the operation of the E-Authentication Federation by electronic mail to the contact person(s) indicated for each

Approved Party and by posting to the E-Authentication Federation web site.

Appendix 1
E-Authentication Federation
CSP Participation Agreement

Version 1.0, 2004-NOV-23

Drafted by Daniel Greenwood. Esq.
[personal email and telephone redacted in public draft and replaced by URL]
http://www.civics.com

1. Recitals
This Participation Agreement constitutes the legal basis for an organization to become a Credential Service Provider (CSP) within the E-Authentication Federation.

2. Parties
The parties to this Participation Agreement are the General Services Administration of the United States federal government (GSA) and _____ (CSP).

3. Agreement to Abide by Business Rules
By signing this Participation Agreement, the CSP agrees to abide by the E-Authentication Federation Business Rules, as in effect during the period of CSP participation in the EAuthentication Federation, and which are expressly incorporated into and make a part of this Agreement.

4. Dispute Resolution: Notice, Investigation, Resolution and Recourse
CSP agrees that the E-Authentication Business Rules Dispute Resolution and Recourse provisions cover issues between Approved CSPs and Relying Parties operating in the Federation. Any dispute resolution process and rules between the CSP and an End-User must be defined and pursued between the CSP and the End-User, and such terms are not within the scope of the Business Rules of this Participation Agreement.

5. Termination and Suspension
The terms of this Participation Agreement and the Business Rules cease to apply to any CSP as of the effective date of termination of Participation in the E-Authentication Federation.

5.1. Voluntary
Participation in the E-Authentication Federation may be terminated by CSP through written notice to GSA, to avoid the imminent effect of amended language to the Business Rules. Such notice shall be effective no less than 30 calendar days from the date of receipt by GSA. Participation in the E-Authentication Federation may be terminated by mutual agreement between the GSA and CSP.

5.2. Involuntary
GSA may suspend the participation of CSP in the E-Authentication Federation, in accordance with the E-Authentication Federation Participation Suspension Policy[38], under extraordinary circumstances necessary to prevent or cease serious harm to the E-Authentication Federation. GSA may terminate the participation of CSP in the E-Authentication Federation in writing for cause, including breach by the CSP of the terms of this Participation Agreement or the Business Rules.

6. Confidentiality and Non-Disclosure
GSA agrees to execute any reasonable confidentiality and/or non-disclosure agreements with the CSP that may be required as a condition of accepting credentials of that CSP and according to the Business Rules. GSA further agrees to require consent to the relevant terms of such agreements by any Relying Party to whom the terms may apply.

7. Legal Terms

7.1. Limitation Of Liability
Recourse against the United States for damage caused by negligence of a government employee is controlled by the Federal Tort Claims Act[39], 28 USC Section 1346 et seq. A non-governmental Approved CSP operating in accordance with the terms of this CSP Participation Agreement and the E-Authentication Federation Business Rules may assert the Government Contractor Defense to tort claims arising under this CSP Participation Agreement and the E-Authentication Federation Business Rules.

There shall be no Recourse for any claim arising out of or in relation to use of or reliance upon an Approved Credential or the E-Authentication Federation against any Approved Party under any theory of liability, beyond the Recourse available under the Federal Tort Claims Act[40], unless agreed by contract among the relevant parties.

7.2. Governing Law
This CSP Participation Agreement and any related materials governing the E-Authentication Federation shall be construed and adjudicated according to the laws of the United States of America.

7.3. Integration and Order of Precedence
This CSP Participation Agreement and the E-Authentication Federation Business Rules constitute the entire agreement of the parties with respect to participation in the EAuthentication Federation. In the event of a conflict between the terms of various EAuthentication Federation related documents, documents shall be accorded the following order of priority: This CSP Participation Agreement shall be construed to prevail over the terms of any other document, followed in order of precedence by the terms of the EAuthentication Federation Business Rules, followed by the terms of any other policies, agreements or other materials formally promulgated for the purpose of documenting legal terms governing participation in the E-Authentication Federation.

7.4. Assignment, Succession and Bankruptcy
CSP agree it may not sell, rent, lease, sublicense, assign, grant a security interest in or otherwise transfer any right and/or obligation contained in this CSP Participation Agreement or the E-Authentication Federation Business Rules except as permitted herein. CSP may request of GSA permission for assignment or succession to a different party, including a creditor of the CSP, of part or all of the rights and/or obligations contained in this CSP Participation Agreement or the E-Authentication Federation Business Rules. Any prohibited assignment shall be null and void.

