GSA U.S. General Services Administration

egov

Privacy Impact Assessment

E-Authentication Initiative
(UPI Code: 023-00-01-04-01-0250-24-409-203)

Authentication Service Component
(ASC)

July 29, 2004

Prepared by:

GSA Office of Governmentwide Policy (OGP)
Identity Policy and Management
1800 F Street NW
Washington DC 20405

Table of Contents

1.0 Introduction

As part of the President's Management Agenda, the E-Authentication Service Component (ASC) was established to enable trust and confidence in E-Government transactions through the establishment of an integrated policy and technical infrastructure for electronic authentication. Through this initiative, citizens, businesses, and governmental entities will have simpler access to multiple agency applications through the re-use of credentials and established identities. GSA is making the ASC available to Federal E-Government applications as a governmentwide service component of the Federal Enterprise Architecture. In this way, Federal agencies can use the common policy and technical infrastructure of the ASC without having to bear the cost and burden of re-creating the infrastructure on their own.

GSA has been designated by the Office of Management and Budget as the lead agency for the development, implementation and operation of the Federal electronic authentication infrastructure. GSA has established a Program Management Office (PMO) in the Federal Technology Service for the ongoing operation of the ASC. The Office of Management and Budget and the GSA Office of Governmentwide Policy provide policy support for the initiative.

GSA recognizes the importance of protecting the privacy of individuals during access to government agencies though the ASC's single sign-on portal. Privacy issues must be addressed when governmentwide service components such as the ASC are being developed and implemented and privacy protections must be integrated into the development life cycle of these services and systems. The vehicle for addressing privacy issues in a system under development is the Privacy Impact Assessment (PIA).

This PIA utilizes the two-part questionnaire provided in a "Memorandum for Designated Approving Authority (DAA) Officials" issued by GSA's Chief People Officer and Chief Information Officer. This questionnaire is designed to identify who is responsible for the system (Part I, "PIA Contacts and Qualification Questions") and addresses the privacy and security issues and requirements of the system (Part II, "System Assessment").

After careful analyses and proofs-of-concept, the General Services Administration (GSA) determined that the most viable means to implement E-Authentication infrastructure was through a decentralized, federated architecture. The ASC leverages credentials from multiple credential providers through certifications, guidelines, standards adoption and policies. The ASC currently supports assertion-based identity authentication (i.e., SAML 1.0) and certificate-based authentication (i.e.,) within the same environment. Over time, the ASC will support multiple schemes such as the Security Assertion Markup Language (SAML) and Liberty Alliance, and therefore is not built around a single scheme or commercial product. The ASC architecture will continue to evolve as new technologies and enhancements are introduced. Therefore, it is acknowledged that this PIA will need to be updated at regular intervals as the ASC evolves in scope and complexity. The ASC is targeted for incorporation into the Federal Enterprise Architecture (FEA), as the government-wide identity authentication component.

1.1 Purpose

The objective of this PIA is to assist GSA ASC Project Managers in identifying and addressing privacy implications when planning, developing, implementing, and operating the ASC. The PIA will also assist in consideration and evaluation of whether existing statutory requirements and key information management concepts and requirements are being properly applied to the ASC. These requirements are drawn from:

- The Privacy Act of 1974;
- The Computer Security Act of 1987;
- The Clinger-Cohen Act of 1996;
- The Government Paperwork Reduction Act of 1995;
- The Freedom of Information Act; and
- Office of Management and Budget (OMB) Circulars A-130 ("Management of Federal Information Resources") and A-123 ("Management Accountability and Control").

This PIA process also helps to identify the ASC as a sensitive system that requires appropriate Information Assurance (IA) countermeasures and controls, such as secured storage media, secured transmission, and access controls.

The goals to be accomplished in completing a PIA include:

- Providing senior GSA management with the tools to make informed policy and system design or procurement decisions based on an understanding of privacy risk, and of options available for mitigating that risk;
- Ensuring accountability for privacy issues with system project managers and system owners;
- Ensuring a consistent format and structured process for analyzing both technical and legal compliance with applicable privacy laws and regulations, as well as accepted privacy policies; and
- Providing basic documentation of the flow of personal information within the ASC for use and review by policy and program staff, systems analysts, and security analysts.

