

# Burton Group Report on the Federal E-Authentication Initiative

*August 30, 2004*

**Authors:** Daniel Blum, Gerry Gebel, Doug Moench

**FINAL**

## Table of Contents

|     |  |    |
|-----|--|----|
| 1   | Executive Summary .....  | 4  |
| 2   | Introduction .....   | 8  |
| 2.1 | Audience, Scope, Methodology .....                                       | 8  |
| 2.2 | Authentication, Identity Management, and Federated Identity .....        | 8  |
| 2.3 | E-Authentication Initiative Goals .....                                  | 10 |
| 2.4 | Electronic Authentication Partnership (EAP) Goals.....                   | 10 |
| 2.5 | E-Authentication Initiative Background.....                              | 11 |
| 2.6 | Business Drivers for E-Authentication and Federated Identity .....       | 14 |
| 3.  | Federated Identity Management: An Industry Analysis .....                | 15 |
| 3.1 | Specifications and Standards.....  | 15 |
| 3.2 | Industry Adoption of Federated Identity .....                            | 17 |
| 3.3 | Enabling Conditions .....  | 19 |
|     | Interoperability .....   | 19 |
|     | Trust and Business Relationships.....                                    | 20 |
| 4   | Analysis - The E-Authentication Initiative.....                          | 23 |
| 4.1 | E-Authentication Technical Architecture and Interoperability .....       | 23 |
|     | Technical Architecture Overview .....                                    | 24 |
|     | Portal Service .....   | 24 |
|     | Validation Service .....   | 26 |
|     | Scheme Translation Service .....   | 26 |
|     | Technical Architecture and Interoperability: Findings .....              | 27 |
|     | Technical Architecture and Interoperability: Future Considerations ..... | 30 |
| 4.2 | E-Authentication Trust Model .....                                       | 34 |
|     | Trust Model Overview .....   | 34 |
|     | Policy - Authentication Levels.....                                      | 34 |
|     | Policy - Authentication Mechanisms.....                                  | 35 |
|     | Key Management and Credentialing Policy .....                            | 36 |
|     | Governance .....   | 37 |
|     | Assessment Framework, Criteria, and Methodology.....                     | 37 |
|     | Trust Model - Findings.....  | 38 |
|     | Trust Model - Future Considerations.....                                 | 38 |
| 4.3 | Other E-Authentication Critical Success Factors.....                     | 41 |
| 5   | Electronic Authentication Partnership Analysis .....                     | 43 |
| 5.1 | Electronic Authentication Partnership Trust Model Overview .....         | 43 |
|     | Assurance Levels.....  | 43 |
|     | Business Rules and Agreements .....                                      | 44 |
|     | Assessment Framework, Criteria, and Methodology.....                     | 45 |
|     | Evaluation, Accreditation and Compliance .....                           | 45 |
|     | Governance .....   | 46 |
| 5.2 | EAP Trust Model - Findings .....   | 47 |
| 5.3 | EAP Trust Model - Future Considerations.....                             | 49 |

|   |    |
|---|----|
| 5.4 Other Critical Success Factors for the EAP.....                     | 51 |
| 6 Recommendations .....   | 54 |
| 6.1 Recommendations for the E-Authentication Initiative.....            | 54 |
| Near Term Recommendations .....   | 54 |
| Longer Term Recommendations .....                                       | 58 |
| 6.2 Recommendations for the Electronic Authentication Partnership ..... | 61 |
| Near Term Recommendations .....   | 61 |
| Longer Term Recommendations .....                                       | 62 |
| 7 Conclusion .....  | 64 |
| 8 References .....  | 65 |
| 9. Appendix A: Authentication, Identity Management, and Federation..... | 66 |
| 10. Appendix B: Federated Identity Specifications and Standards .....   | 70 |
| SAML .....  | 70 |
| Liberty Alliance Project.....   | 71 |
| Shibboleth.....   | 73 |
| WS-Security and WS-* .....  | 73 |
| SAML 2.0 and the Convergence of Standards .....                         | 74 |

# 1 Executive Summary

The General Services Administration (GSA) has engaged Burton Group to perform an independent program review of the E-Authentication Initiative's technical architecture, interoperability, and trust characteristics as well as the related Electronic Authentication Partnership (EAP). Burton Group reviewed the E-Authentication vision, plans, and technical approach and also interviewed a number of key stakeholders to arrive at the findings and recommendations which are included within this report. These findings and recommendations consider over-arching critical success factors for E-Authentication as well as the technical characteristics in scope.

The E-Authentication Initiative is one of twenty-five Electronic Government (E-Gov) services from the President's Management Initiative, which is intended to improve interfaces between citizens, businesses, and all levels of government. E-Authentication is also the first component of the Federal Enterprise Architecture (FEA), and was formally adopted as inter-agency guidance in December 2003. A government-wide operational pilot infrastructure is in place as of July 2004 with multiple Agencies participating, and E-Authentication is authorized to go live for production use in October, 2004.

The E-Authentication Initiative standardizes levels of authentication assurance, assessment of authentication systems for each level, and methods of federated authentication between organizations. Federated authentication is part of federated identity management; it allows organizations to rely on digital credentials issued by partner organizations even if partners deploy different authentication technologies, such as passwords or public key infrastructure (PKI). Federated authentication attains interoperability by specifying the exchange of standards-based authentication assertion formats, scales well to nationwide or Internet-wide use, and is seeing growing adoption. However, considerable effort is still required to broker trust relationships within or between federations, and to assure interoperability between products. The E-Authentication Initiative is doing what is necessary to create a government-wide federation that also includes industry partners and citizens.

The Electronic Authentication Partnership (EAP) is a government/industry collaborative effort whose goals are to provide organizations with a straightforward means of federated authentication without requiring bilateral agreements. Instead, any party operating under EAP rules agrees to follow those rules, resulting in multilateral trust among all participants. While initially

founded with financial support from government, the EAP plans to complete its specifications framework and establish itself as a formal, member-supported organization by the end of 2004. If successful, EAP could considerably advance federations industry-wide. EAP could also promote efficient identity management technology markets and services that might eventually reduce the Federal E-Authentication Initiative's current assessment, testing, and other burdens.

The E-Authentication Initiative's goals are achievable. The anticipated benefits are real and far-reaching, and extend to end-users, governmental organizations, and commercial businesses alike. The E-Authentication Initiative is well-defined, flexible, technically sound, and employs industry best practices such as:

- Supporting a variety of industry standards over time
- Utilizing vendor-supported, Commercial Off-The-Shelf (COTS) software
- Gaining buy-in from Agency stakeholders, conducting a number of operational pilots, and incorporating lessons learned into the program
- Ensuring interoperability through the establishment and ongoing operation of an advanced testing facility
- Promoting collaboration of government and commercial organizations through the EAP
- Reusing existing government investment in the Federal PKI bridge
- Tracking program milestones and performance measures in a Strategic Business Plan

As the E-Authentication Initiative evolves, the government should expect to face an increasing number of challenges, as will other large federations. In the short term, current Agency pilots must be successfully transitioned to production, new projects should begin, and the Office of Management and Budget (OMB) should actively promote E-Authentication support. Progress must be made on engaging commercial Credential Service Providers (CSPs), and on establishing business rules and contract terms for federation between government and industry organizations. New standards and more advanced technologies will emerge that must be supported, inter-organizational privacy issues will need to be addressed, interoperability testing will become more complex and costly, and more efficient methods will be required for establishing and re-assessing trust relationships dynamically. And while the E-Authentication Initiative has appropriately contained its focus on federated authentication using passwords, personal identification numbers (PINs), PKI, and Security Assertion Markup Language 1.0 (SAML 1.0) for now, Agency applications and CSPs have additional identity management or authorization needs that should be addressed through common approaches or guidelines. Although E-Authentication is addressing some of

these issues, others will eventually require modifications to the program scope as well as its underlying policy and trust framework.

Almost any well-managed and well-conceived common authentication solution is preferable to a fragmented and uncoordinated approach. If the E-Authentication Initiative continues to be well-managed and passes unscathed through election period organizational transitions, it seems assured of achieving a significant degree of success. However, the program will be even more successful if it gradually expands its scope to address additional identity management needs and continues to consolidate initial successes in proactively promoting industry participation and alignment.

The full set of recommendations for the E-Authentication Initiative to address its challenges and opportunities includes:

- Near term recommendations
  - Update the Strategic Business Plan with a focus on increasing Agency adoption and involving commercial CSPs
  - Mitigate risks that could lead to breaches through tight security and well-defined business and operating rules
  - Continue communicating the E-Authentication Initiative's efforts and successes
  - Involve state applications, CSPs, and other entities outside of the Federal Agency framework
  - Continue to support and promote the EAP
  - Refine and improve audit and accreditation programs based on industry input
  - Define business rules, operating agreements, and contract terms for working with commercial CSPs and relying parties
- Longer term recommendations
  - Enhance support for application and identity lifecycle requirements while taking a proactive approach on privacy
  - Add additional standards to the roadmap, converging on SAML 2.0 over a 2-3 year time frame
  - Develop requirements for scheme translators jointly with industry, to allow modular adaptation to future standards
  - Continue interoperability testing efforts
  - Develop more options for higher assurance authentication, especially for non-Government users

From the Government's standpoint, EAP represents an excellent opportunity to extend the effectiveness of the E-Authentication Initiative. But the EAP

framework will take time to mature and will not provide a panacea for all federated authentication and identity management needs in the near term. The EAP may indeed be successful in establishing interoperable authentication across multiple industries, but to put the framework into practice it must gain buy in and additional specifications from technical standards groups and audit or accreditation groups. Subsequently it must be accepted, adopted, and deployed in multiple trust circles. Even then, many authorization-related trust, liability, and life cycle identity management issues must still be dealt with on an industry-by-industry basis. The E-Authentication Initiative should continue to support and promote EAP, but it will likely require interim business rules and operating agreements for government-to-business (G2B) as well as government-to-citizen (G2C) federations.

The E-Authentication Initiative must also proactively promote broader participation by providing incentives and clearly articulating the business value to potential partners until a critical mass of CSPs and applications are engaged. Outside of the Agencies themselves, state governments, financial institutions, universities, and online service providers represent some of the best partnership opportunities for increasing E-Authentication adoption and generating a “snowball” effect for the program. A more aggressive approach in analyzing business benefits and business models, coordinating initiatives and encouraging participation (via formal encouragement of Agency adoption, incentives for CSPs, or other means) could increase momentum for the E-Authentication Initiative and help obtain critical mass for additional CSP and Agency participation over time across a broad range of Federal, state, and commercial environments.

Notwithstanding the hard work and challenges that lie ahead, the E-Authentication Initiative should be continued with the government’s full support. Federation has become the dominant paradigm for inter-organization authentication. Large-scale infrastructure projects like E-Authentication are required to establish interoperability and trust for large federations. Without E-Authentication, many Agencies would eventually have to establish federations by identifying their own specifications and conducting their own assessment, testing, and industry outreach programs at a much higher cost to the government as a whole. The industry’s schedule for achieving more efficient federation, which is benefiting considerably from E-Authentication today, would be somewhat set back without it. Without a federation capability, many E-Gov and FEA objectives would be more difficult and expensive to reach.

## **2 Introduction**

Improving digital identity management (IdM) is essential to continuing and increasing the social and economic benefits of e-business, electronic government and the Internet. IdM is complex and must balance the varying needs that business, government and the individual have for security, privacy, and convenience. These issues will be with us as a society for the foreseeable future. Yet much progress can and should be made in the next five years, beginning with improved authentication services. Recognizing the opportunity, the U.S. Government has launched an ambitious E-Authentication Initiative. In turn, the E-Authentication Initiative has engaged industry-wide business and technology leaders in a new forum – the Electronic Authentication Partnership (EAP).

### **2.1 Audience, Scope, Methodology**

This report provides an independent program review of the technical architecture, interoperability, and trust characteristics of the E-Authentication Initiative, and a review of the Electronic Authentication Partnership. The intended audience includes technical managers, security professionals and identity management specialists. While the primary audience consists of Federal managers, the report may also be useful to industry partners of the Government.

Burton Group's methodology in producing the report has been to assess the E-Authentication Initiative and the Electronic Authentication Partnership against their stated goals of enabling interoperable authentication. Burton Group leveraged its extensive knowledge and research into authentication, identity management, federation, and trust while also conducting multiple interviews of Federal stakeholders, EAP stakeholders, identity management vendors, and commercial identity service providers to find strengths in the E-Authentication programs, issues, future considerations, critical success factors, and recommendations.

### **2.2 Authentication, Identity Management, and Federated Identity**

Authentication is part of the larger problem of digital identity management (IdM). IdM comprises a complex mix of processes and technologies including authentication, user administration, authorization, directory services, and audit. Through authentication, computers and applications challenge persons (or systems acting on their behalf) to present credentials, or proofs of their physical identity. Once a user is authenticated, systems and applications may authorize the user to perform actions such as reading or writing files, based on access control information such as group memberships or roles associated with the user.

As increased connectivity and e-business have loaded more and more value onto computer applications and the Internet, the need for IdM has mushroomed and the consequences of digital identity abuse have risen with the value of activities and the rise of privacy regulations. Authentication and IdM have been difficult to manage on an enterprise-wide basis because, historically, they are tightly bound to applications, operating systems, or devices. However, in response to the growing importance, complexity and cost of IdM, organizations across the world have for several years been seeking to consolidate silos of IdM in disparate applications into a reduced number of general-purpose systems with higher assurance.

IdM consolidation and integration is the recommended approach for enterprises, including organizations such as individual Federal Agencies. Yet it is not possible or cost effective to aggregate information about all possible users in multi-domain environments such as the Federal government, an industry, or the Internet itself. Nor is there a one size fits all model for the IdM architecture of every enterprise; in many cases it makes sense for different business units (such as bureaus within an Agency) to operate IdM somewhat autonomously from the parent organization.

Thus, while increased connectivity and e-business created the need for IdM consolidation and integration they have also exposed the limits of these approaches and created the need for a third approach: federated identity management both between enterprises, and within enterprises. Federated identity management involves the use of agreements, standards, and technologies to make identity and entitlements portable across loosely coupled, autonomous security domains.

Over the last two years, the concept of federated identity has emerged as a pragmatic and credible solution. The Security Assertion Markup Language (SAML), Liberty Alliance, and WS-Security are already in the early adopter phase of implementation and deployment, across multiple industries. Federated identity is the right architecture for Internet authentication. Moreover, federated identity is essential to enabling Web services. Applications developed with Web services and federated identity leverage loosely coupled interfaces, service oriented architecture (SOA), and eXtensible Markup Language (XML). Each of these characteristics favors component reusability, vendor independence, platform independence, and location independence - federation in the broadest sense.

Although technical standards for federation have emerged, customers and vendors are still in the process of establishing technical interoperability. Also, business issues such as liability, responsibility and risk apportionment are even

more challenging than technical ones in the absence of industry or national level agreements. The E-Authentication Initiative – like any large federation – must work to address these challenges. See [Appendix A](#) for a more detailed overview of authentication, identity management, and federation. Also see [Section 3](#) for a discussion of industry perspectives on federated identity, interoperability, and trust.

### **2.3 E-Authentication Initiative Goals**

The E-Authentication Initiative’s goal is to provide a common authentication infrastructure for electronic government (E-Gov) initiatives including Government-to-Government (G2G), Government-to-Business (G2B), Government-to-Citizen (G2C), and Internal Efficiency and Effectiveness (IEE) applications. E-Authentication is also the first reusable component of the Federal Enterprise Architecture (FEA), whose plan is that the vast majority of Federal systems incorporating authentication functions should migrate to support E-Authentication over time.

The authentication infrastructure must function without a national identifier card, unique national identifier number, or any single centralized registry of personal information, attributes, or authorization privileges. The infrastructure must support different authentication assurance levels required for different types of transactions, and it must comply with the Privacy Act of 1974, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, and Fair Information Principles.

In October, 2003 the E-Authentication Initiative Program Management Office (PMO) obtained consensus within the government to proceed with a federated authentication architecture, as this architecture provides the best foundation for meeting the goals outlined above. Yet although the advent of federated identity standards is changing the IT industry perspective on authentication, federation will not become ubiquitous overnight. Government must work with industry to create the conditions for interoperability and trust.

### **2.4 Electronic Authentication Partnership (EAP) Goals**

The lack of reliable, widespread authentication and identity management solutions in the United States represents a market failure wherein competing economic and social values of security, convenience and privacy have stymied efforts by government and industry alike to provide common solutions. While other nations may choose to adopt government controlled solutions through national identity cards, that solution is off the table in the United States for the indefinite future. At the same time, public and private identity management needs are intricately connected in financial, health, and many other fields.

Neither private industry nor government intervention, alone, can successfully push the market to interoperable authentication in a reasonable timeframe. Industry needs reasonable regulatory or other guidance from government, and industry requires foundational Federal or state physical identity proofing associated with birth, passport, and driver credentialing or licensing. Government requires industry's innovation, economies of scale and appropriate access to privately held credentials and other identity information.

The Electronic Authentication Partnership (EAP) has been established as a government/industry collaboration to provide organizations with a straightforward means of relying on digital credentials issued by a variety of authentication systems. The EAP seeks to eliminate or at least reduce the need for organizations to establish bilateral agreements with each other party upon whose authentication processes they wish to rely. Instead, any party operating under EAP rules would agree to follow those rules, resulting in multilateral trust among all participants.