7.5. Severability
If any provision, set of provisions or part of a provision of this CSP Participation Agreement is held to be unenforceable or otherwise invalid in whole or in part, the remaining provisions shall remain in full force and effect and shall be construed to the maximum extent practicable as a consistent and reasonable entire agreement.

7.6. Responsibility For Taxes, Expenses
CSP agrees that it is solely responsible for the payment of taxes or expenses incurred by the CSP arising out of or related to participation in the E-Authentication Federation.

8. Amendment
This Participation Agreement may be amended by agreement of the parties, reflected by a signed writing.

9. Signatures

_____ _____

CSP *GSA*

Appendix 2
E-Authentication Federation
Relying Party Participation Agreement

Version 1.0, 2004-NOV-23

Drafted by Daniel Greenwood. Esq.
[personal email and telephone redacted in public draft and replaced by URL]
http://www.civics.com

1. Recitals
This Relying Party Participation Agreement constitutes the legal basis for an organization to become a Relying Party within the E-Authentication Federation.

2. Parties
The parties to this Participation Agreement are the General Services Administration of the United States federal government (GSA) and _____ (Relying Party).

3. **Agreement to Abide by Business Rules**
By signing this Participation Agreement, the Relying Party agrees to abide by the EAuthentication Federation Business Rules, as in effect during the period of participation in the EAuthentication Federation, and which are expressly incorporated into and make a part of this Agreement.

4. Compliance With Requirements
Relying Party agrees that satisfactory completion of the GSA Relying Party Requirements Document, including confirmation of required privacy, regulatory compliance and technical practices, is a pre-requisite to participation in the E-Authentication Federation and must be finalized approval for inclusion in the E-Authentication Federation. Relying Party agrees to maintain continuing compliance with the requirements and other terms contained in the EAuthentication Federation Business Rules, including compliance with the technical, policy and procedural documents incorporated by reference in the E-Authentication Federation Business Rules.

5. Dispute Resolution: Notice, Investigation and Resolution
Relying Party agrees that the E-Authentication Business Rules Dispute Resolution and Recourse provisions cover issues between Approved CSPs and Relying Parties operating in the Federation. Any dispute resolution process and rules between the Relying Party and an End-User must be defined and pursued between the Relying Party and the End-User, and such terms are not within the scope of the Business Rules of this Participation Agreement.

6. Termination and Suspension
The terms of this Participation Agreement and the Business Rules cease to apply to any Relying Party as of the effective date of termination of Participation in the E-Authentication Federation.

6.1. Voluntary
Participation in the E-Authentication Federation may be terminated by written notice to GSA, to be effective no less than 30 calendar days from the date of receipt by GSA. Participation in the E-Authentication Federation may be terminated by mutual agreement between the GSA and Relying Party.

6.2. Involuntary
GSA may suspend the participation of any Relying Party in the E-Authentication Federation in accordance with the E-Authentication Federation Participation Suspension Policy[41], and only under extraordinary circumstances necessary to prevent or cease serious harm to the EAuthentication Federation.

7. Confidentiality and Non-Disclosure
Relying Party agrees to execute any reasonable confidentiality and/or non-disclosure agreements participating CSPs may require as a condition of accepting credentials of that CSP and according to the Business Rules.

8. Liability
There shall be no Recourse for any claim arising out of or in relation to use of or reliance upon an Approved Credential or the E-Authentication Federation against any Approved Party under any theory of liability, beyond the Recourse available under the Federal Tort Claims Act[42], unless agreed by contract among the relevant parties.

9. Amendment
This Participation Agreement may be amended by agreement of the parties, by a signed, writing.

10. Signatures

_____ _____
Relying Party *GSA*
14

Appendix 3
E-Authentication Federation Business Rules Amendment Process
Version 1.0, 2004-NOV-23

The E-Authentication Federation Business Rules may by amended according to the following process. Any Approved CSP or Relying Party may certify a request for consideration of a proposed Amendment of the Business Rules to the GSA, including the reasons therefor and proposed amended language. Any such proposed Amendment shall trigger the Consultative Amendment Process, defined below. The GSA may also propose an Amendment triggering the Consultative Amendment Process.