1.2 Overview

Remote electronic identification and authentication is not new technology; many government agencies have developed and implemented such systems to meet their individual needs and goals. They have identified and assessed the privacy and legislative concerns related to their individual situations on a case-by-case basis. As a result, while remote electronic identification and authentication processes exist in many government agencies, the specific approach across agencies is fragmented and the results of each process are generally not available either across systems or among agencies. The ASC is being designed and implemented to provide a common approach to remote electronic identity management that facilitates sharing of electronic identity credentials and essential personally identifiable information (PII).

The ASC is designed to ensure that government services delivered over the internet go to the intended person, that people are who they claim to be, and that privacy is protected at all times.

The ASC concept, which is aimed at online government-to-citizen (G2C) services, is best described through the trust relationships between Agency Applications (AA), Credential Service Providers (CSPs) and End-Users. CSPs are commercial or government entities authorized by the E-Authentication Program Management Office (PMO) to provide credentials (PINs, Passwords, Digital Certificates, etc) to potential End-Users for access to government systems. AAs are government applications, systems, or services that rely on (or trust) the authentication/credential services of CSPs. End-Users are people or organizations that have credentials issued by a CSP and desire to use those credentials to conduct business with an AA. It is the management of this transitive trust between these entities (AAs, CSPs, and End-Users) that is the essence of the E-Authentication Initiative and the ASC. The ASC provides:

- Policies and Guidelines for remote electronic identity management;
- Credential Assessments and Authorizations;
- Interoperability Testing of candidate products, schemes, or protocols; and
- Management and Control of accepted federation schemes operating within the environment.

To manage the trust relationships, the PMO does not envision building an authentication infrastructure as a central broker for these entities. Instead, the ASC will use federated architecture that leverages credentials from multiple domains through certifications, guidelines, standards adoption, and policies. The architecture, as described in Section 4.0, accommodates the use of Assertion-Based credentials (PINs and Passwords) and Certificate-Based credentials within the same environment. The architecture will leverage multiple emerging federation schemes (such as SAML and Liberty Alliance) over time, and not simply be built around a single scheme or commercial product. As such enhancements occur, delta PIAs will need to be conducted and documented.

2.0 Background

Privacy protection is both a personal and fundamental right of individuals, including GSA associates, clients, and members of the public, whose PII is collected, maintained, and used by GSA organizations to carry out agency missions and responsibilities and to provide services. By law and regulation, privacy issues must be addressed when automated systems are being developed, and privacy protections must be integrated into the life cycle of these systems.

GSA has instituted the PIA as the means for ensuring that GSA's information systems are designed to protect the privacy of individuals. The PIA process is designed to assure compliance with the applicable laws and regulations governing an individual's privacy and to ensure the confidentiality, integrity, and availability of an individual's PII at every stage of system development and operation. The PIA also incorporates privacy into a system's life cycle so at any stage of a major system initiative (from design and development to system upgrades and improvements) privacy is a consideration.

The E-Government Act of 2002, Section 208 ("Implementation Guidance"), specifies a requirement of Federal Agencies to conduct PIAs for electronic information systems and collections and, in general, make them publicly available. This PIA is being conducted prior to developing or procuring an IT system that collects and maintains or disseminates PII from or about members of the public.

3.0 Scope

This initial PIA is based on an information management perspective and will be conducted and maintained throughout the lifecycle of the ASC, as described in section 4.0.

This PIA is confined to the ASC; it does not cover the systems from which the information is gathered or the systems to which the information is disseminated.

4.0 System Architecture

The system architecture for the ASC is based on a framework that allows for the co-existence of multiple federated identity schemes within a single architecture. The framework includes a methodology and process for the evaluation and adoption of these schemes over time. This is in accordance with the applicable National Institute of Standards and Technology (NIST) E-Authentication technical guidance constraint that the ASC approach is as technology neutral as possible.

