

E-AUTHENTICATION INITIATIVE
REQUEST FOR INFORMATION

GSA RFI No. T02-ALD-001.

July 12, 2002

Table of Contents

1. Intent of Request for Information (RFI)
2. Goal of the RFI
3. Scope
4. RFI Responses Due August 8, 2002
5. Descriptions of E-Authentication Privacy, Policies, and Technology
 - 5.1 Privacy Framework Needs
 - 5.1.1 Background
 - 5.1.2 Purpose
 - 5.1.3 Overview of the Authentication Gateway
 - 5.1.4 Gateway Purpose and Scope
 - 5.1.4.1 Purpose
 - 5.1.4.2 Scope
 - 5.1.4.3 Types of Authentication Accepted
 - 5.1.4.4 Users
 - 5.1.4.5 Authorized Uses
 - 5.1.5 Gateway Core Functionality
 - 5.1.5.1 Enrollment
 - 5.1.5.2 Validation of Credentials
 - 5.1.5.3 Agency Application Interface
 - 5.1.5.4 Legal and Policy Structures
 - 5.1.6 Next Steps
 - 5.1.7 Privacy Requirements
 - 5.2 Diagram Descriptions
 - 5.2.1 Illustrative Process Flow Concept
 - 5.2.2 Preliminary Functional Principles
 - 5.2.3 Context Diagram
 - 5.2.4 Components of the Gateway AuthN Services
 - 5.2.5 Summary of Functional Principles
6. Directed Topics for Responses
 - 6.1 Acquisition
 - 6.2 Government/Industry Relationships
 - 6.3 Technical
 - 6.4 Credential Evaluation and “Mapping”
 - 6.5 Compliance with Government Mandates for Protection of Privacy Information
 - 6.6 DCPs
 - 6.7 Anonymous Access
 - 6.8 Session Management
 - 6.9 PCI Gateway
7. Glossary of Terms and Acronyms

1. Request for Information (RFI)

This request for information is intended to seek industry and other interested parties' input into a number of questions relative to the design, build and operation of an Authentication Gateway described in Section 5. The release of this RFI is part of an industry communications strategy that is designed to seek input from a number of venues that have included Technology Day on June 7, 2002, and Industry Day held on June 18, 2002.

This RFI is requesting comments and information on specific questions that relate to acquisition, funding, government/industry partnerships, broad technical considerations, future vision/direction, credential evaluation and mapping, administration and management, record retention and privacy.

2. Goal of the RFI

The goal of this RFI is to continue the Federal government dialogue with industry and other communities of interest, and to ensure to the maximum extent possible that industry input and comments and other information are given proper and due consideration in development of the Authentication Gateway. The information received in response to this RFI may be considered in the development of any subsequent statement of work, may serve as input to policy considerations, and is intended to obtain a "sense of the industry". The information received will be considered and may be factored into future decisions. When the responses to the RFI are received they will be evaluated and analyzed. A report will be prepared that will detail the results of the RFI. Proprietary information submitted as part of responses to the RFI should be clearly identified and will not be disclosed.

3. Scope

This RFI presents and requests information on concepts and approaches that the government is contemplating for government-wide authentication services. This RFI is focused on three areas: technology, acquisition and policy/administration. These three areas will affect the design, build and operation of the Gateway. The government needs to exercise due diligence in its consideration of issues that may arise in any one of the three areas.

This RFI contains the following subsections:

- Descriptions of the E-Authentication Gateway Privacy, Policies and Technology
 - Privacy Framework Needs
 - Diagram Descriptions
- Directed Topics for Responses
 - Acquisition
 - Government/Industry Relationships
 - Technical
 - Credential Evaluation and "Mapping"
 - Compliance with Government Mandates for Protection of Privacy Information
 - Digital Credential Providers (DCP)
 - Anonymous Access
 - Session Management

- PCI Gateway

4. Responses to RFI are due on August 8, 2002.

This RFI is for planning purposes only and shall not be construed as a request for proposal (RFP) or as an obligation on the part of the Government to acquire any products or services. The Government does not intend to award a contract on the basis of this RFI or otherwise pay for the information solicited. No entitlement to payment of direct or indirect costs or charges by the Government will arise as a result of submission of responses to this RFI and the Government's use of such information.

Responses to this RFI must be divided into nine sections. The nine sections must correspond to the Directed Topics for Responses in Section 6 of this RFI. Please limit your response to 50 pages. Additional materials may be placed in an appendix (marketing, technical literature, etc.) Respondents to this RFI may be requested to provide additional information/details based on their initial submittals. Unnecessarily elaborate responses containing extensive marketing materials are not desired.