The EAP is attempting to establish multilateral trust by creating and maintaining common policies and practices for credentials, credential providers and credential processors; developing an evaluation process for credentials, and setting standard approaches and minimum requirements for identity management; and building on or complementing existing credential mechanisms for operating rules and associated processes.

In practice, the EAP will build on a federated identity approach, conceptually similar to the E-Authentication Initiative's approach. EAP could positively impact all online markets, business-to-business (B2B) as well as G2B. The government stands to benefit if it can align its credentialing and accreditation guidelines to those of the EAP, and if additional commercial CSPs come into being through a market driven process and are compatible with E-Authentication or EAP guidelines.

## **2.5 E-Authentication Initiative Background**

The E-Authentication Initiative (also known as the Authentication Service Component of the Federal Enterprise Architecture) demonstrates a clear vision of industry realities by aligning itself with federated identity in general and SAML in particular. The government has also taken bold and pragmatic steps to provide an enabling framework for federated identity interoperability, which at this early stage of industry development cannot be taken for granted. Therefore, E-Authentication provides an enabling framework for federated identity that includes policy, architecture, infrastructure, testing, and trust.

The “Federal Four” authentication levels – low, medium, high, and very high strength – are defined by the [National Institute of Standards \(NIST\) 800-63 special publication](#) and conveyed as Federal policy by the [Office of Management and Budget \(OMB\) Memorandum M-04-04](#). Additional policy documents define risk management guidelines to associate a required level of authentication to applications, and provide a Credentials Assessment Framework (CAF) for evaluating Credential Services Providers (CSPs)<sup>1</sup> to determine whether the identity proofing procedures they use and the credentials they issue can be accredited for any of the specified authentication levels.

E-Authentication also defines a Technical Architecture that leverages federated identity through SAML 1.0, enabling infrastructure components such as a portal that links Agency Applications (AAs)<sup>2</sup> and CSPs, and an Interoperability Test Lab for certifying products as generally compliant with SAML 1.0, compliant with the E-Authentication profile of SAML 1.0, and interoperable with one another. To date, seven products have been approved as interoperable and more are in queue for testing.

E-Authentication has also unified its federation initiative with the preceding Federal PKI (FPKI) work, such that FPKI-compliant credentials can be used at the High and Very High authentication levels. This preserves the progress DoD, NASA, Treasury, USDA/NFC, DOE, and Department of State as well as other entities such as the Government of Canada, State of Illinois, and EDUCAUSE have made through their investment in the Bridge Certification Authority (CA) trust fabric. Meanwhile, FPKI has revised its approach, instituting a policy that additional Federal PKI deployments will be compatible with the Bridge CA, but rooted under a Common Policy CA and provided by accredited PKI service providers. Through recent FPKI changes and the Government Smartcard Initiative, the government has greatly improved and streamlined its approach to PKI. However, FPKI must still achieve interoperability of its specifications with widely used commercial applications, and extend its trust fabric across additional vertical industries to realize its promise.

Recent E-Authentication progress has been impressive, but this does not minimize the challenges that lie ahead. Through these programs the government is tackling the most difficult identity management issues in seeking to enable

---

<sup>1</sup> This document uses the E-Authentication term “Credential Services Provider (CSP)” synonymously with the term Identity Provider (IdP), which is used broadly in the literature.

<sup>2</sup> This document uses the E-Authentication term “Agency Application (AA)” synonymously with the terms “relying party (RP) or “service provider (SP),” which are used broadly in the literature. However, when discussing relying parties that could be hosted by businesses or other non-governmental domains linked through the E-Authentication Initiative, we use the more general term “application.”

interoperability and trust across huge environments while operating within the envelope of federation standards, authentication standards, commercial product availability, and privacy constraints. To succeed, E-Authentication must provide still more support for Agency Applications seeking to meet life cycle identity management needs that cannot be divorced from federated authentication. E-Authentication must also engage with industry to broaden adoption of its interoperability and trust frameworks.

The E-Authentication Initiative has already begun testing or preparing a number of pilot applications to validate various aspects of the E-Authentication service:

- Identity validation at assurance levels 1 and 2 using the SAML 1.0 protocol is being demonstrated in pilots with Grants.gov and eTravel. The Grants.gov implementation demonstrates the use of a variety of credentials to access a single application, while the eTravel pilot allows a ubiquitous government-issued credential (EEX) to be used across multiple agencies.
- PKI-enabled applications that simplify business interaction with the government are being piloted. FedTeDS (GSA/IAE) and eOffer (GSA/FSS) are allowing federal vendors and contractors to electronically obtain sensitive information and submit offers using certificates obtained through approved vendors or from Federal Agencies.
- Two pilots are testing form submission requiring electronic signature. EPA's Central Data Exchange (CDX) is an Agency-sponsored pilot application that uses the Federal PKI Bridge CA for transactions involving environmental data submissions requiring certificate signing. A National Park Service application will provide permits to allow scientists and researchers to electronically submit the required documents related to research performed at parks.
- The groundwork for enterprise-wide E-Authentication implementation is being laid in pilots with the Department of the Treasury and with Veteran's Affairs.
- The ability to use a PKI credential to access a password-protected resource using a translator that turns the PKI response into a SAML assertion is being tested in the Treasury pilot, as well as a GSA pilot.
- The issues of scheme to scheme interoperability are explored in an NIH which maps policies and tests technical interoperability between E-Authentication and Shibboleth based federations in the higher education community.

## **2.6 Business Drivers for E-Authentication and Federated Identity**

The following business drivers for federated identity technologies are promoting early adopter deployment: improved user experience, simplified administration and cost savings, risk transfer or regulatory compliance, and opportunities for competitive advantage, or improved service.

The E-Authentication Initiative provides a valuable set of services to citizens, industry representatives, government agencies, and government workforce members alike. Users across all these groups will be able to re-use credentials that have already been issued to them from a variety of accredited CSPs, such as an accredited financial institution in the end-user's geography or a nearby accredited Federal, state, or local government Agency. This minimizes the number of user IDs and passwords that end users need to remember.

The E-Authentication Portal will also provide a valuable service to users by presenting them with a list of available CSPs that meet the government's requirements for issuing Level 1 through Level 4 credentials, and identifying government AAs accessible through the portal.

Applications relying on E-Authentication can realize significant cost savings through streamlined development processes and simplified administration. Individual applications will not need to develop application-specific authentication capabilities, and will be able to rely on a general set of infrastructure services to provide authentication services with varying levels of assurance that user are who they claim to be. Application administrators will have the option to rely on CSPs to register and validate credentials for them. And since E-Authentication supports other E-Gov initiatives and application compliance with the Government Paperwork Elimination Act (GPEA), it will also provide government-wide savings.

Finally, E-Authentication can improve security by enabling federated use of stronger authentication mechanisms. Much of the benefit will come from increasing the number of Level 2 (Medium Assurance) CSPs and credentials, but higher assurance PKI users can also be federated to applications and in time, additional strong authentication mechanisms can be supported. Stronger, more accessible authentication services will enable improved E-Gov services, and bring competitive advantage to businesses that partner with E-Gov endeavors.

### **3. Federated Identity Management: An Industry Analysis**

Federated identity management is economically inevitable, and offers generally better risk tradeoffs than other alternatives for inter-domain security. But first, standards must coalesce, and interoperability and trust enablers emerge in the industry.

#### **3.1 Specifications and Standards**

While there has been uncertainty and churn in the standards space, standards are beginning to coalesce as follows:

**Security Assertion Markup Language (SAML)** is an industry standard for Web single sign-on (SSO) and Web services authentication, attribute exchange, and authorization. SAML defines assertion message formats that are referenced in Liberty Alliance, Shibboleth, WS-Security, and other specifications. It has broad vendor support and is in early adoption gaining momentum across financial services, government, manufacturing, telecommunications, higher education, and other vertical industries. For all SAML's promise and marketplace momentum, however, enterprises deploying SAML at this stage still face significant issues establishing interoperability, technical interconnection, trust, and business agreements. Much of the E-Authentication Initiative's work is directly addressed at overcoming these issues.

**The Liberty Alliance Project** is an industry consortium that has extended SAML by developing specifications for account linking, permission based attribute sharing, and identity enabled applications. Liberty's Identity Federation Framework (ID-FF) goes beyond the basic SAML authentication use case to address what is the next step for many applications, linking a digital identity asserted by a CSP to an existing account used for authorization in an application. ID-FF has widespread applicability to the enterprise and e-business markets and would be useful to some Federal applications, especially as it provides a relatively privacy-friendly approach by recommending that users opt in to account linking, and requiring an opaque (rather than unique) identifier for each pair of digital identities.

**Shibboleth:** The Internet2's Middleware Architecture Committee for Education (MACE) has developed an architecture model for federated identity management called Shibboleth. Shibboleth is a SAML-enabled application for Web single sign on, with optional anonymity built in as well as mechanisms for user-controlled attribute exchange from CSPs to applications. While Shibboleth is in production use at ten or more universities and a number of others are in pilot, there has been little commercial uptake of Shibboleth outside of vendors that sell

applications to universities. Yet as Shibboleth use expands the E-Authentication Initiative is actively researching adding it as a supported federation scheme due to the high degree of interaction concerning grants and training courses between almost every Federal Agency and many academic institutions.

**Federal PKI:** The Federal Bridge CA provides an alternative kind of federation by enabling mutual acceptance of certificates in cross-certified security domains. To achieve this CAs, PKI-enabled clients, and validation authorities must all follow advanced X.509 standards, and implement extensions that are not yet entirely supported in commercial products. Bridge-enabled federation promises high assurance and leverages robust procedures for trust establishment and assessment, but it is not loosely coupled like assertion-based federation because it puts symmetric requirements on client and application systems across all interoperating domains. Tight coupling limits applicability. Currently, Federal Agencies are the only production users of FPKI. However, there are plans to create a Commercial Bridge CA (initially for the aerospace industry) and an EDUCAUSE Bridge for the academic community is already cross-certified with the Federal Bridge on a pilot basis.

**WS-Security and WS-\*:** Web services, which are emerging as the preferred means of application interoperability and integration, also require federated identity and security services. The WS-Security specification has now been standardized at the Organization for Advancement of Structure Information Standards (OASIS) to provide message level security for Web services. Also, Microsoft and IBM are driving an initiative called WS-\* (pronounced “WS star”). WS-\* defines specifications for Web services security, reliable messaging and transactions in a composable manner. WS-\* security specifications are also designed to interoperate with existing security models such as passwords, Kerberos, SAML and PKI. However, with the exception of WS-Security, the new WS-\* specifications are all at an early stage of their development. Unless vendors produce COTS WS-\* support more rapidly than expected, most of the WS-\* specifications will not meet the E-Authentication Initiative’s maturity requirements over the next three years. However, the OASIS WS-Security standard combined with password, X.509, or SAML tokens may be ready for Federal use sooner. And because the WS-\* specifications take an open and architecturally holistic approach that could ultimately be of great value in delivering secure Web services, they bear watching.

**SAML 2.0 and the Convergence of Standards:** Multiple work streams from the standards community are all converging in SAML 2.0. SAML 2.0 re-factors SAML, Shibboleth, and Liberty ID-FF to enable a number of advanced features. While SAML 2.0 is not backward compatible to SAML 1.x or Liberty ID-FF, it uses many of the same XML constructs and may represent a relatively

incremental effort for existing federation vendors to build. It is also notable that WS-Security, WS-Trust, and WS-Federation (from WS-\*) all support the use of the SAML assertion as a token format enabling web services security services. While additional work is required before WS-\* and SAML can work together seamlessly, it is fortunate that SAML is a point of convergence between the WS-\* and OASIS worlds.

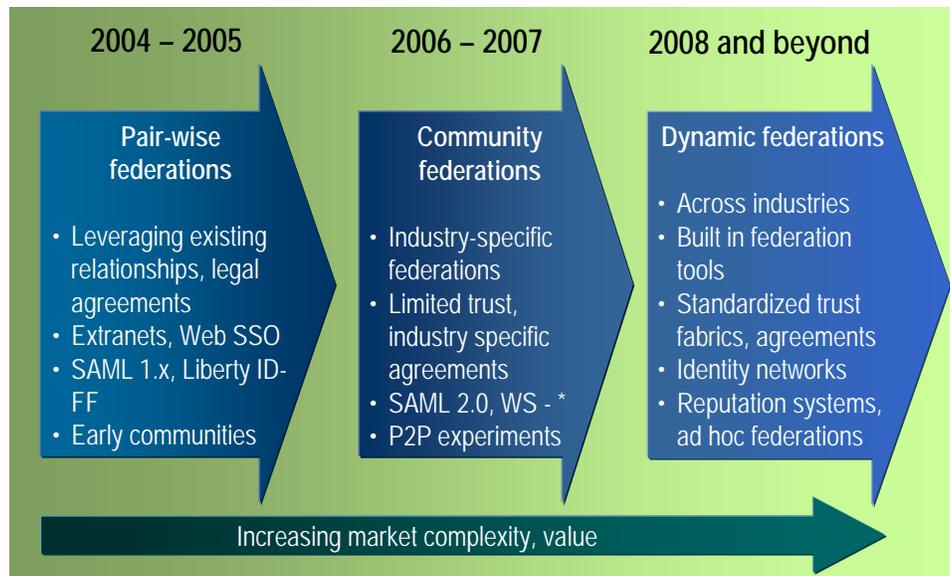
Over time, federated identity standards will change, diverge, and converge as new Web services, privacy, and security requirements are addressed. It is appropriate under the circumstances for the E-Authentication Initiative to implement layers of abstraction to accommodate multiple federation schemes through technical architecture components such as the planned Scheme Translator component.

For more information on the federated identity standards, Web services security, and convergence see [Appendix B](#).

### **3.2 Industry Adoption of Federated Identity**

SAML is entering the early adopter deployment stage, and gaining momentum. Burton Group estimates that, at press time, more than 200 production implementations of SAML (including a smaller number of Liberty and Shibboleth implementations based on SAML) are spanning financial services, government, higher education, manufacturing, insurance, telecommunications, and other industries. Customers are primarily using SAML to support browser-based single sign-on (SSO) across business-to-business (B2B) application environments, and internal application environments.

Notwithstanding these positive factors, current SAML-enabled products are just the beginning of federated identity functionality, and the federated identity management niche within the greater identity management (IdM) market is just taking shape. Longer term, as shown in Figure 1, federated identity will evolve in three waves. The first wave exists today and supports enterprise IT infrastructure and applications with sets of pairwise relationships to internal and external partners. The second wave will emerge when sets of pairwise relationships evolve into communities enabling peer-to-peer interaction. The third wave will appear when enterprises and individuals begin to interact across multiple communities.



**Figure 1:** *Projecting Federated Identity Adoption*

The first wave of federated identity (2003-2005) exists today and supports enterprise IT infrastructure and applications with sets of pairwise relationships to internal and external partners. This wave is evolving from the bottom up. Functionality is confined mostly to authentication assertions, account linking, and simple attribute exchange based on SAML 1.x or Liberty ID-FF.

The second wave (2006-2007) will emerge when sets of pairwise relationships evolve into communities enabling peer-to-peer interaction among the members. Nascent Liberty Alliance circles of trust, E-Authentication, Shibboleth and other communities are harbingers of federations that will proliferate once standards, practices, and mindshare evolve in multiple industries. The functionality in use will grow more sophisticated, and privacy related controls such as provided in Shibboleth or Liberty Identity Web Services Framework (ID-WSF) will be widely implemented.

The third wave will emerge when federated communities become larger and more dynamic. Dynamic federation could emerge in the 2008 (or beyond) timeframe, but this will require that standards become more advanced, federated identity functionality be built into operating systems and other mass produced computing platforms, and trust broker services or identity network services become viable and profitable. At that point, interactions will cross communities and will be initiated much more dynamically thanks to sophisticated token exchange services, policy languages, and distributed claims or authorization services. But for every "trust relationship" there will continue to be much "distrust" and plenty of risk to go around. The wider the multi-lateral trust, the

lower the specific assurances. A universal liability solution will never emerge to cover ALL the needs for all federated identity enabled applications.

Also in the second and third wave, reputation services (such as the vendor rating systems in use today at eBay, Amazon, and other online marketplaces) may prove a potent alternative to more formal "trust networks." But reputation systems will likely be used primarily only in low-risk scenarios, or in cases where applications have compensating controls – such as knowledge based authorization, or insurance - to mitigate a level of uncertainty at the identity layer.

By interoperability testing federation products and engaging commercial CSPs directly and through the EAP, the E-Authentication Initiative is having a positive impact on federated identity adoption. If E-Authentication is broadly adopted by Agencies in production federations, it will spur formation of multiple second wave community federations. Initiatives like the EAP will also help usher in third wave dynamic federation for the industry as a whole. If E-Authentication and EAP are extremely successful, they could even accelerate adoption slightly ahead of Figure 1's schedule. Leadership in establishing advanced federation technical and business infrastructure nationally, and eventually internationally, would also benefit the United States in global markets.

### **3.3 Enabling Conditions**

The critical factor enabling federations to scale from bilateral relationships in the first wave to industry-centric communities in the second wave is **interoperability**. While **trust** and other business issues are also important in enabling second wave communities, these communities in the early stages can leverage industry-specific agreements, technologies, and practices that need not be applicable for broader use. But in the transition from industry specific communities to dynamic federation trust becomes the critical factor.