Consultative Amendment Process
Notice of a proposed Amendment requested by an Approved Party, no later than 30 days from the time the request is received by the GSA, shall be communicated to each Approved Party in the E-Authentication Federation for consideration and comment, Said notice shall be delivered by e-mail to the named contact person(s) in the Participation Agreements of the Approved Parties and may also be posted to the official E-Authentication Federation web site. A period of not less than 30 days shall be afforded Approved Parties to consider, comment upon and, at their discretion, indicate agreement with, disagreement with and/or alternative proposed language to the GSA. The GSA may hold one or more consultative meetings of interested Approved Parties to discuss any proposal and may extend the period for consideration and comment, as needed to accommodate the needs of the parties.

Disposition of Amendment Proposal
No more than 10 days after the period for consideration and comment has closed, the GSA shall communicate to each Approved Party notice of the disposition of the proposal, including whether the proposal has been rejected and no Amendment will be pursued, or the proposal has been modified, or the proposal has been accepted. Said notice shall be delivered by e-mail to the named contact person(s) in the Participation Agreements of the Approved Parties and may also be posted to the official E-Authentication Federation web site. If the proposal is modified, the modified proposal shall trigger a new Consultative Process, defined above. If the proposal is accepted, it shall trigger the Amendment Incorporation Process
defined below.

Amendment Incorporation Process
An Amendment that has been accepted after a Consultative Amendment Process according to the notice provisions specified in the Disposition of Amendment Proposal process shall go into legal effect no less than 90 days from the date notice has been sent, or such later time as specified in the notice. Any Approved Party may terminate participation in the E-Authentication Federation no less than 30 days from the time of sending notice of termination to the GSA according to the Business Rules, and in every case reserves the right to terminate participation prior to any Amendment coming into full force and effect.

Appendix 4

General Overview

Version 1.0, 2004-NOV-23

The E-Authentication Federation is designed to allow electronic access to government services by examining electronic credentials to verify the End-User's identity. This Federation is run by the General Services Administration of the U.S. Federal Government under the name of the EAuthentication Initiative. The E-Authentication Initiative is one of twenty-four Electronic Government (E-Gov) services from the President's Management Agenda, which is intended to improve interfaces between citizens, businesses, and all levels of government.

The credentials may be issued by government agencies, but may also be issued by commercial entities for this purpose or for other purposes. In those cases, the E-Authentication Federation would be providing for reliance on commercially-issued, re-usable credentials. The EAuthentication Federation, including public and private organizations, uses such credentials along with a common technical, policy and legal infrastructure. These Business Rules, and the related Participation Agreements form the cornerstone of the legal aspect of the infrastructure. The Federal Government, in order to support the electronic government initiatives, is undertaking the E-Authentication initiative to allow for federation of identity and creating federation for the government and other entities so that citizens can authenticate to the government. The EAuthentication Federation requires policy and technology infrastructure as well as business rules and participation agreements. The technology infrastructure includes Architectural Components such as a validation service, a discovery portal, a step-down translator and a protocol translator. These components make it possible for parties using different technologies to federate identities from one organization to another. The E-Authentication Federation is the authentication component of the federal enterprise architecture.

The E-Authentication Federation has these key participants: Credential Service Providers (CSPs), End-Users, Relying Parties who are operating Agency Applications (RPs), and the General Services Administration of the U. S. Government, who acts as the administrative, operational, and policy arm of the E-Authentication Federation. End-Users, who will use credentials to access Agency Applications may be government employees or contractors or private citizens who are affiliated with one or more CSPs. That affiliation could include a customer, employee or partnership relationship. Relying Parties may include government agencies at the Federal, State, or local levels.

Credential Service Providers issue credentials to End-Users, who in turn use those credentials to get access to Government services over the world wide web. The E-Authentication Initiative facilitates this process through its service model, which includes policy services, technology services, and customer service.

The E-Authentication Federation utilizes industry standard technologies, implemented through Commercial Off the Shelf Products (COTS). Use of Approved COTS Software is required of all Approved CSPs, Relying Parties and for all communications occurring through the EAuthentication Federation. A complete explanation of the technical architecture is available in the publication 'Technical Approach for the Authentication Service Component'. The architecture supports the concept of credentials at each of four Assurance Levels, allowing the Relying Party to match their acceptance of credentials to the Risk Assessment they will have completed for their Agency Application. Risk assessment guidance is contained in OMB M-04-04[43]. Guidance for credentials at each of the four assurance levels is contained in NIST SP 800-63[44].