All information contained in this RFI is preliminary and subject to modification and is in no way binding on the government. The Government prefers that no proprietary or confidential business data be submitted in response to this RFI. However, responses to this RFI that indicate that the information therein is proprietary or represents confidential business information will be received and held in confidence for U.S. Government use only. However, GSA's intent is to develop a subsequent statement of work from the aggregate of the information provided from industry as a whole.

Send questions/concerns regarding this RFI via e-mail to thomas.crowder@gsa.gov with a copy to reva.hutchinson@gsa.gov. Responses to this RFI are to be submitted and addressed to Thomas Crowder, with a copy to Reva Hutchinson, at the above referenced e-mail address, no later than August 8, 2002. Responses should include the name, telephone number and e-mail address of a point of contact having authority and knowledge to discuss responses with government representatives. All correspondence concerning this RFI should refer to GSA RFI No. T02-ALD-001.

5. Descriptions of E-Authentication Privacy, Policies and Technology

5.1 Privacy Framework Needs

5.1.1 Background

Public trust in the security of the information exchanged over the Internet will play a vital role in an electronic government transformation. The government must address the issues of user authentication, confidentiality and integrity of data transferred, and the ability to hold transacting parties accountable when necessary. Thus, solutions that provide this type of protection are critical components of an organization's cyber security profile.

The current administration, recognizing the need for identity authentication to implement an E-Government, initiated the E-Authentication Initiative. Common authentication services for use across government agencies will reduce the burden on the public and better leverage the government's investments.

5.1.2 Purpose

This section of the RFI presents key concepts, policy and design issues and needs associated with the deployment of a Federal E-Authentication Gateway. It contains an overview of the authentication infrastructure that is critical to achieve the President's Management Agenda for E-Government (Figure 5.1.2). It also presents the proposed operational concept of the Gateway and its core requirements. This RFI is intended as input and support in assisting the Federal government in establishing a design that fits within the Federal enterprise architecture framework, as it conducts testing, and evaluation for ongoing E-Government authentication and identity management needs.

5.1.3 Overview of the Authentication Gateway

Expanding E-Government to enhance citizen-centric government services is a key initiative of the President's domestic management agenda. To advance this agenda, the Administration established the E-Gov Task Force in July 2001 under the Office of Management and Budget (OMB). The Task Force identified the key E-Government initiatives across the Federal Government best positioned to support the management agenda. In November 2001, the President's Management Council approved 24 initiatives. These 24 initiatives (Figure 5.1.3) defined government services and business transactions within four segments: citizen, business, government, and internal operations. All of the initiatives represent cross-agency efforts and are targeted for implementation within 18 – 24 months. In addition, all require some degree of authentication to support some or all of the business services and transactions. It is recognized that the four segments have different characteristics, and thus different authentication requirements.

To support the needs of all of the initiatives, the E-Authentication Integrated Project Team, managed by the General Services Administration was directed to provide common authentication services and infrastructure, and enterprise architecture support. To accomplish this, the E-Authentication Team plans to build and operate a web-based E-Authentication Gateway.

The Gateway will provide common authentication services and single sign-on capability for all E-Government services. The objective is to provide a set of common, shared services that all Federal agencies can use for authenticating the public as well as Federal users.

President's Management Agenda

- *1st Priority: Make Government citizen-centered.*
- **5 Key Government-wide Initiatives:**
 - Strategic Management of Human Capital
 - Competitive Sourcing
 - Improved Financial performance
 - *Expanded Electronic Government*
 - Budget and Performance Integration

Figure 5.1.2

PMCE-Gov Strategy			
Government to Citizen	Managing Partner	Government to Business	Managing Partner
1. USA Service	GSA	1. Federal Asset Sales	GSA
2. EZ Tax Filing	Treasury	2. Online Rulemaking Management	DOT
3. Online Access for Loans	DoEd	3. Simplified and Unified Tax and Wage Reporting	Treasury
4. Recreation One Stop	DOI	4. Consolidated Health Informatics	HHS
5. GovBenefits	Labor	5. Business Compliance 1 Stop	SBA
		6. Int'l Trade Process Streamlining	DOC
Cross-cutting: E-Authentication GSA, Enterprise Architecture OMB			
Government to Government	Managing Partner	Internal Effectiveness & Efficiency	Managing Partner
1. e-Vital	SSA	1. e-Training	OPM
2. e-Grants	HHS	2. Recruitment One Stop	OPM
3. Disaster Assistance and Crisis Response	FEMA	3. Enterprise HR Integration	OPM
4. Geospatial Information One Stop	DOI	4. e-Travel	GSA
5. SAFECOM	Treasury	5. eClearance	OPM
		6. ePayroll	OPM
		7. Integrated Acquisition	GSA
		8. e-Records Management	NAR

Figure 5.1.3

The E-Authentication Team is committed to implementing prototype Gateway authentication services beginning October 2002 with production authentication Gateway services targeted for September 2003. The production Gateway will be scaled to support all 24 initiatives as well as other E-Gov business needs for authentication across agencies.