The major sub-components of the ASC are:

1. **Agency Applications:** E-Government applications that perform some business function online. If an E-Government application has multiple interfaces (e.g., administration and service applications), each interface with distinct authentication requirements is considered a stand-alone AA. AAs manage all business transactions and all End-User authorization decisions. One of the principal goals of the ASC is to provide broad authentication services to AAs, allowing the complete deferral of identity management.
2. **Credential Services:** Credential Services (CSs) are services that provide End-Users with electronic credentials that can be used at ASC -enabled AAs. CSs are provided by CSPs, which are companies or agencies that operate one or more CSs.
3. **E-Authentication Portal (Portal)**: A website that helps End-Users locate the CSs and AAs they need to complete their transactions electronically. The Portal also maintains information about CSs and AAs, referred to as metadata, which includes technical interface data and descriptive information.
4. **End-Users**: Any citizen, government employee, contractor, or business that authenticates its identity to an AA using a credential issued by a government-approved CSP. One of the principal goals of the ASC is to make the End-User experience as simple as possible, by improving the availability and ease of use of electronic identity credentials.

Within this architectural framework, the End-User interacts directly with AAs, CSPs, and the Portal. Typically, the End-User starts at the Portal in order to locate the appropriate AAs and CSPs. The End-User interacts with the CSP to obtain, manage, and validate electronic credentials. The CSP interacts directly with the AA in order to pass the end user’s identity information so that the AA knows with whom it is dealing. Once the AA knows the identity information, the End-User interacts directly with the AA for business transactions. Authorization (decisions relating to access permissions and privileges) is handled solely by the AA.

Governance is accomplished by managing the interaction between the AAs and CSPs. The government will issue electronic credentials to approved AAs and CSPs, which will be validated before the End-User's identity information is handed off.

There are three types of sessions discussed in the ASC architectural framework:

1. **Browser Session:** The period of time the End-User's browser is open. The browser session begins when the End-User opens the browser and ends when it is closed. All session cookies are terminated when the browser session ends. Any browser with Transport Layer Security (TLS) and session cookie support can be used with the ASC, although individual AAs and CSPs may have additional requirements.
2. **Authentication Session:** The period of time that an End-User remains trusted after the End-User authenticates his/her identity. A CSP typically does not require an End-User to re-authenticate for every page requested; they continue to be trusted for some period of time after each authentication. The CSP's allowed period between re-authentications is referred to as the authentication session.
3. **Agency Session:** The period of time an AA will trust an End-User before handing the End-User off to the CSP for re-authentication. AAs do not have access to authentication session information; they must maintain their own session with an End-User and decide how long an End-User remains authenticated once starting a transaction.

The ASC technical approach has two different architectural models, assertion-based authentication and certificate-based authentication. PIN and Password (including one-time use passwords) authentication uses assertion-based authentication, where End-Users authenticate to a CSP, which then asserts their identity to the AA. Assertion-based authentication can be used as defined in NIST Special Publication (SP) 800-63 for assurance levels 1 and 2. Considering certificate-based authentication relies on X.509v3 digital certificates in a Public Key Infrastructure (PKI) for authentication, it can be used at any assurance level. The document entitled "Technical Approach for the Authentication Service Component," which may be accessed at http://www.cio.gov/eauthentication/TechSuite.htm, describes the technical approach for assertion-based and certificate-based authentication in much greater detail.

5.0 Assessment

This PIA is provided in the responses to the Two-Part Questionnaire that follows. While the ASC core architecture does not collect or maintain any personally identifiable information, GSA is performing this assessment as a foundation for the ASC and additional components which may require separate assessments for the future.

PRIVACY IMPACT ASSESSMENT

PART I. PIA Contacts and Qualification Questions

A. Contact Information

System Title: E-Authentication Initiative: Authentication Service Component (ASC) (UPI Code: 023-00-01-04-01-0250-24-409-203)	
Office of Responsibility: GSA/FTS E-Authentication Program Management Office (PMO)	
Program Manager Name and Title: Steve Timchak Program Executive for E-Authentication	Phone: 708-872-8604 Email: stephen.timchak@gsa.gov Organization and Correspondence Code: GSA/FTS
System or Project Manager/Project PIA Contact Name and Title: David Temoshok Director, Identity Policy and Management	Phone: 202-208-7655 Email: david.temoshok@gsa.gov Organization and Correspondence Code: MEI/GSA/OGP
DAA Name and Title: Casey Coleman FTS Chief Information Officer	Phone: 703-306-6178 Email: casey.coleman@gsa.gov Organization and Correspondence Code: GSA/FTS