The E-Authentication Federation uses the Security Assertion Markup Language (SAML) and also PKI as enabling technologies allowing for federation of credentials across organizations in both the public and private sectors. Any CSP in the private or public sector issuing credentials that comply with the SAML standard when configured in accordance with the GSA issued Interface Specification can be considered for Approval by GSA to participate in the E-Authentication Federation at Assurance Levels 1 and 2. In

addition, the CSPs operating within the Federal Public Key Infrastructure, PKI Bridge, and issuing credentials under the ACES, FICC, and FPKIPA programs can also be considered for participation at any Assurance Level. Any CSP, whether a provider of SAML or PKI based credentials, must execute a Participation Agreement legally binding it to the E-Authentication Business Rules in order to be Approved for participation. Other technical standards and specifications may be accepted for use within the E-Authentication Federation as they become available at the sole discretion of the GSA.

Both CSPs and RPs will need to meet a number of requirements for participation in the EAuthentication Federation. Guidance on these requirements is contained in documents published by the GSA including E-Authentication Handbook for Federal Government Agencies, EAuthentication Handbook for Credential Service Providers, and the E-Authentication Cookbook. The GSA evaluates the qualifications of potential participants, assists them in matriculating through the qualification, testing, and activation process, and maintains oversight of the EAuthentication Federation operation. In addition, the GSA operates a conformance testing service for COTS products, an interoperability testing service, and runs some technical services that are designed to lessen the technical burden on the participants.

These Business Rules are intended to define the legal terms and overall structure, including roles and obligations governing participation in the E-Authentication Federation. CSPs and Relying Parties sign Participation Agreements which obligate them to the terms of these rules as well as the policies of the GSA. End-Users, while considered participants, do not sign Participation Agreements directly with GSA. Rather, End-Users sign agreements containing approved E-Authentication Federation terms with the CSP who has issued and Approved Credential to that user. Details of operational processes are contained in GSA documents, including the ones referenced above, and many more that are relevant to various aspects of EAuthentication Federation participation, such as interoperability testing. Documents are available through the E-Authentication Federation website at http://www.cio.gov/eauthentication/

The following diagram illustrates the organizations which oversee the E-Authentication Federation within the US Government, and the major areas of responsibility for both policy (within the Office of Government-wide Policy) and operations (within the Project Management Office or PMO) for the E-Authentication Federation.

Federal E-Authentication Initiative Overview

In 2001, President Bush initiated several government reform efforts, collectively known as the President's Management Agenda (PMA). The five government-wide efforts focus on Strategic Management of Human Capital, Competitive Sourcing, Improved Financial Performance, Expanded Electronic Government, and Budget and Performance Integration. The Chief Information Officers (CIOs) of the federal agencies have a major role in the achievement of the PMA goals. They lead the implementation of many of the programs that help expand electronic government and provide support to others.

CIO Council contributed to several government-wide initiatives, focusing on reducing costs and improving services to citizens. To facilitate efforts to transform the Federal Government the Office of Management and Budget (OMB) is developing the Federal Enterprise Architecture (FEA), a business-based framework for Government-wide improvement.

Operating under the authority of the OMB, the General Services Administration (GSA) is responsible for the Federal government’s electronic authentication effort. Whether through electronic authentication evolution or historical events the Federal Enterprise Architecture is a combination of pre-PMA and new efforts. The Federal government established several significant efforts related to electronic authentication, prior to creation of the Electronic Authentication Initaitive. These efforts include Federal Pubic Key Infrastructure (FPKI), Access Certificates for Electronic Services (ACES), Federal Identity Credentialing Committee (FICC). The E-Authentication Initiative (EAI) provides for incorporation of these prior efforts into the e-Authentication Federation...