5.1.4. Gateway Purpose and Scope

5.1.4.1 Purpose

To provide common authentication services in support of Federal E-Government programs. The Gateway will provide single sign-on capability so that users of E-Government services do not have to sign-on separately for each agency application being accessed.

5.1.4.2 Scope

Initially the E-Authentication Gateway will be scaled as a prototype service. Agencies with applications approved by the Presidents Management Council as part of the Administration's E-Gov strategy (see Figure 5.1.3) and, potentially, other agency E-Gov applications that are ready, may be authorized to use the Gateway. Ultimately, all Federal agencies with E-Government processes requiring authentication will be able to use the Gateway.

5.1.4.3 Types of Authentication Accepted

The Gateway will be technology agnostic, in other words, it will accept multiple forms of authentication and differing credentials. This may require that the Gateway support multiple validation protocols to ensure the current validity and authenticity of credentials. It may also require the establishment of an organizational entity and process to determine the acceptability and trust of different forms of credentials. Currently, the Federal government supports such an accrediting entity only for digital credentials issued using Public Key encryption technology (i.e., the Federal PKI Policy Authority)¹.

5.1.4.4 Users

The user population for the 24 E-Gov initiatives is very broad. Initially, the number of users and applications may be limited, at least until the full scalability of the Gateway is assured, but the ultimate scope of users will include all citizens, businesses and government agencies in the U.S. Use of the Gateway will be voluntary for the public.

5.1.4.5 Authorized Uses

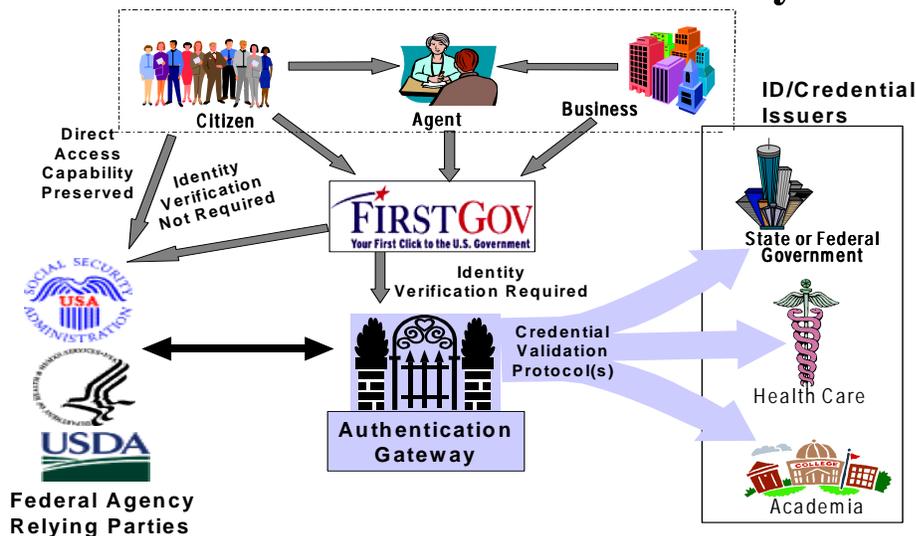
Initially, the only authorized uses of the Gateway will be to support the 24 Federal E-Gov initiatives and, potentially, other key E-Gov initiatives that are

¹ The United Kingdom helped establish TScheme to operate in this capacity.

ready for such authentication services. Ultimately any Federal agency with E-Gov services requiring authentication will be able to use the Gateway. The Gateway is not contemplated for authentication services outside of the Federal government. Use of the Gateway will be voluntary to Federal agencies.

Figure 5.1.5

The Authentication Gateway



5.1.5 Gateway Core Functionality

The high-level schematic above (Figure 5.1.5) presents the general context of the Gateway. The Gateway will be Internet-based and linked directly to FirstGov, the web-based portal to the Federal government. As indicated by the schematic, the Gateway will be accessed through the FirstGov portal and through direct links with agency applications requiring authentication.