#### **Interoperability**

During the very first federated identity pilots, enterprise customers had the luxury of agreeing on a common product that could interoperate using SAML or another protocol with another instance of itself. But as more products appeared, more enterprises created their initial federation deployments, and the number of bilateral relationships expanded, multiple products were required, and interoperability became a real problem.

During the early stages of a standard's evolution, specific versions of products supporting the standard often make first contact in the field, and the burden of ironing out standards interpretation, mismatches of supported features, and outright compliance errors falls on the customer. Add to this the fact that most

federations must establish custom profiles for name and attribute handling as well as procedures for configuration metadata exchange, linking user interfaces, session timeouts, general error handling, and audit and one finds that most federated identity projects require some custom engineering and testing. Aspects of this testing and engineering must also be repeated with each new partner that comes onboard.

An additional problem arises because there are multiple versions of the standard and multiple profiles for each version. Leaving aside SAML 2.0, there are four variants of SAML since both SAML 1.0 and SAML 1.1 can implement either the browser/post or the browser/artifact profile. Shibboleth and Liberty ID-FF comprise additional specifications, and there are multiple versions of each. Further confusion will abound as Web services emerge, bringing WS-Security along with multiple token profiles and eventually WS-\* into the fray.

In the face of specification proliferation, most applications do not implement federation natively, but rely on identity management vendors to provide federation functionality. The efforts of identity management vendors such as E-Authentication tested Entegry, Entrust, HP, IBM, Oblix, RSA, and Sun to support multiple federation standards versions and profiles are critical to broker interoperability among different CSPs and applications. Industry will provide solutions to the interoperability problem over time – at a price. The market will bear the price because the business drivers for federated identity are strong.

Thanks to the E-Authentication Initiative's interoperability testing, Liberty Alliance conformance testing, and a vendor conformance testing initiative for SAML that will soon be announced, most federation product vendors have some experience making their products work together. But until the standards community and the market support commercial interoperability testing labs in a format that vendors can afford, the E-Authentication Initiative and other large federations must continue to be proactive in driving interoperability on their own terms across the community of security middleware vendors, CSPs, and applications.

## **Trust and Business Relationships**

Trust will be a critical enabler for a second wave of community-based federation and the third wave of dynamic federation. Organizations have several options available for creating trust in the network and e-business environments that federation supports, but the industry has not yet achieved its goal of creating the dynamically negotiated trust infrastructure to significantly reduce the friction in online transactions. Within computing circles the concept of trust – the willingness of a party to perform an action based on a relationship – is often

confused with the notion of trustworthiness, which relates specifically to technology and not the broader business issues of risk and recourse. In order to achieve trust for electronic services, organizations must successfully blend both online technologies and offline business processes.

The main building blocks for establishing trust are:

- Legal infrastructure
- Historical business relationships
- Shared policy
- Technical assurance
- Audit and accreditation
- Cryptographic key management
- Assertions

While each building block has its strengths and weaknesses, none can work alone to accommodate e-business, and rarely are all the building blocks in a relationship equally strong. Instead users, enterprises or communities must choose a combination of building blocks that add up to a trust relationship that is acceptable for a particular class of actions and relationships. For example, in the world of Internet credit card transactions, a very clear economic model and well-defined liability structure make up for weak authentication and rudimentary SSL key management. In other cases, very strong technical assurance and audit are used for compliance with regulatory needs. For example, the Federal Identity Credentialing Committee (FICC) combines most of the building blocks with strong cryptographic key management through the Bridge CA standards.

There are a number of trust-related issues holding back federated identity and authentication during the first and second waves of adoption:

- The business relationships building block – on which many pairwise federations rest – doesn't scale to form broad communities (such as E-Authentication) or dynamic federation.
- The legal building block can enable pairwise relationships or even large communities to form within contractual privity. However, contracts take time to develop or approve, and don't scale well across jurisdictions or fundamentally different applications or industries.
- Key management and assertions standards, technologies and practices are used today in Layer Security (TLS) and SAML; more sophisticated protections are still maturing and are not ubiquitously available in products.

- Shared policies can be established only on a static, pairwise basis because standardized policy languages have not been broadly accepted or implemented. This means that policy mapping must be done manually.
- Audit, technical assurance, and accreditation building blocks are weak because there is no generally accepted audit an organization can use with multiple would-be federation partners, especially across industries.

The Electronic Authentication Partnership is trying to create a set of business rules stating minimum requirements, liabilities, and operational assurances. This approach may establish broad common denominators for authentication assurance and liability. But many cross-industry federations and applications need authorization and other services in addition to authentication, and this will require more or different legal protections, operating rules, liability arrangements, and other assurances. Still, by simplifying baseline authentication, EAP framework adoption by multiple industries would help accelerate dynamic federation.

## 4 Analysis - The E-Authentication Initiative

The E-Authentication Initiative is creating the enabling conditions – interoperability and trust - for federation between government applications, government CSPs, and industry partner applications or CSPs. Acting as a broker for what will become a very large community, E-Authentication performs the following roles, which are essential for enabling large federations in today’s environment:

- Interoperability roles
  - Administering common interface specifications, use cases, and profiles
  - Conducting interoperability testing according to the specifications
  - Maintaining a list of approved products
  - Providing a portal service through which users, applications, and CSPs can be matched or discovered, and some errors handled in a consistent manner for users
  - Managing configuration data for CSPs and applications, and issuing certificates to enabling secure communication
  - Planning and developing support for new industry standards as COTS products emerge
  
- Trust and business related roles
  - Managing relations among relying parties and CSPs
  - Administering identity management/authentication policies
  - Establishing and administering common business rules for the relationships among the parties
  - Performing credential assessments
  - Authorizing CSPs on a trust list according to standardized assurance levels
  - Managing compliance/dispute resolution

The following sections describe and analyze the E-Authentication Initiative’s technical architecture, interoperability, and trust models.

### **4.1 E-Authentication Technical Architecture and Interoperability**

Burton Group’s program review of the E-Authentication Initiative’s Technical Architecture and Interoperability focused on key components of the planned architecture by interviewing representatives from the E-Authentication Architecture Work Group (AWG). Ramifications of the existing architecture were discussed with a variety of participants including end-users, CSPs, and AAs. The Technical Architecture review also investigated general testing scenarios and

conformance or interoperability testing experiences from both a vendor and an interoperability lab perspective. A brief overview of the Technical Architecture is presented here, along with Burton Group's general findings and future considerations that should be taken into account as the E-Authentication Initiative continues to evolve over time.

## **Technical Architecture Overview**

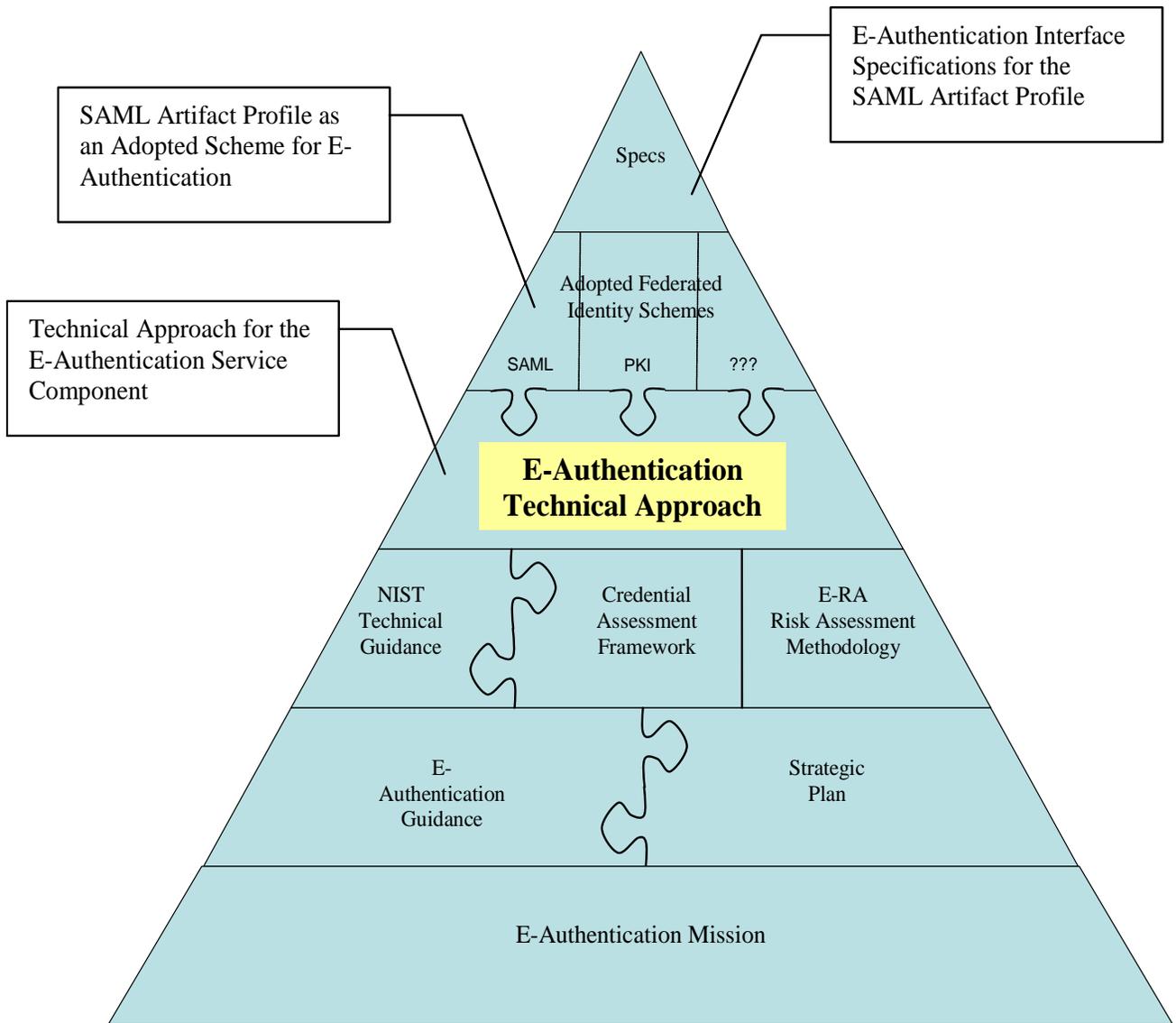
The E-Authentication Technical Architecture is included within the [E-Authentication Technical Approach](#) document. These and related specifications build upon the Office of Management and Budget's E-Authentication Guidance for Federal Agencies (OMB M-04-04), and the National Institute for Standards and Technology's Recommendation for Electronic Authentication (NIST SP 800-63). Figure 2 illustrates how the E-Authentication Technical Architecture document relates to other important specifications.

The E-Authentication Initiative Technical Architecture incorporates a number of over-riding design goals. First and foremost, the Federal Government will not necessarily be a credential provider, but will rely on a network of commercial organizations as well as Federal, state, and local governments acting as CSPs to support a variety of AAs. Federated authentication across a number of application environments will utilize existing industry standards and must account for the evolution of technology over time. During initial deployment (and as the industry continues to evolve), the E-Authentication Initiative plans to rely on vendor-supported COTS solutions, and will avoid using government-provided software.

Besides relying on a number of CSPs, AAs, and the underlying policy framework, the E-Authentication program itself plans to offer a set of value-added services such as portal, validation, and scheme translation services. Each of these services is summarized in more detail in the following sections.

## **Portal Service**

The E-Authentication Technical Approach document identifies a distributed portal environment consisting of an E-Authentication portal interacting with other portals or location services at CSPs and AAs. The E-Authentication Portal provides linkages between available CSPs and AAs that accept their credentials. The Portal links CSPs with AAs, enabling other sites to add value as they see fit without requiring redundant interaction with end users. Once linked, users, applications and CSPs interact directly without portal mediation, however.



**Figure 2:** *E-Authentication Initiative Technical Approach*  
**Source:** “Technical Approach for the Authentication Service Component”

The portal configuration supports a variety of use cases including “CSP-first”, “Portal-first”, or “AA-first”. The “CSP-first” scenario occurs when a CSP presents the end user with a list of AAs that will accept their credentials. CSPs may be able to add value by suggesting AAs that are relevant to a particular end user or related to the business the end user is engaged in during a particular browser session. A CS that has downloaded the metadata about AAs is considered Portal-enabled if it has the ability to present the end user with applications that are accessible with their credential and can redirect them through the Portal to the application.

Other use cases allow end-users to go directly to the E-Authentication Portal first to locate CSPs or AAs, or allow for end-users to access an Agency Application directly. Users who do not have sufficient credentials to access an Agency Application directly will be redirected to the portal so they can identify CSPs that can issue the appropriate credentials.

## **Validation Service**

E-Authentication currently supports 4 levels of credentials. Applications may accept Level 1 or 2 assertion-based credentials, or Level 3 or 4 PKI-based credentials. The E-Authentication technical approach for accepting Level 3 or Level 4 PKI credentials assumes a “validation service” is available for AAs to validate certificates.

The E-Authentication Technical Approach describes various use cases for AAs to validate certificates, including Certificate Validation Services provided as part of the E-Authentication component itself or Local Validation within specific Agency application environments. The validation service assumes that certificates will be issued by trusted CAs that comply with Federal PKI policies, and as a result the validation service will need to support various mechanisms such as Certificate Revocation Lists (CRLs), Online Certificate Status Protocol (OCSP), eXtensible Key Management Services (XKMS), or Mitretek’s Certificate Arbitration Module (CAM).

## **Scheme Translation Service**

In order to support additional federated identity standards such as SAML 1.1, SAML 2.0, Liberty Alliance, WS-\*, and/or Shibboleth in the future, the E-Authentication Technical Architecture has embraced the concept of a Scheme Translation Service. The Scheme Translation Service will allow CSPs and AAs utilizing different federation mechanisms to authenticate users.

A current use case that has been identified is intended for users who authenticate with a Level 3 or Level 4 PKI certificate and want to access assertion-based applications. Instead of requiring these users to re-authenticate at a lower assurance level, the E-Authentication Initiative plans to provide Step-Down Scheme Translation Services that will validate the certificate and create an assertion usable by the application, eliminating the need for PKI-like certificate validation services across multiple assertion-based application environments.

Additional Scheme Translation Services are anticipated in the future to support profile differences and translation services between standards/versions as the E-Authentication Initiative continues to evolve over time.

### **Technical Architecture and Interoperability: Findings**

The E-Authentication Technical Architecture provides a solid foundation for federated authentication that can be extended in the future as products, technologies, and standards evolve. The overall architecture is flexible, leverages capabilities that already exist in the industry, promotes commercial as well as government involvement, ensures interoperability, and can be leveraged by many current and future applications across a number of Agencies. These key findings are summarized below.

**Provides a flexible Architecture.** CSPs and AAs can “opt-in” as they see fit. The architecture supports the concept of distributed portals, including a relatively “thin” portal as a service for mapping Agency applications to CSPs along with additional distributed portal functionality at CSP or AA locations. Validation Services can be deployed as part of the PKI Bridge, on a desktop, or as a dedicated service, and planned Scheme Translation Services will ensure the E-Authentication Initiative is not “locked in” to a single standard in the future. Flexibility also extends to end users as well. End users can opt-in to the SSO environment and have the flexibility to choose a preferred CSP (or CSPs). Various use cases have already been defined that make it easy for individuals to interact with the services.

**Enables agencies to maintain their investments in higher assurance PKI systems.** The Federal government has already made a significant investment in its FPKI infrastructure. Leveraging the trust and policy framework defined within this environment represents a significant cost savings over deploying a similar but different framework.

The Federal Identity Credentialing Committee (FICC) has developed plans to issue a common credential for all Federal employees that can be used for both physical and logical access. The FICC smart card credential also uses biometrics to bind the user to the digital credential during the registration process. FICC credentials are already mapped to E-Authentication Level 3 and demonstrate how agencies can make security investments based on internal requirements and still interoperate in the E-Authentication framework. Technical interoperability is attained by following the government’s smart card interoperability specifications, FPKI common policy, and online validation services. Assurance interoperability is maintained by following the NIST guidance for identity proofing during the registration process.

**Encourages commercial involvement:** The government has learned from unintended consequences of past efforts that it must encourage and attain commercial investment in the technologies it wishes to deploy on a wide scale. Unlike the Certificate Arbitration Module (CAM) – a Government Off the Shelf (GOTS) component developed for FPKI – the vast majority of the systems used among federated E-Authentication CSPs, AAs, and infrastructure components are based on COTS products. Today, the CAM itself is being open sourced back to industry to encourage vendor support for Federal certificate path validation requirements.

The current architecture requires relatively little incremental effort from vendors over and above what is required for commercial federated identity deployments. The E-Authentication program adopted the SAML 1.0 standard – which is becoming a de facto solution for browser based federated sign on – intact. Virtually all vendors have announced support for SAML as a mechanism for exchanging authentication-related information. As a result, many security software vendors have COTS SAML software already available in their latest and most regularly supported versions.

Moreover, credentialing and accreditation processes for Level 1 or Level 2 CSPs map closely to those used within the banking community, and therefore would be relatively easy to deploy in those markets. In this regard, NIST has provided valuable technical guidance to this initiative as well as a number of other standards-related activities. Their continued involvement should be considered crucial to the acceptance of the E-Authentication Initiative today and in the future.

**Many candidate applications:** A number of existing pilot applications have been identified and are currently undergoing testing or plan to leverage many of the E-Authentication Initiative’s features in the near future.