Federal e-Authentication Diagram

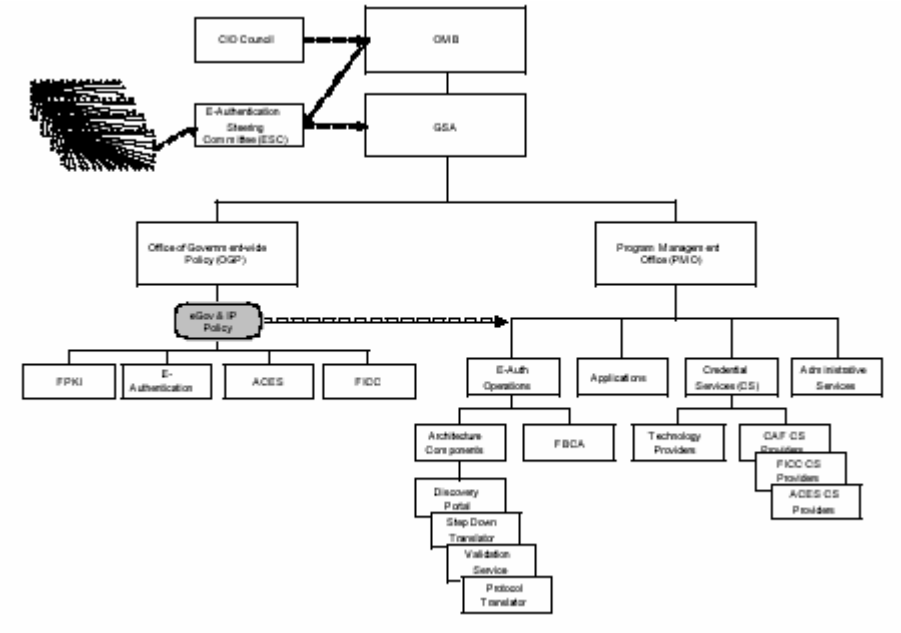


Diagram 1

The Federal authentication architecture is basically divided into two functional areas, policy and operations. Within both policy and operations there are various initiatives to meet the diverse demands of the government. These include historical agency authentication services, various levels of identity assurance, private sector COTS, technical interoperability, and compliance. Please note that this overview uses terms that are not defined and does not use every defined term according it its formal definition. Rather, the document was written for readability and to provide an informal basis to generally understand the overall initiative at a glance.

Appendix 5

E-Authentication Business Rules Glossary

Version 1.0, 2004-NOV-23

Agency Application
A computer applications of a Relying Party that is uniquely identifiable when used within the E-Authentication Federation.

Approved
Authorization or other acceptance by the GSA for purposes of participation or other inclusion or use in the E-Authentication Federation.

Approved Credential
A Credential issued by a Certified Credential Service of an Approved Credential Service Provider to an End-User.

Approved Credential Service Provider (Approved CSP)
A Credential Service Provider that has been approved by the GSA to participate in the EAuthentication Federation.

Approved Parties
Any Approved Relying Party and Approved Credential Service Provider.

Approved Relying Party
A Relying Party that has been approved by the GSA to participate in the E-Authentication Federation.

Certified Credential Service
A Credential Service judged to meet the requirements identified in the Credential Assessment Framework Suite.

Credential
Digital information used in authentication and access control that bind an identity or an attribute to an End-User's Token or some other property such as his or her current network address. Note that this glossary distinguishes between Credentials, and Tokens while other documents may use the terms interchangeably.

Credential Service
A service of a Credential Service Provider that provides credentials to subscribers for use in electronic transactions. If a Credential Service Provider offers more than one type of credential then each one is considered a separate Credential Service.

Credential Service Provider
An organization that offers one or more Certified Credential Services, also known in this document as a CSP.

End-User
An individual person that has been issued an Approved Credential by an Approved Credential Service Provider and who communicates through the E-Authentication Federation with an Approved Relying Party and whose identity is verifiable with reference to that Credential.

Informed Consent
Consent voluntarily signified by an End-User who is competent and who understands the terms of the consent and who has been provided in a clear statement with the appropriate knowledge needed to freely

decide without the intervention of any element of force, fraud, deceit, duress, over-reaching or other ulterior form of constraint of coercion.

Levels of Assurance
Four level of authentication defined based upon consequences of a false positive authentication or misuse of a Credential. These levels are documented in OMB Memorandum M-04-04.

Participant
Any Approved Relying Party, Approved Credential Service Provider or End-User.

Relying Party
A party that relies upon a Credential issued by a Credential Service Provider.

Relying Party Requirements Document
This document contains the checklist of items necessary for a Relying Party to be approved by GSA for participation in the E-Authentication Federation.

Rule
A provision or term of the E-Authentication Business Rules.

Security Assertion Markup Language (SAML)
The XML Schema specified by the open standards organization OASIS-OPEN defining a standard framework for creating and exchanging security information between online partners. The specification, and other information provided by the authoring technical committee, may be found at: http://www.oasisopen.org/committees/workgroup.php?wg_abbrev=security.

Technology Architecture Components
Inclusive of the portal defined in the E-Authentication Federation Technology Architecture, the step-down translator, validation services and the protocol translator.

Token
Something that the End-User possesses or knows (typically a key or password) that can be used to remotely authenticate the claimant's identity. Technically, the Token includes a userid and password that ensures Token uniqueness within a Credential domain.