B. Qualification Questions

Does your system collect any information in identifiable form (personal data) on the general public?	The ASC collects no personal information and does not maintain any PII system of records. The ASC architecture establishes interfaces among other entities where information is collected. Data collection occurs and system records are maintained at the Credential Service Providers (CSPs) and the Agency Applications (AAs). Information collection and systems records authority are maintained directly by those entities. No new data collection or system of records is required for the ASC. The E-Authentication PMO maintains agreements with all CSPs and AAs to participate in the ASC. A complete listing of the participating CSPs and AAs is available from the Director, E-Authentication Program Management Office, GSA Federal Technology Service, 703-872-8604, or at the E-Authentication website: http://www.cio.gov/eauthentication.
Does your system collect any information in identifiable form (personal data/information) on government employees?	Yes. See response to question #1.
Does the public have access to the system?	Yes. The public has complete access to the ASC. However, no system of records is maintained by the ASC. Access to systems maintained by CSPs and AAs is managed directly by those entities.
Has a PIA been done before for your system?	Yes. A preliminary PIA was performed in FY 2003. However, that preliminary PIA did not properly assess the principal components of the ASC as they were still under development at the time.
Has it been at least three years since your last PIA was performed?	No.
Has your system changed since the last PIA was performed?	Yes. See Question #3.

PART II. SYSTEM ASSESSMENT

A. Data in the System

1. Describe the information to be used in the system, including privacy data.	*a. Briefly describe the purpose of the system.* See system description in Part 1. The E-Authentication Service Component (ASC) provides common infrastructure for the authentication of individuals who are users of Federal E-Government services. The ASC does not maintain any system records containing PII. Individuals are enrolled with Credential Service Providers (CSPs) and Agency Applications (AAs) and any PII is maintained by those entities. The scope of systems record data maintained by CSPs and AAs varies, and can be obtained through those entities directly. The ASC provides for the authentication of users to AAs by validating identity credentials with approved CSPs and expressing authentication through identity assertions (i.e., SAML 1.0). or x.509v3 digital certificates. At a minimum, an individual's claimed identity is maintained by the systems records of CSPs and AAs and is passed by the CSP to the AA as part of the identity assertion. Information contained in a digital certificate is public information and includes unique name. One of the components of the e-Authentication initiative is the PKI Multi-Protocol Validation Service (MPVS). This service parses and validates PKI certificates on behalf of agency applications and reports the certificate validation status to the agency application. Because the functionality of the MPVS is fundamentally different than the core ACS architecture, a separate Privacy Impact Assessment was performed of the MPVS. *b. Provide the specific data elements that will be maintained in the system.* The ASC maintains no system of records or PII. The ASC provides for web-based linkages between Federal agencies (AAs) and CSPs in order to provide the validation of identity through identity assertions and digital certificates that contain the claimed identity of the individual user.

1.a. What stage of the life cycle is the system currently in?	Development/Implementation.
2.a. What are the sources of the information in the system?	*Describe where the system data originates, whether the privacy information is provided by the user or entered on behalf of the user or if it comes programmatically from another system.* In general, information collected as part of the enrollment process for CSPs and AAs will originate from the end user. In general, the claimed identity expressed in ASC identity assertions and digital certificates originate with information collected in CSP and AA enrollment processes and maintained in separate and distinct records systems by those entities. It is anticipated that any PII collected in enrollment processes or otherwise collected and maintained in CSP and AA records systems will originate from the end user. However, there may be circumstances where PII is provided by a third party on behalf of the user or from another system. The ASC does not access data from any CSP or AA. The sole data element that is used in ASC assertions is claimed identity.
2.b. What GSA files and databases are used?	GSA maintains an authentication portal as a component to the ASC. The portal maintains information on every AA and CSP authorized to use the ASC architecture. The information maintained consists of identification information for the CSP and AA, AA level of authentication assurance required, CSP level of authentication assurance authorized, and URL address. No PII on individuals is collected or maintained by the portal and, therefore, is not a systems or records covered by the Privacy Act. No other GSA files or databases are used, unless GSA is approved separately as a CSP. The only GSA services authorized as a CSP are services under the ACES Governmentwide Acquisition Contract. ACES Records systems are specified in the GSA System of Records Notice for ACES.