Key pilot participants identified to date include multiple agencies such as the Environmental Protection Agency (EPA), the National Park Service, the National Science Foundation (NSF), the U.S. Department of Agriculture, the U.S. Department of Health and Human Services, and the National Institutes of Health (NIH). Groundwork is being laid for future pilots involving the Department of Treasury and Veteran’s Affairs.

Applications being piloted that promise to improve efficiencies within the federal government include Grants.gov and eTravel. The Grants.gov implementation demonstrates using a variety of credentials to access a single application, while the eTravel pilot allows a ubiquitous government-issued Employee Express (EEX) credential to be used across multiple Agencies.

PKI enabled applications that simplify business interaction with the government are also being piloted. FedTeDS (GSA/IAE) and eOffer (GSA/FSS) are allowing federal vendors and contractors to electronically obtain sensitive information and submit offers using PKI certificates obtained through approved vendors or from federal agencies.

These pilot applications include a good mix AAs and CSPs. In the future, E-Authentication could be used heavily by additional form filing applications, of which there are thousands. These include filings from private citizens, businesses, and state or local governments. Various state governments including Illinois, North Carolina, Michigan, and Montana as well as additional Agencies such as the Department of Justice and the Department of Homeland Security have also expressed interest in the E-Authentication Initiative and are monitoring it's progress.

Most of the pilots mentioned above utilize SAML assertions at Level 2, or PKI-based credentials at Level 3 or 4. Early implementers of federated identity standards have reported only minor changes are required to web-based applications to integrate them with federated identity infrastructures. The E-Authentication technical staff is documenting pilot experiences in "cookbook" documents and handbooks. As the pilots progress, usability will be an important focus. For example, the end user experience can be improved by developing common approaches to error conditions and exceptions.

**Superior Testing Environment:** Unlike complementary testing scenarios such as the Liberty Alliance conformance testing program, and emerging federated identity conformance testing services, the E-Authentication Initiative has adopted an "*N by N*" testing scheme that requires vendors to be compliant with the standard and interoperate with all other vendor solutions already on the [Approved E-Authentication Providers List](#). Testing requirements of this nature will minimize interoperability issues as more government and commercial organizations opt-in to the E-Authentication program, but increase the up-front testing responsibilities of the E-Authentication Interoperability Lab and vendors who want to become approved providers.

Vendors have consistently reported minimal changes to their products during testing, and additional vendors are lined up to become an E-Authentication "approved vendor." Yet another strength of the E-Authentication interoperability testing process has been production of "cookbook" documents to assist applications in deploying products that support SAML 1.0.

## **Technical Architecture and Interoperability: Future Considerations**

The scope of the E-Authentication Technical Architecture is currently limited to provide a small set of capabilities and gain adoption across a broad mix of commercial environments, government agencies/organizations, and end-users. The overall architecture is expected to evolve over time and change as standards, technologies, vendor solutions, and market factors change. The following set of “Future Considerations” investigates issues the E-Authentication Initiative should address, and capabilities it may need to support in the future.

**Enabling authorization, lifecycle identity management, and exception handling across multiple AA and CSP deployments.** Authentication and authorization are two halves of the same coin. Most AAs and planned global applications such as eTravel require more than basic authentication information before decisions can be made on whether to grant access to specific users. The following are typical requirements for coordinating identity management between CSPs and AAs:

- Applications must provide users secure and convenient access, including the ability to handle scores of normal browser behaviors and errors.
- Applications must activate each digital identity corresponding to each CSP through which each user is allowed to authenticate, or associate the fully qualified name used by each CSP for the user with the application’s existing representation of that person’s digital identity.
- Applications must often obtain attribute information about authenticated users for authorization or personalization purposes.
- When additional information, such as the user’s role or title attribute, is required, it may need to be obtained from the CSP using assertion messages or through out of band administrative or directory synchronization solutions.
- Some attribute changes or role changes must be synchronized between the user, the CSP, and the application. Name changes and termination of the CSP’s relationship with a user must also be communicated to applications.
- CSPs and applications must be capable of sharing or correlating audit log information to investigate fraud or security breaches.

Coordination between CSPs and AAs is required for these scenarios, occurs inevitably, raises privacy issues inevitably, and calls for consideration of common approaches or guidance to ensure the most efficient and appropriate approach over time. Facilitating authorization and lifecycle identity management will increase the value of the E-Authentication Initiative to both Agencies and businesses alike, increase usability, simplify user management processes, reduce costs, and ease repeatable deployment – thus increasing acceptance and

utilization of E-Authentication services by multiple commercial and government organizations.

**Ensuing privacy along with providing enhanced services:** Privacy issues and balancing end-user concerns with sufficient security within Agency applications must be considered as the E-Authentication Initiative continues to evolve. The privacy issues are an unavoidable result of interactions that must occur between AAs and CSPs - whether or not the E-Authentication Initiative is in the loop.

Although privacy features are not addressed within the SAML 1.0 specification, features such as permission based attribute sharing are available in Shibboleth and Liberty Alliance specifications, and will be included in SAML 2.0. However, these specifications can only be expected to meet some of the future needs. A more proactive approach to privacy will be required, and might include tools for assessing risk and determining privacy impacts, providing guidance for what to include and not to include within assertions, or assisting CSPs and AAs with developing more mature and comprehensive privacy policies and frameworks.

**Support for additional standards:** The SAML 1.0 specifications represent the industry's first widespread attempt at federated identity standards, and these specifications were initially targeted to gain broad acceptance of basic federated identity concepts without solving all the federated identity challenges organizations may face.

As a result, the SAML 1.0 specifications have some limitations that are commonly known, and since the E-Authentication Initiative does not want to be limited to any one standard, plans are already in place to support additional federated identity standards as COTS products and Agency demand for them emerges. The SAML 1.0 specifications do not support signed assertions, and the E-Authentication Initiative has chosen to support only the Browser/Artifact profile. Neither SAML 1.0 or SAML 1.1 specifications support account linking, global logout, or permission-based attribute sharing which might facilitate improved usability and support application deployment needs.

Adopting some combination of SAML 1.1, Liberty Alliance, Shibboleth, SAML 2.0, and WS-Security would bring the government additional capabilities and increase acceptance within the commercial marketplace, but will increase the complexity of the architecture over time by requiring additional scheme translators, additional portal functionality, and perhaps other components.

Table 1 identifies additional federated identity specifications, incremental benefits they may bring the E-Authentication program, and any pre-requisites these specifications may place on the E-Authentication Initiative. Note that

supporting any standard or specification in addition to SAML 1.0 will require developing and testing Scheme Translator functionality.

As the E-Authentication program evolves and supports more standards, specifications, versions, and profiles, the complexity of interoperability testing increases. However, supporting additional specifications will also address some significant usability and privacy features that may be considered requirements by CSPs, applications, and end-users alike in the future.

**Addressing interoperability issues:** The E-Authentication Initiative should not underestimate the increased complexity of interoperability testing multiple specifications in the future. Already a backlog is building up for testing SAML 1.0 implementations. Interoperability testing within the E-Authentication Initiative will grow increasingly complex over time as the test matrix expands, and it is unlikely that industry will provide services that fully take on the interoperability testing burden for large federations. Every new version of a vendor's solution requires retesting, indicating a need for more efficient testing processes and test suites in the future.

Additional scheme translators will be required as part of the E-Authentication infrastructure, and will be complex and difficult components to deploy and maintain. Fortunately, Web access management products have already started to produce security middleware functionality supporting multiple standards.

E-Authentication should continue to encourage the industry to further develop automated conformance testing services and commercial testing tools in order to raise the quality of products prior to being installed in the interoperability lab for conformance testing purposes.

**Support for additional authentication mechanisms:** Although embracing the Federal PKI policies provides a good initial framework for assuring user identities at Level 3 and Level 4, the E-Authentication Initiative should expect to support other forms of strong authentication in the future such as one time password generator tokens, knowledge based authentication, and biometrics. Since many commercial SSO implementations support some of these services today, support for these added features will be expected by Agency and commercial enterprise applications. Becoming more technology agnostic over strong authentication would also enable the E-Authentication Initiative to be more flexible as innovations emerge in the industry.

| <b>Standard or Specification</b>   | <b>Major Incremental Benefits</b>   | <b>Deployment Pre-Requisites</b>  |
|--|---|---|
| SAML 1.1   | Digital signature increases assertion assurance.  | Additional testing/deployment complexity.<br>Performance enhancements for AAs and CSPs.   |
| Post profile (with SAML 1.1)   | Creates potential for Shibboleth interoperability with existing university deployments.   | Additional testing/deployment complexity.   |
| Liberty Alliance ID-FF 1.2   | Standardized account linking<br>Global Logout<br>Privacy features<br>Interoperability with existing Liberty deployments.  | Privacy impact assessments.<br>Additional security/directory integration and testing/deployment complexity.<br>Provisioning/consistency checking capabilities.  |
| Shibboleth SSO and attribute functionality   | Attribute exchange with privacy features.<br>Interoperability with existing university deployments.   | Privacy impact assessments.<br>Additional security/directory integration and testing/deployment complexity.   |
| Liberty Alliance ID-WSF  | Attribute exchange with privacy features.<br>Discovery service  | Privacy impact assessments.<br>Additional security/directory integration and testing/deployment complexity.   |
| SAML 2.0   | Account Linking<br>Global Logout<br>Attribute exchange with privacy features.<br>Interoperability with Shibboleth and Liberty deployments transitioning to SAML 2.0.  | Privacy impact assessments.<br>Additional security/directory integration and testing/deployment complexity.   |
| WS-Federation passive profile using SAML token   | Enable direct federation with Microsoft's future/planned COTS products.   | Additional testing / deployment complexity.   |
| WS-*:<br>- WS-Security<br>- WS-Trust<br>- WS-SecureConversation<br>- WS-Policy<br>- WS-Federation<br>Active Profile, Pseudonym, and Attribute services | Pass user authentication/identity through Web services using SAML, PKI, Username or other tokens.<br>Dynamic web services security.<br>Alternate ways to accomplish account linking, attribute exchange, global logout, and other services.<br>Enable interoperability with Microsoft's future/planned COTS products. | Completion of the WS-* specifications.<br>Acceptance of WS-* by a standards body.<br>Release and widespread deployment of COTS products.<br>Entirely new scheme for Web services support.<br>Privacy impact assessments.<br>Additional security, integration, deployment, and testing complexity. |

**Table 1:** *Benefits and Pre-Requisites of Additional Federated Identity Standards*

**Further study of assertion based security:** Unless implemented correctly, SAML deployments are vulnerable to a number of security threats associated with stolen and/or forged artifacts. Appropriately, the E-Authentication Initiative mitigates most threats to SAML by requiring TLS between CSPs and applications. Properly implemented digital signature support would strengthen SAML's security in certain scenarios. Robust implementation of audit logs, event analysis/correlation and other risk mitigation strategies may be even more important. A number of studies of assertion security have been provided for the industry; these could serve as a basis for more detailed security analysis by NIST of assertion based security.

See the [E-Authentication Initiative recommendations section](#) for specific guidance on how to address the future considerations discussed above.

## **4.2 E-Authentication Trust Model**

The trust model for E-Authentication is based on policies for authentication levels and methods, governance, and the assessment framework.

### **Trust Model Overview**

The E-Authentication trust model rests on policy, key management, and governance as well as the assessment framework, criteria, and methodology for CSP, AA, and infrastructure components.

### **Policy – Authentication Levels**

E-Authentication policy defines the four accepted levels of authentication, based on guidance provided at the Federal level by the OMB and at the technical level by NIST. The four levels describe the degree of assurance, or confidence, that an AA should assign to an authenticated user. According to OMB, Level 1 provides little or no confidence in the validity of the asserted identity, Level 2 provides some confidence in the asserted identity, Level 3 provides high confidence in the asserted identity, and Level 4 indicates very high confidence in the asserted identity.

The OMB M-04-04 specifies further guidance on how to determine what assurance level is appropriate for each application by outlining six categories of potential impact if authentication problems arise. The categories are 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; or criminal or civil violations. Furthermore, a matrix is used to determine the likelihood – low, medium, or high – for each impact category. It is important to note that even for medium or high risk situations, low levels of authentication assurance may be acceptable provided that risks are mitigated through other compensating controls such as

audit, physical security, personnel security, or other measures. As a result, there is reason to believe that large numbers of applications can be served at Level 2, or medium assurance.

## Policy - Authentication Mechanisms

At the technical level, NIST matches authentication methods to the four assurance levels in its Special Publication 800-63. This document provides minimum guidance for the four assurance levels; in some cases, the E-Authentication Initiative has taken more restrictive approaches than NIST requires. SP 800-63 analyzes authentication assurance levels according to the token used during authentication, the registration process where users are vetted before issuing credentials, the process of remote authentication, and the process of sharing remote authentication results to other parties through assertions. Table 2 summarizes which token types are permitted at each assurance level.

| Type                   | Level 1 | Level 2 | Level 3 | Level 4 |
|------------------------|---------|---------|---------|---------|
| PIN                    | •       |         |         |         |
| Password               | •       | •       |         |         |
| Soft crypto token, OTP | •       | •       | •       |         |
| Hard crypto token      | •       | •       | •       | •       |

**Table 2:** *Token Types at Different Authentication Assurance Levels*

**Note:** NIST deems one time password (OTP) generators to be viable at Level 3, but OTP is not yet supported by the E-Authentication Initiative

According to NIST, assertions can be used to convey authentication results for all but Level 4 mechanisms at this time. At Level 4, the assertion mechanism is not bound tightly enough to the authentication protocol to maintain the highest assurance level. This analysis may change in the future as assertion mechanisms evolve and NIST conducts further evaluation.

NIST plans to evaluate additional mechanisms, such as one time password tokens, knowledge-based authentication, and biometrics so as to provide guidance in future documents. Many commercial enterprises and government agencies have deployed one time password generators and are interested in leveraging these strong credentials for more applications. On the biometrics front, government projects will be making significant investments in biometric technology.

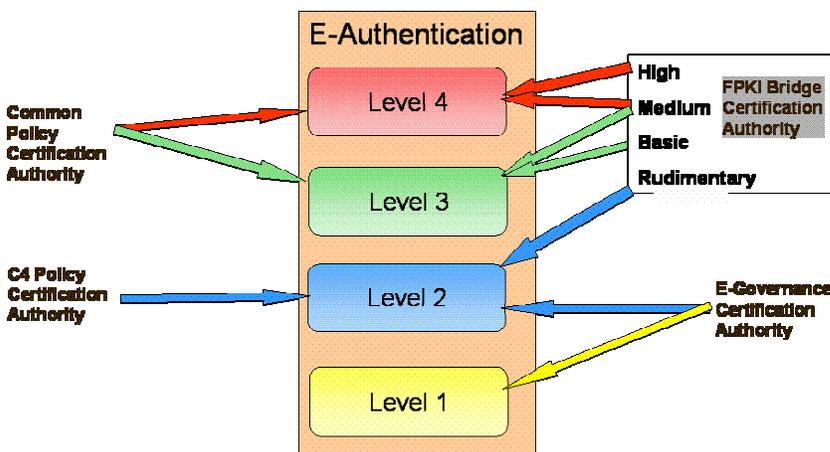
Today, biometrics are acceptable only for unlocking the hardware token in place of a PIN or password. However, NIST provides no explicit guidance for what

type of biometric can be used to unlock the token, how enrollment is performed, where biometric templates are created/stored/compared, or what biometric standards should be implemented. NIST considers biometrics unreliable in a remote authentication scenario.

Agencies determine what authentication levels to accept for a particular application by conducting a risk assessment on each application. The E-Authentication Initiative has provided an E-Authentication Risk and Requirements Assessment (e-RA) tool that enables agencies to match authentication levels to the sensitivity and risk of AAs. Note, however, that high risk applications can use lower assurance authentication methods provided compensating controls in addition to authentication are in place.

### Key Management and Credentialing Policy

Key management provides the technical representation of trust, such that trust can be evaluated dynamically at runtime. The Federal Identity Credentialing Committee (FICC) specifies requirements and provides infrastructure for issuing “common credential” certificates to users at Levels 3 and 4. An E-Governance CA issues certificates to the SAML servers operated by E-Authentication-enabled CSPs and applications. Thus, although assertion-enabled users are authenticated through PINs or passwords at Levels 1 and 2, key management using the E-Governance certificates strengthens the assurance among the SAML servers, and provides a means of controlling membership in the E-Authentication environment. Figure 3 diagrams the various CAs providing key management to Level 3 and 4 PKI users, and Level 1 and 2 assertion servers in the E-Authentication environment.



**Figure 3:** Key management and trust in E-Authentication Environment  
**Source:** Federal Identity Credentialing Committee (FICC)

## **Governance**

The Executive Steering Committee (ESC) governs the E-Authentication Initiative. The ESC is made up of Agency Executives that have invested in the E-Authentication Initiative, provide guidance to the program, and approve policies. Day-to-day operations - including final approval of the Trust List, assignment of Credential Managers, and approval of Assessors - are run by the GSA-led Program Management Office (PMO), but will be transitioning to a line of business organization within GSA.