Following are core principles for the Gateway:

- Each level of information assurance has specific identity authentication requirements and may use a different authentication solution to determine trust
- If an individual requires a higher information assurance level to transact business, they will be able to upgrade to the next assurance level, provided that they meet the requirements for the higher level
- An identity assurance that allows access at a higher assurance level will be accepted by processes requiring lower assurance levels

The E-Authentication Team is currently developing requirements. The business model for using the Gateway has not yet been established. However, it is expected that agencies will enter into a Memorandum of Understanding (MOU) with GSA in order to clarify roles and responsibilities and to authorize agency use of the Gateway, similar to relying party agreements that agencies have executed for ACES.

5.1.5.1 Enrollment

- Agencies with applications requiring authentication will enroll in the Gateway by executing a MOU with GSA
- The enrolling agency will specify the level of authentication required for each application through the MOU
- It is anticipated that GSA will maintain an authorization control system on behalf of the agency applications. The authorization control would ensure that authentication requirements meet the assurance levels specified for each Agency application. This system will be a logical, rules-based system for all applications supported by the Gateway

5.1.5.2 Validation of Credentials

- The Gateway will validate the authenticity of credentials. The Gateway may need to support multiple protocols for such validation. Standard processes and protocols for the validation of public key certificates are in place today. This public key validation function is performed by cross certifying through the Federal Bridge Certification Authority. The Federal government may find it necessary to establish standard processes and protocols for validating other forms of identity credentials
- The Validation process will include querying the credential-issuing entities concerning the authenticity of the credential. This may require agreements between the Gateway operating authority and the credential issuers

5.1.5.3 Agency Application Interface

- The Gateway will support a uniform interface(s) with agency applications
- The gateway will support a defined protocol(s) for interfacing with agency applications. The protocol will include presenting the information concerning the authenticated user in a standard way for the agency applications to accept that information

5.1.5.4 Legal and Policy Structures

GSA is authorized to provide goods and services to the entire Federal government. Such services include information technologies and security services. The GSA has statutory authority to provide IT and E-Gov services, such as those contemplated for the E-Authentication initiative, to the Federal government. Similarly, GSA established the Access Certificates for Electronic Services program (ACES) for PKI services and Common Access Card program for smart card services, under this statutory authority. These service offerings are available through government-wide contract awards. These contracts provide for the issuance of identity credentials to Federal employees and to the public. GSA

established the legal structure for these services through legally binding contracts with third-party service providers. In addition, other agencies with more limited authorities have potentially suitable services for segments of users, which will be leveraged, to the extent possible. GSA intends to provide Gateway services with one or more third-party service providers.

The protection of privacy and private information is a primary policy objective for the Gateway and E-Authentication services. It is not contemplated that the E-Authentication Gateway would collect or maintain personal information. The Federal government will ensure that the Gateway and the E-Authentication services are used only for their intended purposes as described above. The Gateway and other E-Gov services and infrastructure will comply with and support the Office of Management and Budget Federal information privacy standards, requirements and guidelines for E-Government.

5.1.6 Next Steps

The E-Authentication Team will proceed with building the policy and privacy framework (e.g., policies, practices, reviews, communications) for the Authentication Gateway that will lead to public confidence and trust in using Federal E-Gov services. Several key steps will be taken:

- Conduct risk assessments for all 24 E-Government initiatives to determine the appropriate levels of assurance and map to known classes of credentials
- Map business processes and technical solutions to the data security, privacy, and protection requirements of the system of records and Gateway operations
- Design, test and, beginning in September 2002, deploy the Gateway prototype
- Conduct a full and open competition for the acquisition of a fully functional Gateway, whose requirements will be based on the lessons learned from the prototype deployment
- Evaluate and test the Production Gateway for large-scale deployment and rollout in September 2003
- Determine the need for and develop, as appropriate, branding and marketing for the Authentication Gateway and/or the Presidents Management Council E-Government strategy in order to further build trust and protect the government's E-Gov services

5.1.7 Privacy Requirements

Information to be maintained by the Gateway will include personally identifiable information. The Privacy Act of 1974 5 U.S.C. 552a As Amended requires Federal Agencies to protect personally identifiable information. It states specifically:

- Each agency that maintains a system of records shall:

- Maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President
 - Collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs
 - Maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination
 - Establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained
- To properly protect citizen data, several issues must be addressed with respect to privacy:
 - The use of information must be controlled
 - Information may be used only for a necessary and lawful purpose
 - Individuals must be informed in writing of the principal purpose and routine uses of the information being collected from them
 - Information collected for a particular purpose should not be used for another purpose without the data subject's consent unless such other uses are specifically authorized or mandated by law
 - Any information used must be sufficiently accurate, relevant, timely and complete to assure fair treatment of the individual

5.2 Diagram Descriptions

The following diagrams and related text identify notional concepts in the evolving E-Authentication process. The first is meant to show one possible interaction with a government agency. The second shows preliminary functional principles.