Appendix 6

E-Authentication Business Rules Endnotes

Version 1.0, 2004-NOV-23

[1] **Credential Assessment Framework Suite (CAF)**
The GSA published documents defining a process for the Certification of Credential Services of Credential Service Providers, including the Interim PKI Credential Assessment Profile, Interim Password Credential Assessment Profile, Interim PIN Credential Assessment Profile, Interim Credential Assessment Framework, Interim Credential Assessment Guidance and Interim Common Credential Assessment Profile. This suite of documents collectively can be found at http://cio.gov/eauthentication/CredSuite.htm.

[2] **E-Authentication Federation Trusted Credential Service Provider List**
The list of Certified Credential Services and their associated Levels of Assurance. This list is published at http://cio.gov/eauthentication/TCSPlist.htm.

[3] **U.S. Federal Enterprise Architecture**
A business and performance-based framework to support cross-agency collaboration, transformation, and government-wide improvement, including reference models for business, service components, data, and a technical reference model. Information about this architecture, and the architecture itself, can be found at: http://www.feapmo.gov/.

[4] **President's Management Agenda**
A collection of government reform efforts initiated in 2001 including strategic management of human capital, competitive sourcing, improved financial performance, expanded electronic government and budget and performance integration. Information about these initiatives can be found at: http://www.cio.gov/documents/CIO_Council_Strategic_Plan_FY04.pdf.

[5] **OMB Memorandum M-04-04**
This document is published by OMB regarding e-authentication guidance for federal Agencies. This document can be found at: http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf.

[6] **NIST SP 800-63**
This document is published by the National Institute of Standards and Technology entitled Electronic Authentication Guideline. This document can be found at: http://cio.gov/eauthentication/documents/SP800-63V6_3_3.pdf.

[7] **E-Authentication Federation Business Rules Amendment Process**
Definition of the circumstances and procedures necessary to formally amend the EAuthentication Federation Business Rules. This document can be found in Appendix 3 of the Business Rules.

[8] See note 1.

[9] **E-Authentication Federation Technical Architecture**
Suite of documents defining required implementations and configurations of technology for use in the E-Authentication Federation, including the Interface Specification relevant to use of SAML and path discovery and validation requirements relevant to PKI. This suite of documents can be found at: http://cio.gov/eauthentication/TechSuite.htm.

[10] **Interface Specification**
Interface specifications for the SAML Artifact Profile for use in the E-Authentication Federation. This document can be found at: http://cio.gov/eauthentication/documents/SAMLspec.pdf.

[11] See note 2.

[12] See note 9.

[13] See note 10.

[14] **Approved Communication Software**
Software approved by the GSA for communications through the E-Authentication Federation. The list of such software, along with the technology providers of those

products, can be found at:
http://www.cio.gov/eauthentication/documents/ApprovedProviders.htm
[15] See note 14.
[16] **OMB Circular No. A-130**
This document is published by OMB regarding the management of federal information resources. This document can be found at:
http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html.
[17] **OMB Circular No. A-130, Appendix III**
This document is published by OMB regarding security of federal automated information resources. This document can be found at:
http://www.whitehouse.gov/omb/circulars/a130/a130appendix_iii.html.
[18] **Privacy Act of 1974**
Federal legislation defining allowed federal collection, use or dissemination of personal information. This legislation may be cited as 5 USC § 552a, and can be found at:
http://www.law.cornell.edu/uscode/html/uscode05/usc_sec_05_00000552---a000-.html.
[19] **OMB Memorandum M-03-22**
This document is published by OMB regarding guidance for implementing the privacy provisions of the e-government act of 2002. This document can be found at:
http://www.whitehouse.gov/omb/memoranda/m03-22.html.
[20] See note 5.
[21] See note 6.
[22] See note 9.
[23] See note 10.
[24] See note 2
[25] See note 1.
[26] See note 1.
[27] See note 9.
[28] See note 18.
[29] **E-Authentication Federation Participation Suspension Policy**
A policy defining the extraordinary circumstances under which an Approved Party may have participation in the Federation suspended. As of the date of publication of version 1 of the E-Authentication Business Rules, this document is not yet finalized.
[30] See note 9.
[31] See note 1.
[32] See note 9.
[33] See note 18.
[34] See note 29.
[35] **Federal Tort Claims Act**
Federal legislation defining U.S. Federal Government liability under tort law. This legislation may be cited as 28 USC § 1346 et seq. and can be found at:
http://www.law.cornell.edu/uscode/html/uscode28/usc_sup_01_28_10_VI_20_171.html.
[36] See note 35.
[37] See note 7.
[38] See note 29.
[39] See note 35.
[40] See note 35.
[41] See note 29.
[42] See note 35.
[43] See note 5.
[44] See note 6.