Credential Managers (CMs) oversee the processes of CSP application, assessment, and monitoring. CMs are assigned to one or more Credential Service by the PM. The application and accompanying documentation is collected by the CM and summarized for the Credential Evaluation Working Group (CEWG) to review. The CEWG determines whether to accept an application for assessment of a CSP. Once the application is accepted, the CM manages the Assessment Team that reviews the applicant, prepares a report, and the CM presents the findings to the PM. The CEWG also is responsible for approving changes to credential profiles or guidance for assessors.

## **Assessment Framework, Criteria, and Methodology**

As noted previously, E-Authentication takes high-level guidance from OMB and NIST when determining authentication levels and mechanisms. E-Authentication uses this guidance to create the Credential Assessment Framework (CAF), which outlines a process for evaluating and assessing Credential Service Providers (CSPs) and the credentials they issue. The CAF describes the process CSPs follow to apply for assessment and the steps conducted to evaluate the CSP against one or more Credential Assessment Profiles (CAP).

The Credential Assessment Guidance (CAG) provides general guidelines for Assessors while they go through the process of evaluating Credential Service Providers. Credential Assessment Profiles contain criteria for assessing the different levels of credentials that are issued by CSPs. Profiles have been established for passwords, PINs, and PKI as well as a common profile for all non-PKI systems. The CAF, CAG, and CAP profiles comprise the suite of documents that outline the assessment process, but they still have interim status and will undergo further development over time. Assessments are performed and approved before the CSP is added to the approved CSP list. Assessments will be conducted on an annual basis during the regular security review.

## **Trust Model – Findings**

Federation schemes require a technical trust mechanism to share assertions in a secure manner. E-Authentication policy levels and the accompanying assessment framework permit Agencies and commercial industry to more readily participate in the program. Stable policies and widely known accreditation methodologies give prospective E-Authentication participants more confidence in the overall process and lower some of the barriers for adoption. By leveraging the Federal PKI as described in Figure 3 and the discussion above, E-Authentication is able to utilize well-defined trust models that are accepted in the Federal environment. The CAF and CAG documents and assessment processes provide a basis for establishing trust with commercial applications and credential services at the medium or low assurance levels, which are suitable for many applications.

Field experience with the CAF suite has varied somewhat among agencies that are conducting E-Authentication pilots. One well organized and prepared Agency required only three days of on-site assessment to complete the accreditation process. Other agencies have taken longer to adjust process or policy to meet baseline requirements. Future assessments are expected to show similar results, where the time commitment varies based on Agency preparedness and documentation as well as the proficiency of the assessor.

The commercial sector also stands to benefit from the government's efforts to codify authentication, PKI, and federation trust models. Commercial entities could leverage guidance put forth by OMB M-04-04 and NIST 800-63, which will raise the level of security practice within commercial enterprises and make them more compatible with the E-Authentication framework if they choose to federate with the government or other commercial entities. However, more uptake within the Federal environment itself, more communication with commercial partners, and better definition of the business rules for government-to-industry federation are required to encourage commercial adoption of E-Authentication as a means of communicating with government.

## **Trust Model – Future Considerations**

To become more comprehensive and successful, the E-Authentication Initiative must (over time) build the business case for commercial participation; reach a critical mass of CSPs; enable more commercial CSPs to operate at Level 2 (medium assurance); proactively address the possibility of security breaches; expand relying party guidance; address liability, dispute resolution and cooperative risk management in government/commercial federations; and expand the trust model to extend the FPKI investment to enable additional technical trust mechanisms.

**Build the business case for commercial participation:** Commercial entities will support E-Authentication if and when they recognize value, whether value is found in new revenue streams, providing additional services to existing customers, entering new channels to gain customers, improving customer satisfaction, or other possibilities. The E-Authentication Initiative must understand and try to enable business models that provide many benefits for government and non-government participants. It is important to note that G2G initiatives tend to have different business models than those found in commercial scenarios.

Potential prospects include revenue opportunities for CSPs, expanded electronic services to citizens and customers, and mutually beneficial applications. Issues include the relatively high cost that commercial CSPs must pay (currently) for in-person identity proofing, or for proofing against a financial database such as a credit bureau. Somehow, reliable identity proofing and authentication needs to evolve from fragmented, high cost, and low volume services into high volume, low cost services that many CSPs and applications can benefit from.

**Reaching critical mass of CSPs:** At this point, it is unknown how difficult or easy it will be to sign up significant commercial CSPs that lend prestige and success to the E-Authentication Initiative. Some have expressed interest, but questions linger regarding liability models, extra operational costs, and business or revenue opportunities. As noted earlier, medium assurance (Level 2) authentication suffices for most government applications, with or without compensating controls. Industry CSPs, such as private enterprises and financial institutions already support credentials services that are assessable at, or could be improved to Level 2.

**Enable more commercial CSPs to operate at Level 2 (medium assurance):** It is not easy for Microsoft .NET PassPort, VeriSign Class 1 certificate service, and other commercial CSPs to support Level 2 in person identity proofing, and financial records checks against the credit bureaus or other sources come at a cost. In the future, legislation or other arrangements enabling qualified commercial CSPs to cross check against financial databases, or leverage proofing systems and databases deployed at government in-person proofing facilities such as USDA offices, Post Offices, and state motor vehicle departments might make it easier for commercial identity services to achieve Level 2 compliance at a reasonable per-credential cost.

**Establish templates for business rules and operating agreements when federating government and commercial entities:** E-Authentication has not yet defined business rules and operating rules for federations. This could be an issue for G2B or G2C deployments where AAs federate with commercial CSPs, or

commercial applications federate with Agency CSPs. The E-Authentication Initiative will need to leverage the EAP framework or interim templates for agreements to avoid the need for multiple sets of bilateral agreements as adoption grows.

**Expand relying party guidance:** Relying parties must be given guidelines to ensure they are practicing due diligence and not putting all the responsibility on credential service providers. Particularly for higher risk applications, relying parties should ensure that credentials are still valid before granting access to resources.

**Address liability, dispute resolution and cooperative risk management in government / commercial federations:** Liability is a big question for the E-Authentication Initiative, or any other federated identity deployment scenario. For E-Authentication, several questions arise: What liability should be imposed on federally approved CSPs? How much liability is required? What are the requirements for the relying party? Special circumstances apply because the government is involved. If the Federal government is the CSP, damages can be treated under tort claims since the government prefers not to accept defined liability. When the government is the relying party and a failure occurs, contract provisions can determine the rules outlining proper conduct of all parties. Ideally, contracts would be based on standard templates as discussed above. To ensure commercial acceptance, such templates should ensure fair redress to commercial entities in cases where the government is at fault.

**Proactively address the possibility of security breaches:** Both CSPs and AAs are subject to security breaches that can impact other participants in the E-Authentication Initiative. An attacker could forge assertions or replay stolen assertions in an attempt to defraud a CSP or AA. These attacks are difficult to perform due to the E-Authentication Initiative's use of TLS between components. A scheme that supports digital signatures on assertion messages would make attacks even more difficult. Nevertheless, continuous monitoring is key to detecting security breaches within the federation model, which will allow Agencies or CSPs to respond quickly to a problem. Also, if a CSP or AA suffers a breach to their general security systems (not the assertion system), then a large-scale disclosure of credentials poses a serious threat. In either case, security and media response protocols should provide a coordinated effort to contain the technical and public relations impact of a breach.

**Extend the FPKI investment to enable additional technical trust mechanisms:** The government has invested significant time and resources into its PKI systems and plans to leverage this capability where possible. However, the FPKI system has not yet been adopted by any commercial services, although discussions are

underway with the aerospace industry. Over time, the FPKI has evolved to permit additional trust mechanisms by adding the E-Governance Certificate Authority, FCPF Policy Certificate Authority, and C4 Policy Certificate Authority. These new CA instances shelter some of the FPKI complexity and accommodate more potential cross certifiers.

### **4.3 Other E-Authentication Critical Success Factors**

The E-Authentication program must have strong top-down support, similar to any large and complex project that involves many diverse organizations and divergent requirements. The ESC and GSA must be prepared for the long and arduous process of guiding E-Authentication from infancy to wide adoption in the face of technical, political, funding, and other obstacles.

**Addressing risks to success:** Several risks pose threats to the success of E-Authentication and must be dealt with accordingly. Risks include: not getting enough third party CSP participation, lack of successful AAs, project funding uncertainties, compromise of personal user information or other major security breaches, or technological obsolescence.

To ensure long-term success, E-Authentication must solidify funding to maintain momentum and not scare off tentative Agencies at this time. The E-Authentication Initiative plans to deploy a subscription based funding model where all applications share costs of the program. A flat service fee will be imposed plus an additional fee for transaction volumes. There will need to be enough applications to sustain the program, but also to keep the costs low enough for the agencies to afford. Many AAs have yet to comply with the Government Paperwork Elimination Act (GPEA), so there is a large pool of prospective customers that E-Authentication can garner.

Agency adoption is obviously critical and early pilot testers, including EEX, eTravel, NSF, USDA, VA Grants.gov, and others have given positive marks to this point. But some Agencies are understandably skeptical, having seen IdM initiatives like authentication gateway come and go. Others have seen difficulties with PKI projects. First and foremost, E-Authentication must demonstrate and communicate successes to increase Agency adoption. Also, most Agencies do not have comprehensive studies of their existing or projected identity management and authentication costs in the absence of E-Authentication, and might be more amenable to using E-Authentication if GSA and OMB provide financial justifications. As E-Authentication successes accumulate, OMB can increase formal encouragement for Agencies to participate. Broad adoption by Agencies is also the critical factor in motivating commercial CSPs to invest in supporting the program.

Any handling of sensitive user information opens E-Authentication to potentially damaging results if this data is somehow compromised. E-Authentication must be very particular regarding practices for handling attributes, whether through the federation framework or other back channel mechanisms. Any unauthorized release of data could taint the program, even if it is not directly responsible.

**Dealing with Executive level changes:** Governance challenges will occur with changes in Agency leadership positions, whether a new administration is elected in 2004 or not. E-Authentication opponents may re-emerge during Administration or Cabinet transitions, and the Initiative must be prepared with an effective communications program. This also emphasizes the need for excellent project management that identifies achievable short- and medium-term goals, keeps the project on track, and in continued communication with stakeholders. E-Authentication can minimize the impact of opposing forces by meeting short term objectives, continually growing the number of AAs in the program, re-working the business plan with latest information, and arguing that delays will cause even more incompatible authentication systems to emerge.

See the [E-Authentication Initiative recommendations section](#) for specific guidance on how to address the findings, future considerations, and critical success factors discussed above.

## 5 Electronic Authentication Partnership Analysis

For the Independent Program Review, Burton Group also examined the Electronic Authentication Partnership (EAP), a group consisting of participants from government, commercial industry, higher education, and other segments that is focused on creating authentication interoperability on a broad, nationwide scale.

At the time this report was written, the EAP framework was still being drafted and many provisions had not been approved by the full body of participants. The following sections review the EAP trust model defined so far and discuss findings, discuss future considerations, and present critical success factors.

### 5.1 Electronic Authentication Partnership Trust Model Overview

EAP intends to provide a framework for industry and government alike to leverage digital credentials using the federated identity model. The EAP expects to deliver common policies and practices for credentials, credential issuers, and relying parties that will facilitate interoperability. EAP will also publish the assessment and accreditation process that participants must adhere to. Figure 4 provides a basic diagram of the EAP operational framework.



Figure 4: The EAP Framework

#### Assurance Levels

The EAP Levels of Assurance Work Group is assigned with the task of establishing identity assurance gradations that credential service providers, relying parties, and other entities interact with. EAP is supporting the four E-

Authentication assurance levels on an interim basis in order to leverage an established model during its startup phase. Names for the four levels are different than those used by the E-Authentication Initiative: Assurance level 1 is Minimal, Assurance level 2 is Moderate, Assurance level 3 is Substantial, and Assurance level 4 is High. Using the E-Authentication approach helps to create continuity during the early stages of adoption between and among government and non-government systems. But EAP also proposes to explore an algorithmic model that offers more granularity.

EAP has also adopted the authentication mechanisms outlined by the E-Authentication Initiative as a baseline starting point. Evaluation of additional mechanisms has been deferred to a future date when schedules permit and market requirements demand it.

### **Business Rules and Agreements**

The Business Requirements and Processes (BRP) Workgroup uses an Operational Framework to depict the EAP vision of federated authentication. The Framework comprises a set of business rules and processes, credentials and assurance levels, and accreditation criteria.

The BRP Workgroup has also been developing the general operating rules for EAP credentials. The business rules include legal terms, basic policy, processes, and operational governance, and are intended to replace bi-lateral agreements and immensely streamline the adoption of federation in community or pair-wise scenarios. BRP Workgroup is also creating the operating rules and the process for validating credentials.

EAP is striving to eliminate all the bi-lateral negotiations and contract agreements that might otherwise be required without common business rules. Parties that sign operating rules agreements will know their obligations up front and shouldn't need additional authentication contract terms codified, although additions are not prohibited. A set of base rules will apply to all parties and additional modular sets of rules may be applied to CSPs. Certain rules govern eligibility and participation. CSPs must first be certified before they are eligible to sign an agreement, which binds them to the rules contained in it. At the time this report was published, the EAP participants had not decided on agreement requirements for relying parties and end users.

The operating rules will contain dispute resolution steps for each type of participant, should any of them raise issue with an EAP enabled system. At the time this report was published, the EAP participants had not decided whether the EAP would act as an arbitrator of disputes, or turn them over to third parties for resolution.

Default liability positions state that CSPs are not liable for losses incurred by a Relying Party if the CSP followed operating rules. Further, any liability is for authentication only and does not include authorization services. In a recent development, EAP has decoupled liability from the assurance level. That is, CSPs can provide a high assurance identity that comes with a low level of liability. CSPs that issue EAP branded credentials, though, must provide quantifiable recourse at each assurance level that it offers.

The operating rules state that EAP will not be held responsible for any losses or other liability for actions taken while using EAP branded credentials, but this may be challenged if serious consequences occur. EAP participants, however, can be penalized through a variety of measures, including censure, fines, suspension, and termination.

### **Assessment Framework, Criteria, and Methodology**

The Credential Services Assessment Criteria (CSAC) subgroup is developing a standard set of criteria for evaluating and approving credential service providers for participation in EAP branded systems. This subgroup also is creating guidelines for those who will be responsible for conducting assessments to ensure consistent results.

CSAC chose to leverage and extend existing work as it created the EAP assessment framework instead of creating unique approaches for EAP. A set of Services Assessment Criteria (SAC) have been drafted that uses the Credential Assessment Framework of the E-Authentication Initiative as a basis. It includes Common Service Assessment Criteria (CO-SAC), Identity Proofing Service Assessment Criteria (ID-SAC), and Credential Management Service Assessment Criteria (CM-SAC). By following the E-Authentication format, EAP fosters continuity between government and industry authentication systems, while creating EAP specific extensions and modifications. CSAC extends the model by breaking credential service providers into more discrete functions covering identity proofing, authentication, status management and credential issuance.

In addition to leveraging E-Authentication, OMB, and NIST efforts, CSAC is using work from Mortgage Bankers Association (MBAA), Federal PKI, ISO 17799, tScheme, and National Safety Council (NSC). This range of standardization and certification inputs helps to broaden the EAP foundation to support an any-to-any model rather than just a government-to-industry model.

### **Evaluation, Accreditation and Compliance**

Another subgroup, the Evaluation, Accreditation, and Compliance Work Group is drafting guidelines for use in accrediting assessors that will be evaluating

credential service providers. This subgroup is also creating the process and criteria for certifying CSPs that are seeking EAP branding.

## **Governance**

EAP is presently operating under an interim organizational structure with four working groups:

- **Credential standards and levels of assurance:** Defining rules for relying upon, trusting, and using credentials issued by others for the purpose of online authentication, and for assessing the risks of relying upon these credentials according to various assurance levels.
- **Business requirements and processes:** Defining business models and use cases for interoperable authentication and trust.
- **Evaluation, accreditation, and compliance:** Developing a framework of policies and criteria for use in accrediting credentials providers for various assurance levels.
- **EAP governance:** Defining the EAP's ultimate governance structure.

All the working groups are operating under a timeline to produce draft documents by Labor Day for the full EAP to review. A full EAP Framework is planned for December, 2004.

After the framework is complete, EAP will become a member-governed and funded organization. It would maintain its framework of federated authentication business rules and operational guidelines, and accredit CSPs. EAP is also considering whether to operate federation infrastructure services itself.

EAP has developed draft bylaws that explain membership levels, duties for the board of directors, officer levels, and committees and workgroups for the permanent organization. The board of directors consists of elected and appointed members. Two thirds of the board will be determined through an election process and the remaining third will be appointed to ensure the broadest set of interests are represented.

Membership levels consist of Business (for profit firms) and Non-Business (nonprofit organizations or government agencies) interested in e-authentication issues. The schedule for membership dues has not been established at this time, but will have a tier structure to allow participation by a variety of organizations.

Officers for EAP include Chair, Vice Chair, Secretary, Treasurer, and President. The Board of Directors elects the Chair, Vice Chair, Secretary, and Treasurer for one year terms and may appoint the President as the executive director for EAP.

## **5.2 EAP Trust Model – Findings**

The Electronic Authentication Partnership includes members from government, commercial enterprises, and other segments that can greatly expand the pool of certified and interoperable credentials. EAP is taking a comprehensive approach to federated authentication that includes evaluation criteria, assessment methodologies, and accreditation guidelines to ensure consistency, interoperability, and trust. Building upon the work of E-Authentication Initiative, EAP is seeking to extend the framework to one more broadly applicable outside government centric applications.