5.2.1 Illustrative Process Flow Concept

Figure 5.2.1, *E-Authentication Process Flow Concept*, depicts an overview of the E-Authentication gateway concept and how it may work, followed by a description of the steps represented. This is one possible configuration of an illustrative process flow. The government is interested in other possible process flows.

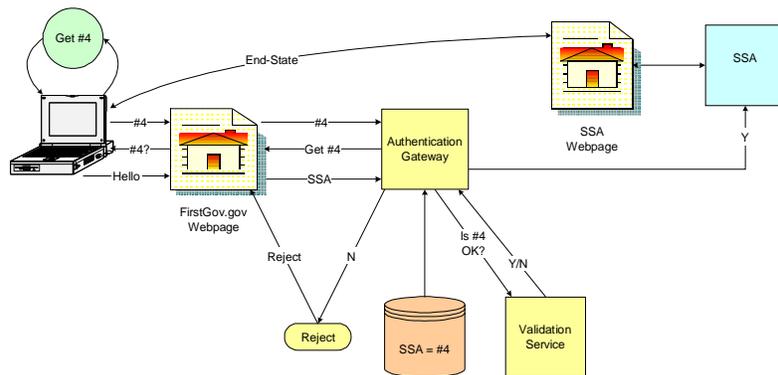


Figure 5.2.1: E-Authentication Process Flow Concept

The following interactions could take place in a typical E-Authentication session:

The scenario described below assumes the user initially discovers the desired E-Gov application via a portal, such as FirstGov.gov:

- A user comes to an official government web portal
- At the portal, the user selects an E-Gov application such as one from the Social Security Administration (SSA)
- Before the user begins interacting with the SSA application, the portal queries the E-Authentication gateway for SSA's authentication level requirements (e.g., must be level #4 in the example above). (The gateway retrieves the authentication level requirements from federated lists and databases and does not necessarily store the information locally.) Recommendations are needed on quality of service requirements – what should be done if agency system cannot support
- The gateway conveys to the user the authentication level requirements and queries the user for a credential matching or exceeding the required level
- If the user does not have a digital credential of the appropriate level, the user may go to a third party (called a Digital Credential Provider [DCP]) to obtain the appropriate digital credential
- The user's digital credential is presented to the gateway
- The E-Authentication gateway validates the user's digital credential via a validation service (this step may be transparent)
- If the digital credential is valid, the gateway's response to this effect is conveyed to the SSA application and/or the user. If the credential is not valid, the user is informed that their digital credential has been rejected

- A user may have multiple digital credentials, at the same or different levels. If the user obtains higher level credentials, the lower level credentials are still useable where appropriate
- If a user has no digital credentials, the government will provide information on credential requirements and will maintain a list of digital credential providers (DCPs) that offer digital credentials of the appropriate or higher level
- Support for validation of credentials to support anonymous access to agency applications is also expected

5.2.3 Context Diagram

Figure 5.2.3, *Context Diagram*, is a pictorial representation of the sample component roles and how they interact with the E-Authentication gateway.

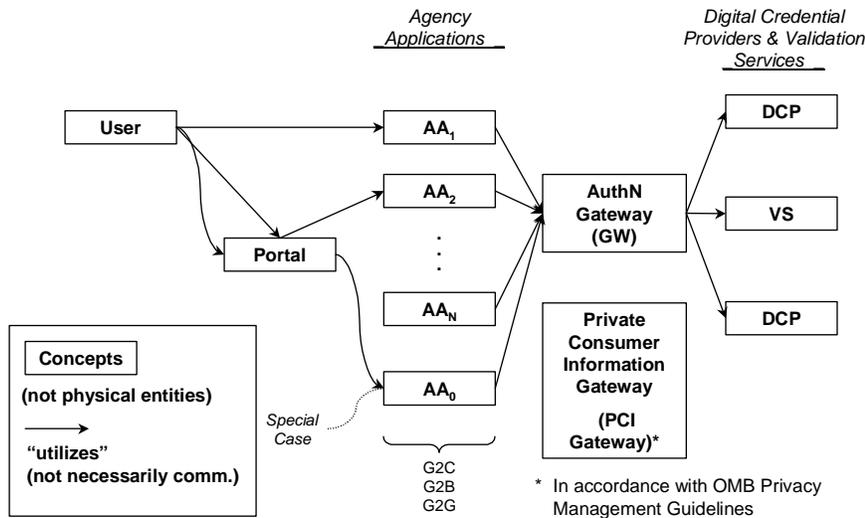


Figure 5.2.3: Context Diagram

- A user may access an agency application in the following three ways:
 - Directly
 - By visiting the portal and clicking on a link for the application (The portal may be a government portal or a private portal of a DCP)
 - Via the portal as a proxy to the application, i.e., all communications between the user and the agency application must flow through the portal
- Agency applications (AAs) may use the E-Authentication gateway to authenticate users who access the application directly, rather than through the portal. In that case, AA0 could be used to provide consistent interoperations among the component roles
- The Private Consumer Information (PCI) Gateway is a specific technical role defined to address the concept of sharing of information among the components, assuming appropriate user permissions, policies and procedures are in place. The PCI gateway supports the technical capability to transfer information collected and maintained by