2.c. What Federal agencies are providing data for use in the system?	The ASC uses validated claimed identity as the only PII transferred within the ASC network. Any Federal Agency may serve as a CSP and provide authentication validation and validated claimed identity. Current Federal CSPs are: GSA ACES Program, USDA National Finance Center PKI, Department of Defense PKI, Department of Treasury PKI, Department of State PKI, and Department of Energy PKI.
2.d. What State and local agencies are providing data for use in the system?	The ASC uses validated claimed identity as the only PII transferred within the ASC network. A State/local government agency may serve as a CSP and provide authentication validation and validated claimed identity. No State or local agency may provide data for use in the ASC network unless approved as a CSP. The State of Illinois PKI is the only State/local government service authorized as a CSP for the ASC.
2.e. What other third party sources will the data be collected from?	The ASC uses validated claimed identity as the only PII transferred within the ASC network. A nongovernmental/commercial entity may serve as a CSP and provide authentication validation and validated claimed identity. No nongovernmental/commercial entity may provide data for use in the ASC network unless approved as a CSP. There are currently no nongovernmental/commercial entities authorized to participate in the ASC as CSPs.
2.f. What information will be collected from the individual whose record is in the system?	No records are maintained in the ASC system.
3.a. How will the data collected from sources other than Federal agency records or the individual be verified for accuracy?	The ASC has established standards for identity proofing for CSP enrollment and registration processes. CSPs must meet the standards in order to be authorized to participate in the ASC. The requirements for identity proofing and vetting information are specified in the Credential Assessment Framework (CAF). The CAF suite of documents is available at the website: http://www.cio.gov/eauthentication. GSA assesses potential CSPs against the CAF standards at the level of assurance requested by the CSP. Authorized CSPs are made available to Federal; AAs through the ASC architecture and are posted publicly at the website above.

3.b. How will data be checked for completeness?	See response to question 3.a.
3.c. Is the data current? How do you know?	Currency of information is the function of the CSP and AA, not the ASC. Since validated claimed identity is the only information used by the ASC and is not dynamic data (i.e., subject to change), currency of other information in CSP and AA records is not relevant for the ASC. All authentication transactions within the ASC architecture require current, real-time validation of identity credentials. Any revoked or inactive credentials/accounts will not be validated.
4. Are the data elements described in detail and documented? If yes, what is the name of the document?	No data elements are maintained by the ASC. The only PII that is included in the interfaces among the ASC, CSPs and AAS is validated claimed identity. Interface specifications for the interfaces between the ASC, CSPs and AAs can be accessed at the website: http://www.cio.gov/eauthentication.

B. Access to the Data

1.a. Who will have access to the data in the system?	*Users or groups who have access to the entire system:* • Public Access – citizens, businesses, governmental agencies • Federal agency applications • Approved CSPs *People who have access to privacy data:* • Federal agency applications • Approved CSPs
1.b. Is any of the data subject to exclusion from disclosure under the Freedom of Information Act (FOIA)? If yes, explain the policy and rationale supporting this decision.	No.
2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?	No PII data elements are maintained by the ASC. The ASC architecture creates interfaces between approved CSPs and AAs. The interfaces allow validation of claimed identity; no other information is passed through the interfaces. User rights to information maintained by CSPs or AAs are specified in system of records notices and other administrative information maintained by those entities. The principal technical interface and architecture documents for the ASC are: • "Technical Approach for the E-Authentication Service Component" • "E-Authentication Interface Specification for the SAML Artifact Profile" • "SAML Artifact Profile as an Adopted Scheme for E-Authentication" • "E- Authentication Handbook for Agency Applications" • "E- Authentication Handbook for Credential Service Providers". These documents are publicly available at the website: http://www.cio.gov/eauthentication.
3. Will users have access to all data in the system or will the user's access be restricted? Explain.	See response to question #2.