The EAP is an attempt to overcome market failure by consolidating naturally occurring market forces and supportive government intervention to build trust, interoperability, and confidence in federated identity systems. EAP supporters understand the value its organization can bring to the industry, but realize they must avoid some of the pitfalls that previous government/industry partnerships, like the Internet Corporation for Assigned Names and Numbers (ICANN), have experienced in the past. But federation is very much a political and organizational issue, and topics such as privacy are very sensitive flashpoints.

**Determining the EAP's long term direction, and operational mode:** EAP has yet to determine whether it will be a standards body, an operator of federation infrastructure, or both. Most of the energy to establish EAP has been focused on developing the business rules and agreements that participants must adhere to, but there may be circumstances where EAP becomes compelled to provide infrastructure services - such as handling trust lists, metadata, accreditation, directory services or portals - on behalf of federated communities so as to spur adoption.

The degree to which membership wishes to maintain control over EAP business rules is a primary factor that will determine which direction EAP takes on the infrastructure issue. If rigid control over business rules is desired, then EAP may have to shoulder the burden of operating federation infrastructure to prevent deviation from approved practices. However, a strict control model is likely to be less appealing to the broad market where EAP hopes to garner wide adoption. A more flexible approach could be provided by accrediting industry communities that accept the EAP framework, make extensions or changes within reasonable limits to meet community-specific requirements, and operate their own infrastructure.

Added flexibility means somewhat less control for EAP as adopters may seek change control authority over assessment criteria or other baseline functions. Some market segments may wish to adopt EAP business rules and map accreditation requirements to leverage audits that have already been performed and paid for. For example, service providers that have already performed a WebTrust assessment would like to map it to EAP criteria, and conduct only an incremental assessment for EAP.

Beyond maintaining control over EAP business rules, other factors will influence whether EAP operates federation infrastructure. Available funding, market timing, and the level of early adopter participation are all critical elements in this decision making process. Lack of funding will clearly deter forays into the operation of infrastructure services as it entails expenses for interoperability testing, data center facilities, and staffing. Moreover, if EAP does decide to provide federation infrastructure, it must be careful not to do so in a way that stifles adoption by competing with the same commercial CSPs that form part of the membership and wish to adopt the EAP framework.

**Balancing commercial and government or academic interests is challenging:**

Several regular EAP attendees and contributors informally expressed some concerns that EAP is not focused enough on practical business concerns and is too theoretical in some instances. Whether real or imagined, EAP has fostered this impression because of strong academic and Government representation. While the representatives we contacted had no complaints that Government representation was at all heavy handed, there was a concern that it tilts EAP to positions that are not necessarily commercially viable. It should also be noted, however, that providers and vendors dominate commercial representation at the EAP; commercial relying party views, if more heavily represented, might be more in accord with government views.

**How will dispute resolution work in practice?** While EAP is constructing thorough dispute resolution procedures, several challenges remain before it can be declared successful. First, Relying Parties and CSPs have to recognize the value of dispute resolution processes that limit or eliminate legal recourse. There may be certain types of applications or transactions where Relying Parties may prefer more options for recourse that include legal measures.

Second, the effectiveness of dispute resolution by EAP is an unknown quantity at this point. It is preferable that most disputes will be resolved between parties using the procedures instituted by EAP. But EAP may be required to arbitrate a high percentage of disputes, which overburdens EAP staff and could lead to negative perceptions in the market or to litigation against the EAP.

**Liability parameters are untested:** EAP is attempting to assign strict liability levels to all participants as well as itself for federated authentication scenarios. CSPs have shown some reluctance to sign up for currently constructed liability models, so this may have to be adjusted for broader acceptance. In a society that sues with little to no provocation, the EAP's liability measures seem destined to be tested vigorously.

**Rules for Relying Parties:** EAP does not anticipate conducting assessments on Relying Parties as it will for CSPs. This could become an issue in the future during dispute resolution if CSPs feel they are being excessively held to a higher standard than RP counterparts. EAP must further evaluate if business rules adequately provide assurance that RPs are operating within the intent and letter of their agreements.

### ***5.3 EAP Trust Model – Future Considerations***

The effort to launch and stabilize EAP is producing a flurry of activity and continuous change as all the work groups meet and circulate new document drafts. Only active participants have a chance to keep up at this point, which can make it difficult for prospective members to decide whether or not to join. While this controlled chaos can be overwhelming for some, EAP is under pressure at the same time to move quickly to establish federated authentication frameworks. If EAP delays or is not successful, competitive groups might emerge. Longer term, global communities like the European Union could also establish standards or frameworks that could impact national trade negatively or limit U.S. ability to influence international standards.

**Biggest obstacles to success:** Several issues pose considerable obstacles to the ultimate success of EAP and should be addressed by interim and permanent leadership. They include membership dues structure, reliance on volunteer labor, complexity of federation, and potential legal costs. The membership dues structure must support startup and operational costs of EAP, but equitably share the expense across as many entities as possible. To date, EAP has relied heavily on volunteer labor to construct the documents and processes that EAP is based on. Many who would otherwise be actively involved are overly consumed by their "day jobs" and have not been able to contribute even though their input is of paramount importance. Indeed, current volunteers can have their priorities changed at a moments notice, causing them to abandon or limit EAP work. Building federation agreements among many divergent industries is very challenging and complex, which is taxing on participants and could result in some early mistakes or challenges. EAP will be challenged to keep leadership and workgroup participants engaged over the long term required to reach success. Finally, EAP is working on a structure to limit liability of participants in a federated authentication model. This effort will require considerable legal input

and review up front and could consume more resources than expected to monitor the program.

**Building a strategic plan:** The first phase of EAP has addressed some of the big ticket items to get the organization started. These include adoption of the Federal Four levels of assurance and development of accreditation guidelines as well creating initial EAP accreditation processes and liability guidelines. A longer-term strategic plan is needed to address additional challenges and keep the EAP moving on the path to success. A strategic plan and roadmap should include steps to put EAP on a solid financial footing by obtaining funding from a wide range of participants. In 2005, much work is needed to develop accreditation partners and services, and recruit additional industry support. The EAP will also have to address some of the back burner issues, described later, that have been avoided in order to get the organization off the ground. Continued progress on these items will broaden the appeal of EAP and meet more requirements of potential participants. Later in 2005 and early 2006, EAP should push to have production services in place using the initial framework and have a migration path to enhanced or extended services.

Production services could be provided by other organizations, or they could include EAP operated federation infrastructure to spur adoption of services or markets that can't get started without some outside assistance. Commercial vendors, auditors, and service providers will expect clear signals from EAP so that they can make their own investment decisions.

**Dealing with overlaps:** Overlaps with other federation initiatives such as Liberty Alliance are emerging as the EAP develops its operating rules and other documentation. This can generate confusion in the market if prospective members can't easily distinguish between similar efforts. For the relative novice on federated authentication, it can appear difficult to determine whether to adopt the EAP program, Liberty Alliance, WS-\*, or just install a specific federation product. EAP can help to reduce some chaos or confusion by working more closely with efforts such as Liberty Alliance, Web Services Interoperability Organization (WS-I), Banking Information Technology Secretariat (BITS), or Identrus to share operating rules, interoperability testing, or certification practices.

**Beyond authentication:** Like the E-Authentication Initiative, EAP has put authorization and lifecycle management issues on the back burner to concentrate on authentication. It's important for large, complex projects to concentrate on the short-term achievable goals first, but prospective EAP adopters need a more holistic roadmap for federated identity that includes authorization and lifecycle identity management. For many federations liability, dispute resolution, and

trust must address more than just authentication. The challenge is to encourage organizations and industries to use the EAP framework as a starting point, even though they will often need to create agreements and processes in addition to EAP's.

**Technical considerations:** At present, the EAP is trying to keep its business rules and operating agreements technology neutral so that multiple federation standards could be employed. However, some technical issues such as the handling of error conditions have security implications, and need to be included in operating agreements and assessment criteria. If the EAP decides to take on infrastructure roles, additional technical considerations – such as interoperability testing – might apply. The challenge is to encourage technical standards organizations, and audit or assessment organizations, to adopt the EAP framework in the context of actual standards in real world use. The EAP Assurance Levels workgroup recently formed an Interoperability sub-group to begin examining technical issues.

**Competing efforts:** EAP is attempting to build a flexible enough framework to garner wide adoption, but industry segments may remain that have specific requirements that can't be met by a general-purpose architecture. In some cases, competing efforts may overlap with EAP and potentially limit participation. Organizations such as financial services that already undergo heavy audit and assessment processes will not welcome additional assessment from EAP that do not piggyback on the time and money they have already spent. The challenge is to dovetail EAP assessment – at least partially – with WebTrust or other existing audits.

In one example, BITS has undertaken an effort to improve software stability and security for the financial industry in particular as well as the industry at large. Part of this effort includes a certification program to identify software that meets certain minimum requirements. EAP may be able to leverage or partner with BITS to benefit from this certification process that is now in its third year of operation.

**Accreditation of auditors:** EAP has been developing the standards for accreditation of CSPs, but has yet to define the rules and processes for accrediting the auditors that will conduct assessments. This is another case where EAP can leverage the work in other organizations, such as BITS, ISACA, and NIST, to kick start the assessment program.

#### **5.4 Other Critical Success Factors for the EAP**

EAP faces many challenges to reach its lofty goals of interoperable authentication between government, commercial, and other parties. Many industries are

represented in current EAP working groups, but success will be judged by how many industries sign up for the EAP framework and then by how many federations in multiple industries deploy EAP-branded services. To reach broad adoption, EAP must be compelling enough to attract IdM technology vendors, all levels of government agencies, higher education, financial services, health, and many other industries. Support from large identity-based communities such as Amazon.com, eBay, Yahoo, or AOL could lend significant credibility to the EAP program. Several other industry specific projects like Internet2, Secure Access for Everyone (SAFE), and the Aerospace Bridge provide mutually beneficial opportunities for EAP.

**Transitioning to a permanent management structure:** Much work remains to take EAP from an interim body funded primarily by GSA to an independent organization with a clear mission, strong leadership, and good prospects for success. First, there are several governance, policy, business rules, methodology, and other documents to finalize by year end 2004. A new management team must be elected that can maintain momentum and develop a marketing strategy that attracts more members and support. It will be a tough balancing act to satisfy all the diverse interests of a large, successful membership.

The new EAP leadership must also plan a transition from the theoretical phase it is now engaged in to one where the industry at large is putting the EAP program into practice. There are many moving parts that have to act together in concert for EAP to be effective and successful.

**Kick starting the assessment and accreditation process:** To facilitate adoption, the accreditation and audit process must quickly ramp up to certify all the potential participants. A backlog of applicants or faulty process can delay early adopters and give a bad impression to those waiting for the first wave to go through the break in period.

**Funding model:** The new EAP funding model must strike a delicate balance between supporting the startup and operating costs of the organization while being affordable enough to foster a large membership. Several current and prospective members are waiting for the dues structure to solidify before committing. EAP must be careful to not implement a dues model that doesn't permit small but valuable companies from participating.

**Building a compelling business model:** The fastest path to broad commercial CSP and RP adoption is one paved with compelling business value. Federation is still in the early adopter phase and many in the industry may not be able to visualize the value in this architectural approach. The industry may need to see

various practical business scenarios that describe the value of the EAP model for end users, CSPs, and applications.

**In-person proofing challenges:** Only a subset of CSPs have the infrastructure or capability to meet face-to-face with users to reach Level 2 or higher assurance levels. Financial institutions with their branch locations, USDA extension offices, state motor vehicle centers, and US Postal Offices are a few institutions that can meet end users in person, check various physical credentials, and issue higher assurance digital credentials. EAP should study ways to leverage identity proofing infrastructure so that not only could identity proofing organizations become CSPs themselves, but also open the possibility of extending their capabilities to other CSPs without running afoul of privacy and civil liberty interests.

## **6 Recommendations**

The following sections extrapolate from industry perspectives as well as E-Authentication and EAP findings and future considerations to provide recommendations for both programs.

### **6.1 Recommendations for the E-Authentication Initiative**

The E-Authentication Initiative has already developed a sound initial Technical Approach, established an interoperability test environment, and fostered key partnerships within the industry and government agencies alike that are crucial to the overall success of the project. Although more hard work and challenges lie ahead, the E-Authentication Initiative should be continued with the government's full support. Without E-Authentication, many Agencies would eventually have to establish federations by conducting their own specification, assessment, testing, industry outreach, contracting, and other activities with much less reusability, at much higher cost and other E-Gov objectives would be set back.

This section identifies additional recommendations that should be considered by the E-Authentication Initiative as a way of improving the overall program and its chances for gaining wide acceptance across various government Agencies and commercial organizations.

#### **Near Term Recommendations**

In the near term, the E-Authentication Initiative should:

- Update the Strategic Business Plan with a focus on increasing Agency adoption and involving commercial CSPs
- Mitigate risks that could lead to breaches through tight security and well-defined business and operating rules
- Continue communicating the E-Authentication Initiative's efforts and successes
- Involve state applications, CSPs, and other entities outside of the Federal Agency framework
- Continue to support and promote the EAP
- Refine and improve audit and accreditation programs based on industry input
- Define business rules, operating agreements, and contract terms for working with commercial CSPs and relying parties

**Update the Strategic Business Plan with a focus on increasing Agency adoption and involving commercial CSPs:** The current Strategic Business Plan addresses the long term E-Authentication vision and identifies performance measures, but many of the milestones in the plan have already been successfully completed. A new plan that brings the same degree of focus and transparency to E-Authentication efforts in FY05 and FY06 is required to help the initiative weather the election year and other organizational transitions. This plan should incorporate Exhibit 300 documentation, but in a more readable format. Early efforts under the new plan should include successfully completing current pilots, incorporating usability and deployment lessons learned, obtaining more detailed information on Agency needs than was forthcoming in the July 25 Data Call, recruiting additional Agency partners, developing business models or incentives necessary to recruit commercial CSP support, and addressing other recommendations below as appropriate. The more Agencies that adopt E-Authentication, and the more formal encouragement exerted by OMB, the more motivation commercial CSPs will have to invest in supporting E-Authentication compliant services.

**Mitigate risks that could lead to breaches through tight security and well-defined business and operating rules:** Each AA and CSP should be assessed (or existing assessments reviewed) for possible consequences from a security breach, and response plans should exist to mitigate consequences. Applications that serve the public are more sensitive than internal or inter-agency applications and should be treated with extra diligence. The assessment and response plans should be documented and the Agency or CSP should be prepared to show that due diligence was taken should a breach occur.

The E-Authentication infrastructure team should assess ways to prevent a breach of assertion security and implement means for detecting a breach quickly if it were to occur. Steps that can be taken include assuring the integrity of insiders with access to the infrastructure, strong key management, and well-defined audit log management and review procedures. The E-Authentication Initiative should not wait for the EAP to develop operating rules for G2B and G2C interactions; it should bring the same specificity to operational federations that it has brought to CSP assessment by developing or employing reusable templates for federation agreements.

If a breach occurs, E-Authentication must be prepared to respond from a technical and public relations perspective. A plan should designate who responds to a breach and how the process will escalate among E-Authentication, AA, and CSP staff. If the breach is not assertion-related, management should be ready to make this case and indicate that additional reviews of CAF/CAG guidelines will be performed if necessary. For an assertion-related breach that is

detected quickly, the response plan could communicate that security problems occurred but E-Authentication has taken measures that resulted in fast detection and this proves the security of the program. In the event of a long-running assertion breach, E-Authentication would face more serious repercussions because not one, but all, CSPs and AAs rely on the assertion mechanism. People, tools, processes, and audits should be continually deployed to mitigate any possibility of a long-running assertion breach due to the high risk it would pose to the program.

**Continue communicating the E-Authentication Initiative's efforts and successes:** The E-Authentication Initiative has made very significant strides to date in several areas and should be actively marketing these accomplishments internally to government agencies and the industry at large. The government recognized that federation is the right model to use for sharing authentication services between security domains and has laid out a strong technical architecture to reach its long term goals. Along the way, E-Authentication (along with others like NIST and OMB) is outlining identity assurance levels, matching authentication mechanisms, assessment criteria, and other guidelines that can be very valuable to all industries. E-Authentication interoperability testing far surpasses any other efforts in the industry, and the entire industry will benefit from the Government's efforts. By being more aggressive about spreading the good news, E-Authentication can raise awareness, build more confidence in the program, and help to recruit additional participants.

**Involve state applications, CSPs, and other entities outside of the Agency framework:** In addition to the pilot applications already undergoing testing, the E-Authentication Initiative should strive to include other non-Federal applications in order to generate additional interest in the program. For example, some states are reviewing federated identity solutions for businesses to access various state government applications distributed across multiple state agencies. Other states are looking to improve citizen's access to government applications using federated identity solutions.

State-based initiatives are in early stages of development, and are faced with many of the same issues the E-Authentication Initiative is currently solving for the government. The E-Authentication Initiative and the EAP should proactively work towards engaging more state governments to act as CSPs and/or AAs, and the E-Authentication Initiative, the EAP, or some new working group should be charged to coordinate government sponsored authentication-related efforts so the public perceives E-Authentication, the EAP, and state-based initiatives as cooperative efforts that are all working toward the same goal to the benefit of citizens and businesses.