others. Beyond that required for logging purposes, it is not anticipated that there will be private consumer information collected or maintained at or by the gateway

5.2.4 Components of the Gateway AuthN Services

Figure 5.2.4: Digital Credential Providers (DCP) and Validation Services (VS), depicts the components of the DCPs and their relationship to the E-Authentication gateway.

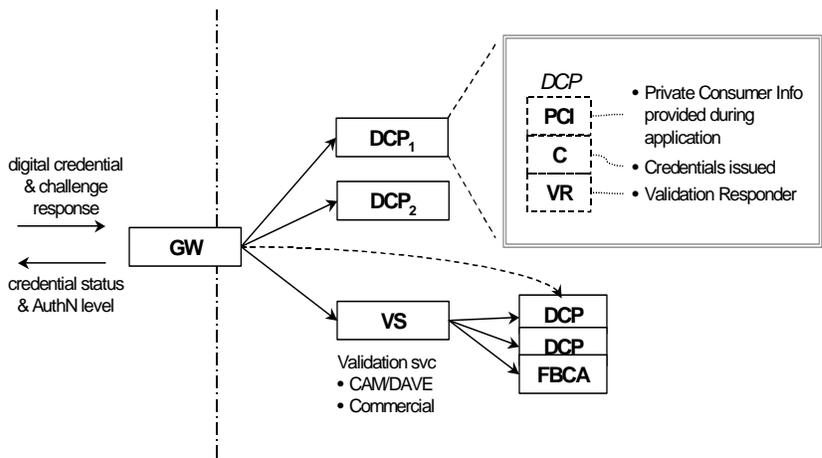


Figure 5.2.4: Digital Credential Providers (DCP) and Validation Services (VS)

- Figure 4 illustrates validation of services via direct access to the DCP and via validation services, where the validation service does not actually issue credentials.

5.2.5 Summary of Functional Principles

- Browser
 - Session management via non-persistent cookies if user permits
 - “No cookie” option must be supported
- Portal
 - Presents E-Gov services available to users
 - May request user credentials (via AA0)
 - May be session manager
 - Via “opt in” – User may indicate location of preferences
- Agency Application
 - Accepts user requests for services
 - May request user credentials
 - May utilize GW to authenticate user credentials
 - May authenticate user credential
 - Maintains list/database of Authentication (AuthN) level requirements
 - Manages Authorization (AuthZ)
- Gateway
 - Requests validation of credentials from DCP
 - Returns GW response type [including authentication requirements level]

- May be session manager
- DCP
 - Issues and manages credentials
 - Responds to status/validation requests
 - Highly federated

6. Directed Topics for Responses

6.1 Acquisition

The government has at its disposal a number of contracting vehicles from which authentication gateway services may be obtained. These include the Federal Supply Service (FSS) multiple award schedules, numerous government-wide agency contracts, or the ability to create a new contract. The purpose of this section is to ascertain if industry has a preference for a particular contract vehicle type.

- Existing Contracts
 - Is your company a prime contractor on a Government-Wide Agency Contract (GWAC) as of this writing? If so, which one(s)?
 - Are you a subcontractor for a prime that is on a GWAC? If so, which GWAC and which prime?
- Multi-vendor contract award – The government contemplates that the long-term objectives of the E-Authentication Gateway may be best served through a multiple award with common functional and contractual requirements. This configuration would require coordination and interoperability among multiple awardees in order to provide common, seamless service delivery and single sign-on capability. Input is requested on the viability of this approach and the technical and policy considerations that would be necessary for interoperable authentication services for user agency applications in a multiple award configuration

6.2 Government/Industry Relationships

The government is interested in determining if there are unique and innovative ways to build, fund, and administer the Gateway development and subsequent operation that would accomplish the government’s business objectives, leverage investment and operational costs and responsibilities, and facilitate the long-term viability of the Gateway services.