4. What controls are in place to prevent the misuse (e.g., browsing) of data by those having access?	The ASC architecture controls sessions through TSL/SSL authentication and encryption between the access points in the architecture (i.e., ASC portal, CSPs, AAs).
5.a. Do other systems share data or have access to data in this system? If yes, explain.	*List any systems that will either send or receive data in this system. Explain the purpose of the connection and methods used to ensure integrity and security of the data being exchanged.* The ASC does not maintain PII records systems. However, CSPs and AAS interface through the ASC technical architecture. The purpose of the interface is to express validated identity authentication through expressing identity assertions using SAML. The ASC architecture controls sessions through TLS/SSL authentication and channel encryption between the access points in the architecture (i.e., ASC portal, CSPs, AAs).
5.b. Who will be responsible for protecting the privacy rights of the clients and employees affected by the interface?	The e-Authentication Project Manager and Information System Security Officer, Federal Technology Service, GSA.
6.a. Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)?	The ASC does not maintain a system of records. Access to data maintained by CSPs and AAs is governed by the privacy and security policies of those entities.
6.b. How will the data be used by the agency?	Validated claimed identity is used by agency applications to authorize users of Federal e-government services to gain access to information and services, submit filings or other communications, and/or conduct web-based business/government transactions.
6.c. Who is responsible for assuring proper use of the data?	The e-Authentication Project Manager and Information System Security Officer, Federal Technology Service, GSA.

6.d. How will the system ensure that agencies only get the information they are entitled to?	*List the controls and security mechanisms to ensure that exchange of data is appropriate.* The ASC architecture allows for the retrieval of assertions over a client and server authenticated SSL channel. The e-Authentication PMO will authorize the issuance of digital certificates for this use within the ASC. Only properly authorized AAs and CSPs that have been evaluated under the CAF may participate in the ASC and receive the e-Authentication governance certificates. Only appropriately authorized e-Authentication governance certificates may be accepted by participating CSPs and AAs. For more detail see the document "Technical Approach for the E-Authentication Component" at the website: http://www.cio.gov/eauthentication.
7. What is the life expectancy of the data?	*Indicate whether the data will be collected and used for a one-time process or whether the data will be maintained min a database.* Information that is exchanged within the ASC architecture is a one-time exchange for the period that the web-based session is open. No PII records system is maintained by the ASC. Information maintenance by CSPs and AAS will be in accordance with the agencies' records maintenance and disposition schedule.
8. How will the data be disposed when it is no longer needed?	No PII records system is maintained by the ASC. Information disposal by CSPs and AAS will be in accordance with the agencies' records maintenance and disposition schedule.

C. Attributes of the Data

1. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?	*List each data element and the relevance to the system.* Validated claimed identity is used by agency applications to authorize users of Federal e-government services to gain access to information and services, submit filings or other communications, and/or conduct web-based business/government transactions.
2.a. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?	No.
2.b. Will the new data be placed in the individual's record (client or employee)?	N/A.
2.c. Can the system make determinations about individuals that would not be possible without the new data?	N/A.
2.d. How will the data be verified for relevance and accuracy?	The ASC has established standards for identity proofing for CSP enrollment and registration processes. CSPs must meet the standards in order to be authorized to participate in the ASC. The requirements for identity proofing and vetting information are specified in the Credential Assessment Framework (CAF). The CAF suite of documents is available at the website: http://www.cio.gov/eauthentication. GSA assesses potential CSPs against the CAF standards at the level of assurance requested by the CSP. Authorized CSPs are made available to Federal; AAs through the ASC architecture and are posted publicly at the website above.
3.a. If the data is being consolidated, what controls are in place to protect the data and prevent unauthorized access? Explain.	N/A.

3.b. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.	N/A.
4. How will the data be retrieved? Can it be retrieved by personal identifier? If yes, explain.	*Explain all processes for retrieving the data. If personal identifiers are used, list.* Validated claimed identity is used for purposes of identity authentication. This data is expressed as unique common name. If no claimed identity is known, (i.e., unique common name not provided), the users' pseudonym or userid will be expressed. The e-Authentication PMO will authorize the issuance of client and server governance certificates to CSPs and AAs. All CSPs and AAs will be issued identifiers by the PMO. The identifiers are used as keys to reference metadata and will be made available for download by all CSPs and AAs. These identifiers are issued to organizations – CSPs and AAs – and do not represent PII or systems records under the Privacy Act.