**Continue to support and promote the EAP:** Although the EAP framework will take time to mature, from the government's standpoint, EAP represents an excellent opportunity to extend the effectiveness of the E-Authentication Initiative. The E-Authentication Initiative should continue to support and promote EAP, even though the government will likely require interim business rules and operating agreements for government to business (G2B) as well as government to consumer (G2C) federations.

**Refine and improve audit and accreditation programs based on industry input through the EAP or other sources:** Based on a comparison of the Secure Identity Services Accreditation Corporation (SISAC) assessment framework with that of E-Authentication Initiative, a study by A&Y Associates provided a number of additional recommendations. The study suggests (and Burton Group concurs) that it should be possible to assess CSPs' credential issuance functions separately from the runtime authentication and federation services. This is similar to the PKI model where Registration Authorities perform the function of identity vetting and credential issuance and the Certificate Authority sets the general policy controls for each level of assurance. More work is also needed on the audit and accreditation program; E-Authentication should describe the necessary experience levels for assessors and engage more directly with commercial audit firms to validate concepts and gain access to additional assessment resources.

**Define business rules, operating agreements, and contract terms for working with commercial CSPs and relying parties:** In the area of liability and dispute resolution, E-Authentication should continue current efforts to define additional guidelines to build more confidence among commercial partners. The guidelines under development should define requirements that relying parties must follow to participate in E-Authentication and enhance the agreement structure to bind relying parties more closely with credential issuers, and provide commercial partners with defined recourse in disputes with government. Because the EAP framework is evolving with commercial input and is already influenced by SISAC, the E-Authentication Initiative could also plan to make changes for EAP compatibility at a later time.

## Longer Term Recommendations

In the longer term, the E-Authentication Initiative should:

- Enhance support for application and identity lifecycle requirements while taking a proactive approach on privacy
- Add additional standards to the roadmap, converging on SAML 2.0 over a 2-3 year time frame
- Develop requirements for scheme translators jointly with industry, to allow modular adaptation to future standards
- Continue interoperability testing efforts
- Develop more options for higher assurance authentication, especially for non-government users

**Enhance support for application and identity lifecycle requirements while taking a proactive approach on privacy:** In addition to the guidance provided in CAF, OMB, and NIST documentation, E-Authentication can help stakeholders be successful by providing technical, privacy compliance, and project management guidelines or tools for applications and CSPs endeavoring to deploy functionality across the digital identity lifecycle of account activation, name mapping, authentication, name change, and de-activation as well as, in some cases, attribute or role information exchanges. Although these functions are currently considered out-of-scope and may not impact all E-Authentication components directly, Agencies will be looking to the E-Authentication Initiative for expertise, guidance and solutions. Initial guidance should be provided in the near term to facilitate deployment planning.

Over the long term, the E-Authentication Initiative should also consider supporting rich attribute exchange through the federation protocols themselves to support application personalization or authorization functions. While these changes would introduce additional requirements for privacy planning, lifecycle identity requirements necessitate data exchange and raise privacy issues regardless. The government might benefit from taking a holistic, proactive approach to privacy and developing capability maturity models across CSPs and applications that interact with one another, and with users.

Ideas and alternatives should be exchanged between developers and architects of existing or planned pilot applications via E-Authentication sponsored meetings that provide agencies with a more holistic framework. The facilitated process could ultimately provide a roadmap to future services that support identity lifecycle requirements and privacy compliance planning. Agencies are more likely to participate if they understand and can influence the longer term vision. Privacy advocacy organizations should be consulted on both technical and

process measures as the E-Authentication Initiative (or other components of the Federal Enterprise Architecture) work to provide more comprehensive identity management services in support of E-Gov programs.

**Add additional standards to the roadmap, converging on SAML 2.0 over a 2-3 year time frame:** The ultimate roadmap should identify additional standards as discussed in the section on [E-Authentication Technical Architecture and Interoperability - Future Considerations](#). SAML 1.1, Shibboleth, SAML 2.0, and Liberty Alliance address some of the technical shortcomings of SAML 1.0 with signed assertions, global logout, account linking, attribute exchange, and additional capabilities. But due to the cost and complexity of testing and support for multiple federation schemes, the E-Authentication Initiative should selectively support only those standards that provide the biggest incremental increase in stakeholder value, functionality and usability.

Based on the findings on emerging federation standards from [Table 1](#), the E-Authentication Initiative should support SAML 1.1. and the browser/post profile in the near term, provided a joint program can be planned to enable Shibboleth interoperability with universities and significant stakeholder value achieved in more than one Agency. (Note that studies are actively underway to evaluate Shibboleth interoperability.) Liberty Alliance ID-FF 1.1 or 1.2 support could also be considered if major application stakeholders emerge.

SAML 2.0 represents the best long term opportunity to reach a point of stability in standards. The E-Authentication Initiative should attempt to accelerate industry development of interoperable SAML 2.0 products and deployments by participating in meetings to profile the standard once it is completed, and by funding or encouraging early SAML 2.0 conformance or interoperability testing efforts.

The E-Authentication Initiative should also monitor the WS-\* standards suite as it matures, and as Agencies develop requirements for federating Web services as well as browser-enabled applications.

**Continue interoperability testing efforts, and develop requirements for scheme translators jointly with industry:** As the E-Authentication continues to evolve and supports additional standards and specifications, interoperability will continue to be a challenge. As the federated identity standards continue to mature, interoperability testing of SAML 1.0 will become less important, while interoperability testing of more recent specifications will become more pressing. While industry is relatively unlikely to assume all of the interoperability testing burden for large federations such as the Government and its trading partners, over time, the E-Authentication Initiative should consider relying more heavily

on NIST and/or work with industry to find ways to seed improved commercial testing tools and services that raise the base level of conformance or interoperability of the products coming in for Federal testing.

Once multiple standards are supported, scheme translator deployment and testing will become a significant and complex task. The E-Authentication Initiative should begin developing requirements for scheme translators that will provide the necessary layer of abstraction and flexibility as standards change. These requirements should be developed jointly with, or reviewed periodically with vendors so as to maximize COTS componentry and thus reduce long term costs.

**Develop more options for higher assurance authentication:** Most applications are expected to operate at Level 1 and 2 assurance levels, but a very important segment will require higher levels of assurance. To meet these requirements, E-Authentication should work to certify more authentication methods at Levels 3 and 4, support assertions at Level 3, and study the security of assertions at Level 4. Based on NIST analysis, E-Authentication only supports hard cryptographic tokens such as smartcards at Level 4.

However, E-Authentication should not rely just on PKI for the higher levels of assurance. NIST should continue to evaluate one time password generators, biometrics, and knowledge based authentication mechanisms to provide a full range of options. Where appropriate, NIST should also point out shortcomings that are keeping specific authentication systems from reaching higher assurance levels, giving industry a clear path to improvement. In addition to investigating additional authentication mechanisms, NIST should also examine how assertions can be securely implemented at Levels 3 and 4. Security improvements have been introduced in SAML 1.1 and further enhancements are being added to SAML 2.0 (due to complete year end 2004) and NIST should provide an analysis of these schemes in a timely manner to aid E-Authentication progress.

NIST and FPKI are making strides to improve the Federal PKI environment, but there is more work to do. The groups should continue working on open issues related to the validation of Bridge certificates and interoperability with Windows platforms and applications. NIST and FPKI should continue to improve Bridge functionality and work with Microsoft and other vendors to provide workable, standards-based solutions for path discovery and validation in a bridge environment.

## **6.2 Recommendations for the Electronic Authentication Partnership**

The Electronic Authentication Partnership is quickly ramping up its organizational structure to meet end of year 2004 deadlines. The following recommendations are offered to assist in the final phases of interim planning and provide a solid foundation for success with government and industry participants.

### **Near Term Recommendations**

In the near term, the EAP should focus on completing current tasks, solidify the audit and assessment process while avoiding excessive liability exposure, and determine technical criteria for operational rules.

**Focus on completing current tasks:** EAP has a full plate of deliverables to complete by year end 2004 and plenty of additional work to transition into the permanent organizational structure. EAP should concentrate on this initial phase of work before venturing to additional areas. When moving to the next phase, EAP should actively engage other industry groups rather than going it alone. Building additional partnerships will be more effective in building support for EAP and the organization should also seek to become the launching pad for other identity networks that can serve more specific interests.

Business rules must be sufficiently technical to effectively support the complex nature of federated identity systems. While EAP may not require a testing facility such as the E-Authentication Interoperability Lab, it can't ignore technical issues. Operating rules and assessment criteria need to address – at a minimum – technical federation issues concerning standards versions, security protections, required or prohibited features, and audit logging. It is possible that federations may emerge with different profiles based on the EAP framework, and these profiles may introduce interoperability and security issues that require assessment for EAP compliance. EAP must ensure that EAP sanctioned auditors can clearly determine if service providers are or are not in compliance with EAP standards.

**Solidify the audit and assessment process:** Many questions remain about the audit and assessment process. EAP has yet to determine who will conduct audits or what level of liability auditors will be responsible for. EAP should engage the commercial audit industry to evaluate potential outcomes for this issue. EAP should also reach out to organizations like the Information Systems Audit and Control Association (ISACA) to seek additional opportunities for commercial auditing professionals. BITS, the Technology Group for the Financial Services Round Table has been conducting extensive analysis for assessing and certifying

the security of commercial software systems and EAP should attempt to work with BITS in a mutually beneficial manner on this topic.

**Avoid excessive liability exposure:** EAP may be taking on more responsibility as an arbitrator than is reasonable for a non-sovereign entity. EAP should be careful not to over extend in this area and leave itself open to litigation. A possible solution is to certify independent arbitrators and require that CSPs and relying parties use one of these arbitrators. This can also have the advantage of encouraging the legal community to support EAP with their involvement.

**Determine technical criteria for EAP operational rules:** EAP must determine how tightly to bind the operational and business rules to specific technologies. It is recommended that EAP develop a modular framework that is independent of particular technical standards to provide more choices for prospective implementers. A single set of business rules should be leveraged across multiple federation standards, including SAML, Liberty Alliance, and WS-\*.

## **Longer Term Recommendations**

Longer term, the EAP should conduct strategic planning beyond January 2005, determine if the organization should provide federation infrastructure services or just standards, and reach out to extend commercial involvement.

**Conduct strategic planning beyond January 2005:** Despite all the effort required to meet end of year 2004 deadlines, EAP should be looking to the next phase in order to anticipate requirements and keep the momentum moving forward. Several back burner issues like one time tokens, biometrics, attribute exchange and other issues will need to be dealt with early on by the new management team. Once EAP officially launches in January 2005, committees should be established to focus on technical, legal, business, marketing, membership, press relations, and other issues – with clear objectives and short timelines. Specific, measurable objectives should be defined for conducting joint efforts with standards bodies, industry associations, or federations that could be early adopters of EAP.

**Determine EAP's long term operational model:** A key issue to address is the operational model that EAP will adopt for the long term and decide whether to just develop business and operating rules, operate federation services, or provide both services to the industry. EAP should continue to push for the adoption of EAP authentication by federations where a certain amount of flexibility is granted to modify or extend the basic model. EAP can also choose to provide federation services itself or through a close partner where necessary to spur adoption or when market opportunities emerge.

**Reach out to extend commercial involvement:** The Electronic Authentication Partnership is making good strides as it transitions from a startup organization chiefly funded by GSA to a stand-alone organization starting in 2005. But EAP must be careful not to be painted in perception or reality as beholden primarily to the government and its interests. EAP should move to obtain more commercial involvement (by relying parties as well as service providers) in significant management and workgroup positions to make the organization truly balanced. To foster additional commercial involvement, EAP could also schedule seminars or other meetings outside of Washington DC as part of an outreach program. Visits to New York to meet with financial services, the Midwest for manufacturing concerns, and California to meet with technology providers can further demonstrate EAP's commitment to the commercial sector and provide direct feedback to the partnership. This outreach program must also be adequately funded to ensure its effectiveness.

## 7 Conclusion

The E-Authentication Initiative is off to an excellent start, has gained momentum over time, and has fostered a number of partnerships critical to its success. However, the initiative should expect to face an increasing number of difficult challenges in the near future that will determine the overall success or failure of the project in the long run.

Success or failure will depend on the overall success of the pilots, the number of CSPs and AAs that “opt-in” and participate over time, and the initiative’s ability to manage a complex set of end-user, CSP, and Agency needs even if these needs extend beyond authentication. The E-Authentication Initiative must quickly react to citizen’s needs concerning privacy and usability, business needs for quickly establishing trust relationships and limiting liabilities, Agency needs for authenticating users and simplifying access control, and Federal as well as state government’s needs to become more efficient and effective when interacting with citizens, businesses, and employees.

These factors will force the E-Authentication Initiative to fine-tune its plans over time to include support for additional standards, address privacy, trust, and liability head-on, and develop plans for more proactive programs promoting the use of federated identity standards as the most efficient and logical way for citizens and businesses to interact with Federal Agencies as well as state and local agencies via the Internet.

As the number of applications and services available through the portal increases, the demand for additional CSPs should also increase. This “snowball” effect will signal the success of the E-Authentication Initiative.

## 8 References

[E-Authentication Initiative Web Site](#)

[Electronic Authentication Partnership Web Site](#)

[National Institute of Standards \(NIST\) Special Publication 800-63](#)

[Office of Management and Budget \(OMB\) Memorandum M-04-04](#)

[Technical Approach for the Authentication Service Component](#)

[Approved E-Authentication Providers List](#)

U.S. Federal Government Credential Assessment Framework Suite and Mortgage Bankers Association Secure Identity Services Accreditation Framework: A Comparison White Paper

[Burton Group Directory and Security Strategies \(DSS\) documents:](#)

- SAML: Bringing on the First Wave of Federation
- WS-\*: A Composable Framework for Web Services Security
- How Can We Achieve Trust in E-Business?
- Federated Identity Management: Early Adopter Case Studies and Lessons Learned
- Toward Federated Identity Management: The Journey Continues
- Liberty Alliance: Meeting Early Adopter Requirements
- Enterprise Identity Management: It's About the Business

## **9. Appendix A: Authentication, Identity Management, and Federation**

Authentication is part of the larger problem of digital identity management (IdM). In a networked computing environment such as the Internet, or even an Agency's private network, people and applications do not interact physically and may be separated by wide distances and multiple technical components. On the network, people assume "digital identities" –electronic representations of themselves – asserted by the computers or applications claiming to act on their behalf. There are multiple digital identities for a person acting in different roles or using different applications. Each digital identity may reflect a person's actual (or legal) name, or it may be pseudonymous.

A complex mix of processes and technologies – including authentication, user administration, authorization, directory services, and audit - are required to manage digital identities. Through the act of authentication, computers and applications challenge persons (or systems acting on their behalf) to present credentials, or proofs of their physical identity. Once a user is authenticated, systems and applications may authorize the user to perform actions such as reading or writing files, based on access control information such as group memberships or roles associated with the user.

Credentials used for authentication comprise account identifiers, passwords, biometrics, cryptographic tokens or other "factors" established in advance during user administration. But credentials are only as accurate as the identity proofing, or verification of the real user, at initial setup time, and only as strong as the technical means of storing, checking or transmitting the credentials over the network. Once disclosed to the wrong parties, credentials can be used fraudulently to impersonate the user or to obtain their private information. Security, convenience, and privacy have a paradoxical relationship in identity management: the more value we put online, the more digital identities we create and the more we rely on them. Multiple identities create inconvenience for users who must carry or remember multiple credentials; attempts to consolidate, or link, identities enable reduced sign on convenience but increase privacy risk.

As increased connectivity and e-business have loaded more and more value onto computer applications and the Internet, the need for IdM has mushroomed and the consequences of digital identity abuse have risen with the value of activities and rise of privacy regulations. In response to the growing importance, complexity, and cost of IdM organizations across the world have for several

years been seeking to consolidate silos of IdM in disparate applications into a reduced number of general-purpose systems with higher assurance.

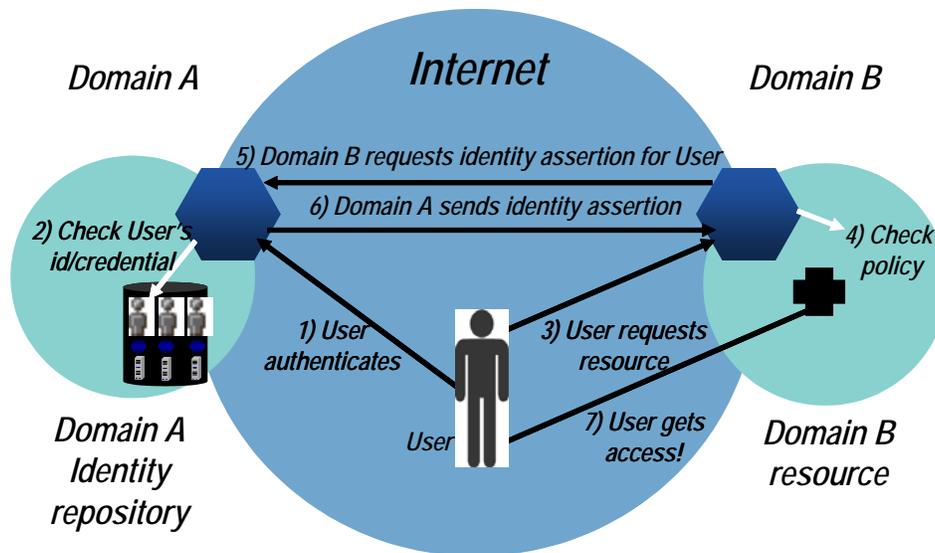
IdM consolidation and integration is the recommended approach for enterprises, including organizations such as individual Federal agencies. However, in the multi-domain environments such as the government, an industry, or the Internet itself it is not cost effective or even always possible for an enterprise to aggregate information about all the users in the general public or partner organizations that it might eventually interact with. Nor is there a one size fits all model for the IdM architecture of every enterprise; in many cases it makes sense for different business units (such as bureaus within an Agency) to operate IdM somewhat autonomously from the parent organization.