- Commercial Value of Gateway Components – The government anticipates that there will be several components of the Gateway that may have broad commercial appeal to industry and non-Federal governmental entities and other organizations/communities. These components include:
 - The Authentication Requirements Level (ARL) profile. The ARL profile will clearly define authentication levels relative to transaction types and the risks associated with them. It is envisioned that the ARL profile will provide for authentication services ranging from strong to less than strong. This Profile may be “branded” to allow for easy identification and association, and to permit marketing and brand development to develop public confidence and trust in the Profile

- Credential Evaluation and Mapping Scheme. The government envisions that it will be necessary to develop and administer a scheme for evaluating, “accrediting”, and mapping different forms of credentials that can be used to authenticate users for E-Gov services. Such credentials would include both Federal government-issued credentials and credentials issued by non-Federal entity
- Credential Validation Services. The government anticipates that some, if not all, of the credentials required for authentication will require validation of current status and/or authenticity. Validation Services, as depicted in Figure 1 of this RFI, will be required and may be performed by government entities, the Gateway Service Provider(s), or other entities

The government anticipates that these components and, potentially, other components of the Gateway may have commercial appeal and value to the private sector and other public sector entities. The government requests information on the following:

- What is the commercial value of the E-Authentication Gateway and, in particular, the Gateway components described above in the private sector and do these components and services have broader based application than just for the Federal government?
- In what ways can the government leverage that value with industry in terms of innovative funding strategies, such as share in savings, cost sharing, fee for service, subscription fees, or other approaches?
- The Development and Administration of Gateway Components – The government anticipates that the development and administration of the Gateway components described above and, potentially, other components of the Gateway may be facilitated through efforts already underway in industry. The government seeks information on the existence of industry-based efforts to develop and administer service components needed for the Gateway and the application of those efforts to the Federal E-Gov initiative. In particular the government seeks information on:
 - What are the potential relationships (contractual and otherwise) between government and industry that could facilitate the development and administration of Gateway services and how is it envisioned that it would work?
 - What is the value proposition for such relationships/partnerships? What is the value to the government? What is the value to industry?
 - Are there any particular alliances, consortia or standards bodies that the government should be participating in? If so, what are they?

6.3 Technical

- Response Types – It is anticipated that the gateway will provide the following types of responses for use by the agency application:
 - An “anonymous ticket” (similar to movie tickets) that do not contain user-specific information, and that are used for anonymous access. The presence or possession of an anonymous ticket means that some criteria have been met. There is no way for an agency application to obtain additional user information automatically.
 - A “pass” (similar to an airline pass) that has a full, stand-alone payload, which contains the user’s submitted credentials. There is no need for an agency application to obtain additional user information automatically.
 - A “partial pass” which contains some user-specific information, and which an agency application use to obtain additional user information automatically if desired.

- A “voucher” (e.g., an ephemeral handle or index into a database to which additional user information is obtained). There is no user-specific information in a voucher.

Please comment on these suggestion response types. Are they sufficient, or are additional types needed? Are their existing, applicable “standards” in this area?

- APIs – Please provide architectural and technical information and/or recommendations on applicable APIs for consideration for use in the E-Authentication gateway system. (As appropriate, please discuss from the perspective of ease of interfacing to the portal, gateway, AAs, and DCPs.)
- Applicable standards – Please provide recommendations on applicable standards (e.g., application communication protocols, session management techniques, etc.) that should be considered for use in the E-Authentication gateway system. A part of the gateway strategy is an open design and a desire to allow the gateway to evolve with technology. (As applicable, please consider interactions between: the portal and the gateway; the portal and agency applications [AAs]; AAs and the gateway; the gateway and digital credential providers [DCPs].) (Please apply a flexible definition to the term “standards”. Please feel free to comment on ISO standards, IETF, RFCs, OASIS standards, de facto standards, best common business practices, etc.)
- Architecture constraints (e.g., use of federated models)
 - Please provide architectural and technical information as well as viability considerations regarding an implementation where the E-Authentication gateway provides authentication services only; where authorization and access privilege information is neither maintained nor managed at the E-Authentication gateway (e.g., authorization and access privilege information maintained and managed at the AA or at a portal).
 - Please provide architectural and technical information as well as viability considerations regarding an implementation where the E-Authentication gateway provides validation of credentials on behalf of the AA, when AAs are accessed directly by the user, via the portal as a set of links, and via the portal as a “proxy” for the AA.
 - Please provide architectural and technical information as well as viability considerations regarding an implementation where the E-Authentication gateway determines if the user credential presented for validation meets or exceeds the AA identity authentication (AuthN) requirements for the requested service, where the AA AuthN requirement information is maintained in federated lists/databases (e.g., not located as part of the E-Authentication gateway).
 - Implications on AuthZ of this federated AuthN process given the highly diverse AuthZ environment of the Federal government.