5. What are the potential effects on the privacy rights of individuals of: a. Consolidation and linkage of files and systems; b. Derivation of data; c. Accelerated information processing and decision making; and d. Use of new technologies. How are the effects to be mitigated?	a. The ASC architecture uses a decentralized approach rather than a consolidated central registry of information and attributes for individuals. This is a fundamental privacy protection. While the ASC creates linkages among many disparate, distinct databases, the architecture ensures privacy protection by controlling who and what information can be accessed. b. N/A c. The ASC architecture does not make authorization decisions in any case for AAs. Rather, the ASC provides for authentication of claimed identity so that decisions can be made within the controls and processes of AAs operating systems and environment. The common authentication infrastructure of the ASC will make such decisions more timely and should provide for greater controls since there is greater security and greater controls through the ASC. d. New technologies will allow the capability for expanded linkages among more entities using more authentication technologies than currently deployed (i.e., knowledge-based authentication, biometrics). These new technologies will expand the convenience of the e-Authentication, but should also increase the security. As more authentication technologies are added to the ASC, the opportunity for greater controls, enhanced authentication and multi-factor authentication will become available. This will have the direct impact of improving controls over identity theft and improve authorization processes.

D. Maintenance of Administrative Controls

1.a. Explain how the system and its use will ensure equitable treatment of individuals.	• There is not a single, mandatory process to authenticate to the Federal Government, but multiple trusted means at four different assurance levels. • Users can choose the CSP and processes by which they authenticate and sign-on to web-based services. • Users can choose which CSPs they enroll in. • The only personal information that is passed is claimed identity. • All sessions are protected by SSL, regardless of the authentication assurance level.
1.b. If the system is operated in more than one site, how will consistent use of the system be maintained at all sites?	• Common mandatory architecture. • Common mandatory interface specifications. • Common trust and policy framework.
1.c. Explain any possibility of disparate treatment of individuals or groups.	N/A
2.a. What are the retention periods of data in this system?	Information that is exchanged within the ASC architecture is a one-time exchange for the period that the web-based session is open. No PII records system is maintained by the ASC. Information maintenance by CSPs and AAS will be in accordance with the agencies' records maintenance and disposition schedule.
2.b. What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?	See response to question #2.a.

2.c. While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?	The ASC has established standards for identity proofing for CSP enrollment and registration processes. CSPs must meet the standards in order to be authorized to participate in the ASC. The requirements for identity proofing and vetting information are specified in the Credential Assessment Framework (CAF). The CAF suite of documents is available at the website: http://www.cio.gov/eauthentication. GSA assesses potential CSPs against the CAF standards at the level of assurance requested by the CSP. Authorized CSPs are made available to Federal; AAs through the ASC architecture and are posted publicly at the website above.
3.a. Is the system using technologies in ways that Federal agencies have not previously employed (e.g., Caller-ID)?	Yes. The ASC technical approach uses the standard protocol SAML (Security Assertion Mark-Up Language) 1.0 and SAML 1.0 products. SAML is an XML-based language and industry standard specifically intended to enable expressing identity assertions in a browser environment. This is emerging technology in industry and has not been deployed in Government previously. However, the purpose of SAML-based assertions is to allow for robust authentication of users in a common, secure way that will heighten the security and personal privacy protection of users.
3.b. How does the use of this technology affect individuals' privacy?	The ASC does not collect, maintain, or disseminate End-User PII. Rather, it provides the means for securely passing this information between approved CSPs and participating AAs. It should have no impact on the privacy rights of End-Users
4.a. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.	No.
4.b. Will this system provide the capability to identify, locate, and monitor groups of people? If yes, explain.	No.
4.c. What controls will be used to prevent unauthorized monitoring?	No data elements are maintained by the ASC. All sessions are secured through SSL/TLS channel controls.

5.a. Under which Privacy Act System of Records notice (SOR) does the system operate? Provide number and name.	An SOR is not applicable. However, a notice will be issued to provide an explanation of the ASC and its relationship to systems of records that are maintained by Federal entities.
5.b. If the system is being modified, will the SOR require amendment or revision? Explain.	It is anticipated that there will be changes to the technical architecture (i.e., new technologies and protocols added) that may require the ASC notice to be updated.