Thus, while increased connectivity and e-business created the need for IdM consolidation and integration they also exposed the limits of these approaches and created the need for a third approach: federated identity management both between enterprises, and within enterprises.

Burton Group defines federated identity as follows:

*Federated Identity Management: Use of agreements, standards, and technologies to make identity and entitlements portable across loosely coupled, autonomous identity domains.*

An example use case for federated identity is standards based, reduced sign on for browsers. In this scenario, users log into their home domain. When they attempt to access a resource in another domain, rather than being required to sign into some other account, their browser is redirected back to a security server in the home domain, which issues an authentication assertion message for the target domain allowing the user seamless access to the resource. Figure 5 displays this scenario. Somewhat similar scenarios can be drawn for portals, web services, and other use cases.



**Figure 5: Federated Identity Scenario**

We can also define federated identity by what it is not.

- Federated identity management is different from X.500 Directory Services. X.500 requires enterprises to agree not only on internal schema and naming rules for identity, but also on internal access control models, replication protocols, and a very limited selection of vendors that support it.
- Federated identity is different from meta-directory services, which require pair-wise schema mapping and non-standard connectors between enterprises.
- Federated identity is different from – though highly synergistic with – public key infrastructure (PKI). On one hand, PKI provides key management services that protect authentication assertions or other message used in federating identity. And federated identity assertions can be used to bridge authentication between those domains that support PKI and those that do not, or between domains with non-interoperable PKIs. But on the other hand, federated identity does not require that every user and every application support PKI, or that a tightly integrated PKI enabled trust fabric exist worldwide.

Instead, federated identity management allows heterogeneous enterprises to disagree over what technology to deploy as well as the very meaning, ownership, and schema of identity – while still implementing portable identity standards at the edges of their autonomous domains.

Fundamentally, federated identity management should be loosely coupled. Relying parties shouldn't need prior knowledge of the internal details of each other's IT systems, or pair-wise mappings to manage or use identity information. Instead, identity federation standards should define rules that bind autonomous identity domains to a common method of exchanging identity information with one another.

Over the last two years, the concept of federated identity has emerged as a pragmatic and credible solution. The Security Assertion Markup Language (SAML), Liberty Alliance, and WS-Security are already in the early adopter phase of implementation and deployment, across multiple industries. Federated identity is the right architecture for Internet authentication.

It's also important to view federated identity in the larger context of enterprise application integration and interoperability. As organizations continue to integrate processes that span organizational boundaries, authentication is not the only area in which complex interoperability problems arise. A variety of different operational semantics - such as transactions, not to mention data - must cross boundaries. One cannot assume that each point in the chain is based on identical technologies, products, and implementation specifics. Thus, where they were once predicated on the assumption that every organization would adopt the same set of standards simultaneously, today's integration models are based on the assumption that organizations will use a widely diverse set of technologies and standards. Integration frameworks, such as the Web services framework, are based on federated models. They're using federation techniques to enable loose couplings and connections not just for interoperable authentication, but for interoperable transactions, data transformation, and other equally essential operational semantics. In that light, the move toward federated identity is even more meaningful, because it's well-aligned with the general trends in application integration.

## 10. Appendix B: Federated Identity Specifications and Standards

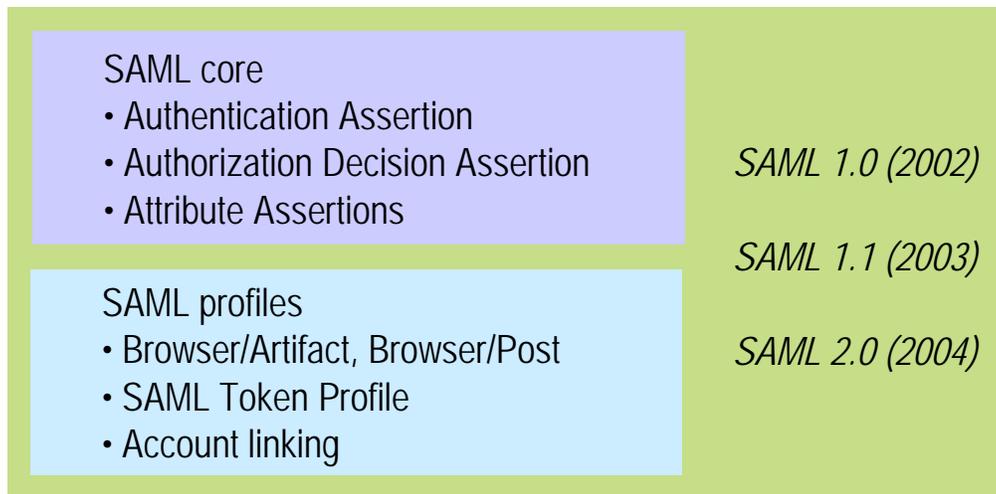
While there has been uncertainty and churn in the standards space, standards are beginning to coalesce. Currently, a breakthrough of sorts is underway in OASIS with SAML 2.0. SAML 2.0 will re-factor SAML, Liberty, and Shibboleth into a comprehensive federation “front channel” for browser based federation that overcomes a number of SAML 1.x limitations.

Meanwhile, WS-Security and WS-\* are enabling a comprehensive Web services “back channel” leveraging federated identity that will become increasingly important as applications migrate to the web services model. However, there is a need for standardization and convergence of the work that Microsoft and IBM have done on WS-Federation and work that Liberty Alliance has done on its Web Services Framework (ID-WSF).

### **SAML**

Security Assertion Markup Language (SAML) is an industry standard for Web single sign-on (SSO) and Web services authentication, attribute exchange, and authorization. SAML enables interoperability between loosely coupled security domains using different platforms, applications, and security infrastructure. SAML is referenced in Liberty Alliance, WS-Security, and other specifications. It has broad vendor support and is in early adoption gaining momentum across financial services, government, manufacturing, higher education, telecommunications, and other vertical industries. For all SAML’s promise and marketplace momentum, however, enterprises deploying SAML at this stage still face significant issues establishing interoperability, technical interconnection, trust, and business agreements.

SAML has been broadly implemented by all major Web access management vendors. BEA and IBM also support SAML in their application server products, and SAP supports SAML from within its application environment. SAML support is also common among Web services management and security vendors. In addition to packaged products that support SAML as one of many features, standalone federation toolkits or packages enable customers to bolt SAML support onto existing applications without modifying the applications or committing to a broader “platform” of any kind.



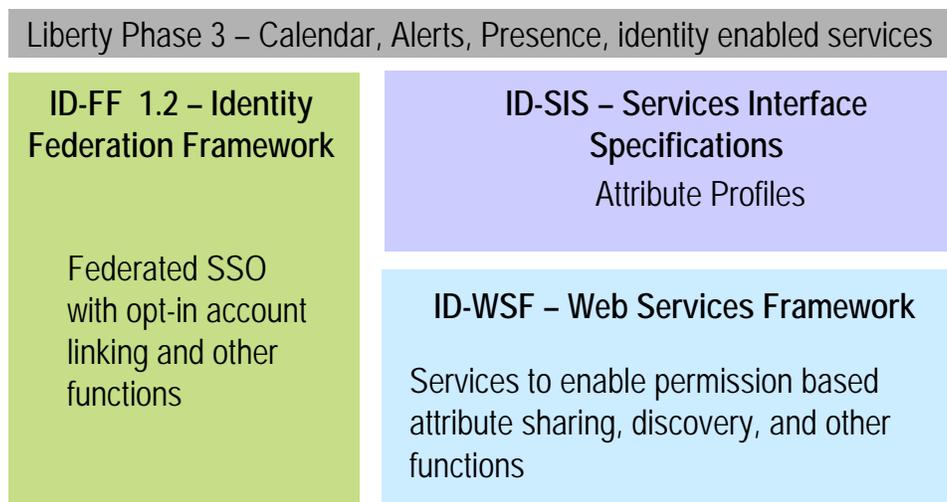
**Figure 6:** *Elements of the SAML Standard*

However, SAML is not a magic-bullet solution for all federation needs. SAML provides an impressive amount of functionality, but mostly in the form of basic assertion requests and responses. Additional protocols are required to support advanced federated authorization or complex trust models, for example. In addition, name mapping and the use of SAML features such as attribute assertions require careful technical coordination between partners. While SAML 1.1 improved on SAML 1.0 by fixing the digitally signed assertion function, SAML 1.1 still has a number of gaps, such as the lack of a mechanism for session timeout, or logout across federated domains. SAML 2.0 will close some of these gaps but also introduce more profiles – raising new interoperability and backward compatibility issues.

Due to these gaps, and the immaturity of business, trust, and management models, SAML is challenging to deploy in a wide scale environment. But SAML and the products that support it are powerful and flexible enough to support pairwise federation between domains with existing business relationships, as is mostly the current practice. The profiling and interoperability testing performed by the E-Authentication Initiative for SAML 1.0 is exactly the kind of effort required to bring the standard into wider use.

### ***Liberty Alliance Project***

The Liberty Alliance Project is an industry consortium that has extended SAML by developing specifications for account linking, permission based attribute sharing, and identity enabled applications. Membership in the Alliance, now more than 170, continues to expand, and includes many end-user organizations, which is unusual in the standards development process.



**Figure 7:** *Liberty Alliance Specifications*

In the first half of 2003, Liberty introduced a new architectural framework within which it will develop and manage specifications in a phased approach. Phase 1 produced the “Identity Federation Framework” (ID-FF) 1.1. In November 2003, Phase 2 added anonymity and affiliation enhancements to ID-FF 1.2 and introduced the Liberty “Identity Web Services Framework” (ID-WSF) Version 1.0 and “Identity Services Interface Specifications” (ID-SIS) Version 1.0. Phase 3 work in 2004 includes the development of additional identity enabled services.

Vendor support for Liberty’s ID-FF 1.x specifications continues to grow. More than 20 vendors have publicly announced support or commitments to implement the Liberty ID-FF specifications in their products over the coming year. ID-FF has been deployed in new versions of Fidelity Investment’s NetBenefits offering and in multiple other cross-enterprise financial services, telecommunications, and travel applications. ID-WSF, however, has seen adoption mainly confined to telecommunications and service provider market niches with fewer vendors supporting these specifications.

Liberty’s ID-FF goes beyond the basic SAML Authentication Assertion use case to address what is the next step for many applications, linking a digital identity asserted by a CSP to an existing account used for authorization in an application. However, Liberty ID-FF does not address new account activation, which may still require out of band processing (such as PIN issuance, or provisioning) between CSPs and applications. Nonetheless, ID-FF has widespread applicability to the enterprise and e-business markets and would be useful to some Federal applications, especially as it provides a relatively privacy-friendly approach by recommending a user opt in process to account linking, and requiring an opaque (rather than unique) identifier for each pair of digital identities.

## **Shibboleth**

The Internet2's Middleware Architecture Committee for Education (MACE) has developed an architecture model for federated identity management called Shibboleth. Shibboleth is a SAML-enabled application for Web single sign on, with optional anonymity built in as well as mechanisms for user-controlled attribute exchange from CSPs to applications.

Due in large part to federally mandated requirements to safeguard information about students and their families through the Family Educational Rights and Privacy Act of 1974 (FERPA), higher education IT infrastructures must try to protect a user's anonymity outside the institution's confines. Therefore, Shibboleth protects privacy by letting the user control attribute access, while at the same time enabling a federated technology and trust model that fosters secure collaboration among disparate universities, libraries, academic research partners, content providers and similar environments.

While Shibboleth is in production use at ten or more universities and a number of others are in pilot, there has been little commercial uptake of Shibboleth outside of vendors that sell applications to universities. Yet as Shibboleth use expands the E-Authentication Initiative is considering adding it as a supported federation scheme due to the high degree of interaction concerning grants and training courses between almost every Federal Agency and university.

To interoperate with Shibboleth the Government would have to adopt SAML 1.1 with the browser/post profile, or the OpenSAML implementation underlying Shibboleth would have to be modified. Another possibility would be for government and higher education to converge on SAML 2.0, which incorporates almost all of the Shibboleth functionality, and to which future versions of Shibboleth will migrate.

## **WS-Security and WS-\***

Through Web services, the industry has an opportunity to create a network application platform that enables applications to consume services that interoperate with other applications, even if the various applications were built on different operating systems with different tools. But security and policy must be part of the equation. To that end, Microsoft and IBM are driving an initiative called WS-\* (pronounced "WS star"). WS-\* defines specifications for Web services security, reliable messaging and transactions in a composable manner. WS-\* security specifications are also designed to interoperate with existing security models such as passwords, Kerberos, SAML, and PKI.

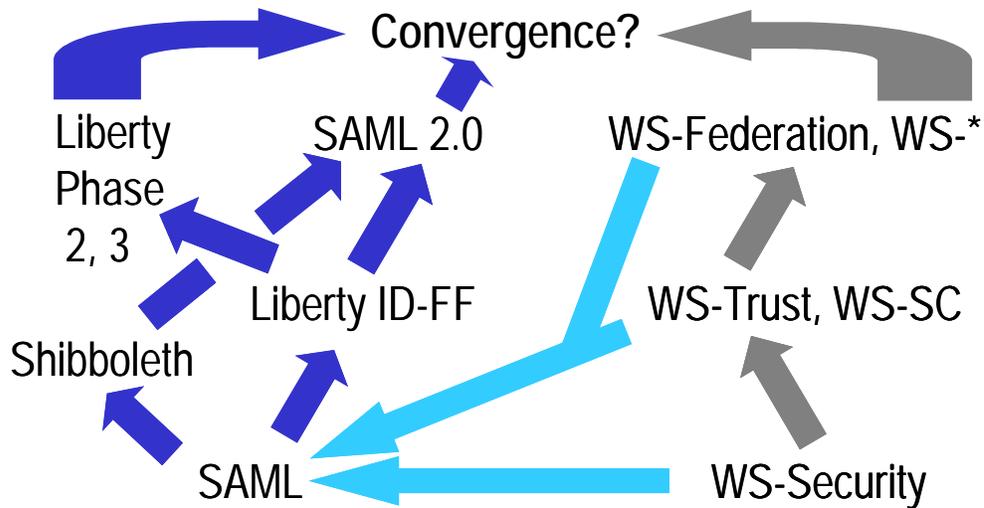
The WS-Security specification has been standardized at the Organization for the Advancement of Structured Information Standards (OASIS) and forms the foundation for the entire WS-\* security architecture by enabling basic application message security functionality, including authentication, message integrity, and message confidentiality. But WS-Security is just the beginning. Microsoft, IBM, and partners are also developing WS-Policy, WS-Trust, WS-SecureConversation, WS-Federation, and other specifications.

With the exception of WS-Security, the new WS-\* specifications are all at an early stage of their development. Each specification needs additional review, rewrites, and proof of concept testing. WS-Policy and WS-Federation are less far along than WS-Trust and WS-SecureConversation. None of the specifications except WS-Security has been submitted to OASIS or any other open standards group, and this – along with WS-Federation’s overlaps with the Security Assertion Markup Language (SAML) and the Liberty Alliance specifications – has caused considerable controversy. Yet Microsoft and IBM have committed to providing the specifications to an open standards body on a royalty free (RF) basis.

Unless vendors produce COTS WS-\* support more rapidly than expected, most of the WS-\* specifications will not meet the E-Authentication Initiative’s maturity requirements over the next three years. However, the OASIS WS-Security standard combined with password, X.509, or SAML tokens may be ready for Federal use within one to two years. And because the WS-\* specifications take an open and architecturally holistic approach that could ultimately be of great value in delivering secure Web services, they bear watching.

### ***SAML 2.0 and the Convergence of Standards***

As shown in Figure 8, multiple work streams from the standards community are all converging in SAML 2.0. SAML 2.0 re-factors SAML, Shibboleth, and Liberty ID-FF to enable account linking with optional privacy and anonymity features; attribute definitions and exchange; single logout; a metadata and exchange protocol; “destination site first” functionality; client profiles; and XML schema, encryption, and extensibility. While it is not backward compatible to SAML 1.x or Liberty ID-FF, SAML 2.0 uses many of the same XML constructs and may represent a relatively incremental effort for existing federation vendors to build.



**Figure 8:** *Convergence of Federated Identity Standards and Specifications*

It is also notable that WS-Security, WS-Trust, and WS-Federation all support the use of the SAML assertion as a token format enabling web services security services. Thus, SAML is already a point of convergence between the WS-\* and OASIS worlds. However, WS-Federation overlaps with SAML by implementing a rival browser profile and overlaps with Liberty Alliance by implementing pseudonym and attribute services.

Over time, federated identity standards will change, diverge, and converge as new Web services, privacy, and security requirements are addressed. It is appropriate under the circumstances for the E-Authentication Initiative to implement layers of abstraction to accommodate multiple federation schemes through technical architecture components such as the planned E-Authentication Scheme Translator.