- Scalability strategies
 - Please provide architectural and technical information regarding scalability strategies and considerations. (Consider this in the context of anticipating continued increased public usage that exceeds timely response capabilities of the initial gateway system.)
- Interoperability with multi-vendor, multi-sector approach
 - Please provide architectural and technical information regarding an implementation where multiple gateways by different vendors are deployed. (Please elaborate on circumstances where E-Authentication sessions begun in one gateway could be transferred to another gateway. Are there established standards [e.g., SAML] that are applicable in this scenario?)
- Session Management – Please provide architectural and technical information regarding session management strategies. Please address issues such as: access via traditional wireless devices (e.g., cell phones, PDAs); access via browsers configured to prohibit cookies; session management transfer between different gateways; ephemeral handles or keys to minimize user tracking vis-a-vis activity logs; etc.) Also, please provide suggestions for how an agency application (AA) could correlate ephemeral session handles to static entries in that AA’s customer database.
- Conceptual drawings and diagrams identifying alternative process flows to those identified above are encouraged.

6.4 Credential Evaluation and “Mapping”

Please provide architectural and technical information concerning methods for establishing, mapping and maintaining a finite but potentially large spectrum of digital credential relationships and equivalences. Consider applicable standards and protocols for exchange and communication of credential characteristics, currency, issuing bases and interfacing with Agency applications both modern and legacy.

6.5 Compliance with Government Mandates for Protection of Privacy Information

The government anticipates that the E-Authentication Gateway will not maintain locally stored personal information other than standard logs of authentication transaction activity. The government intends that any of the information that must be maintained by the Gateway for transaction audit purposes will be required to meet, at a minimum, all protection, confidentiality, and disclosure requirements of the Federal Privacy Act. As stated above in this RFI, the government anticipates that the services of the Gateway may have broader commercial and public sector application than just for Federal services. The government requests information on the willingness of potential private and public sector participants and users of Gateway services to meet the requirements of the Privacy Act and other Federal requirements associated with the protection of personal information.

6.6 DCPs

The government anticipates an operating environment where digital credentials issued by entities other than the gateway are submitted to and validated by the gateway to meet authentication requirements of AAs. It is expected that the community of digital credential providers (DCPs) will be highly federated. As indicated in Section 6.2 of this RFI, the

government envisions that it will be necessary to develop and administer validation processes. The government requests information on this approach from potential DCPs pertaining to:

- What is the willingness of potential DCPs to participate in the Federal E-Gov authentication process?
- What are potential processes and forums for the development of schemas for evaluating types of credentials for different assurance levels? In particular, the government is interested in information on industry-based forums that could be used to meet the government's objectives.
- What are the business models for DCPs for the authentication services as presented in this RFI?

6.7 Anonymous Access

What technologies are available for anonymous but authenticated access? What is the maturity of such technology? Is it scalable to a level appropriate for use within the E-Authentication program?

6.8 Session Management

What technology is or is not required for session management? Can single sign on solutions be provided without session cookies being utilized?

6.9 PCI Gateway

Please provide input on the following:

- To identify the requesting agency application is authorized to receive the requested user information.
- Where should that agency authorization information be stored?
- How a user pre-authorizes release of user-selected private information?
- Situations where the user does not give a pre-release authorization, but yet agencies are permitted by law to share?

7. Glossary of Terms and Acronyms

Term/Acronym	Definition
AA _n	An “arbitrary” Agency Application
ACES	Access Certificates for Electronic Services
API	Applications Programming Interface
ARL	Authentication Requirements Level
AuthN	Authentication
AuthZ	Authorization
CAM	Certificate Arbitration Module
CRL	(digital) Credential Revocation List
DAVE	(path) Discovery and Validation Engine
DCP	Digital Credential Providers
FBCA	Federal Bridge Certification Authority
FirstGov	Government wide portal found at www.firstgov.gov
FPKIPA	Federal Public Key Infrastructure Policy Authority
FSS	Federal Supply Service
G2B	Government – Business transactions
G2C	Government – Citizen transactions
G2G	Government – Government transactions
GSA	General Services Administration
GW	Gateway
GWAC	Government-wide Agency Contract
IETF	Internet Engineering Task Force
ISO	International Standards Organization
MOU	Memorandum of Understanding
OASIS	Organization for the Advancement of Structured Information Standards
OMB	Office of Management and Budget
PCI	Private Consumer Information
PDA	Personal Digital Assistant
PKI	Public Key Infrastructure
RFC	Request for Comment
SAML	Security Assertion Markup Language
SSA	Social Security Administration
VS	(Digital Credential) Validation Service