

**General Services Administration
e-Authentication Gateway Request for Information
Synthesis of Responses**



**e-Authentication Program Management Office
January 2003**

Question 6.1 Acquisition – Preferred Contract Vehicle

RFI Question 6.1 -- Response Synthesis

6.1.a. Is your company a prime contractor on Government-wide Acquisition Contract (GWAC)? If so, which one?

6.1.b. Are you a subcontractor for a prime that is on a GWAC? If so, which GWAC?

Twenty-eight (28) respondents indicated that they are currently on a GWAC; the remaining twenty-six are not. It should be noted that some respondents indicated that they were on a GWAC when, in fact, there was a government contract vehicle in place, but not necessarily a GWAC.

The schedules which respondents indicated that they were currently on most frequently were: GSA Schedule-70 Information Technology Schedule, GSA Millennia and Millennia Lite, and GSA Schedule-874 Management, Organizational, and Business Improvement Services (MOBIS) MOBIS.

However, the following list contains GWACS and contract vehicles that respondents reported currently being on:

- GSA Safeguard Program
- GSA Schedule-539 Solutions and More
- GSA Schedule-871 Professional Engineering Services Schedule (PES)
- GSA Schedule-36 Document Imaging and Records Management GS-25F-0143M,
- GSA Safeguard
- GSA Seat Management
- GSA Smart Access ID Card
- GSA ANSWER
- NIH Chief Information Officer Solutions and Partner 2 Innovations CIOSP2
- NIH - NIH ECS2
- DOT Specialized Technical and Technology User Support Contract
- DOT VANITS
- DOT TASC
- DISA ENCORE
- DISA NexGEN
- DISA ITS
- ITOP ISS
- NASA SEWP
- DOJ ITSS
- DOJ JCON I & II
- DOT Physical Security Systems DTRS57-01-D-30004,
- DOT Value-Added "Niche" Information Technology Services (VANITS)
- DOC Commerce Information Technology Solutions
- DISA I-Assure

Question 6.1 Acquisition – Preferred Contract Vehicle

6.1.c. Provide input on viability of multi-vendor contract award. Identify technical and policy considerations for interoperable authentication services with this approach.

Convergent Responses:

The majority of respondents indicated that a multi-vendor award was necessary given the breadth and scope of services envisioned for the Authentication Gateway. There was general convergence on the following:

- A large and diverse program such as E-Authentication is best served by allowing competing approaches to the services the program will provide through multi-award contracts.
- Service providers under such an arrangement will likely be consortiums – best of breed service providers and technology vendors teaming to provide each of the technical and operational services required by the Authentication Gateway.
- Multi-vendor award would best meet Government's needs but require common policy, functional, and contractual requirements for all vendors.

Issues:

While the majority of respondents recommended that the Government pursue multi-vendor awards for the Gateway, most respondents also raised issues/concerns with this approach.

- The multiple award contract is an ideal vehicle for commodity products, however experience has shown that for unique or new technology, or for implementations requiring a considerable integration of a number of other technologies, the multi-award contract presents considerable challenges.
- Multi-vendor awards may lead to considerably higher infrastructure and operating costs due to redundant implementations that constrain deployment and success.
- Multi-vendor awards may lead to competitive distractions that tend to focus vendors more on beating each versus working cooperatively to produce the best solution and make it successful.
- The project management will be complicated. The timeframe will potentially be extended, and the need to mitigate the risks associated with this type of award could increase the overall project costs.
- Technical considerations exist in implementing an interface that can provide equitable interoperation between multiple authentication services, and awardees. These issues can be reduced through the use of common communication protocols. A common interface between the AA and Authentication Services to handle AA specific policies would substantially mitigate the time and risk to bring AAs on-line.

- Duplication of contracts and implementations will add to the cost.
- Special care must be taken to avoid the very real potential of shifting systems integration risk from the vendors to the Government.

Divergent Responses/Outliers:

While a minority, several respondents indicated that a multi-vendor award would not be in the Government's best interests and a single vendor award better meet Government's needs.

- Government should consider a single award acquisition on a current GWAC contract and look for a multi-contractor team that consists of sub-contractors with proven e-authentication expertise and knowledge as preferred acquisition approach.
- Given the scope and complexity of the e-Authentication initiative, a multi-vendor award may not be the best acquisition approach in light of the Government's aggressive timeline to have a full operational capability by September 2003. Rather, the Government should look to deploy the most streamlined acquisition strategy possible to include rapid release of the RFP and a single award to a team of proven industry performers.
- A complex acquisition strategy requiring multi-vendor awards would jeopardize the achievement of the target date.
- There are no similar projects involving several vendors providing seamless service delivery and single sign-on across multiple platforms, applications and databases. The technology required to do this is in early stages of development and deployment that will increase the risk to GSA of a successful project.
- There is not a clear business case for a multi-vendor contract award given the uncertainties involved in large-scale deployment of e-Government services to date.

In addition, several vendors recommended that the Government pursue performance-based contracts with a single vendor/integrator as the best approach for success.

- Of all the tasks associated with the E-Authentication initiative, the R&D effort required to develop a functional Gateway product entails the greatest performance uncertainties, as the likelihood of changing requirements is high. These uncertainties make it difficult to estimate performance costs in advance. Correspondingly, a performance-based contract in which both the government and the contractor share the risk will likely be the best approach.
- A performance-type structure with incentives would provide the Government with the ability to target specific objectives and enforce schedules for completion of those objectives.

Question 6.2 Government/ Industry Relationships – Innovative Gateway Development and Operation

6.2.a. What is the commercial value of the Gateway, specifically the components Authentication Requirements Level profile, Credential Evaluation and Mapping Scheme, and Credential Validation Services. Do these components and services have broader applicability outside the Federal Government?

Convergent Responses:

The majority of respondents indicated that the Gateway components, as presented in the RFI, would have value for use for commercial applications. In particular, respondents indicated that the Authentication Requirements Levels would and should have broader application than just the Federal Government, and this would be an important stimulus for generating public trust and confidence for e-authentication services and e-transactions.

- Conceptually, the overall functionality represented in the government's objective should have broad commercial appeal. The e-Authentication Gateway Service clearly has value beyond the government market, and could provide a very cost-effective managed service for the commercial mid-market, where corporations require the security, but lack the funding to develop and deploy a comprehensive security solution.
- The various components of the E-Authentication Gateway will have value to a broad range of commercial and other public entities. The need of commercial entities, for example, to interface with and utilize government services with respect to information retrieval, contract opportunities, and required federal filings, to list only a few, is significant.
- The commercial value of the E-Authentication Gateway, in particular, the Gateway components, have a much broader based application than just for the Federal government. If the E-authentication Initiative is successful and the trust elements and levels of trust receive general acceptance with the general public and American business, they could become the de facto standard.
- The fact that a Gateway/portal can consolidate access to data from various sources behind a common, easy-to-use interface is also of commercial value.
- In the immediate future, we see some commercial value in the E-Authentication Gateway components. Industry may, at some point, follow the Government architecture and adopt the same components that make up the architecture. If the trend for greater authentication carries over to business in the same manner as designed by Government for this acquisition then they will have greater appeal.
- The Authentication Requirements Level (ARL) profile: The ability to provide a range of authentication services would be of immediate commercial interest. The preponderance of industry effort to date centers on "hard" authentication, such as PKI implementations, and most recently biometric authentication. By providing a range of alternatives across the authentication spectrum, the potential to offer the availability of such products to smaller organizations that cannot afford the full implementation of PKI, but are nonetheless concerned about security in an E-Government or E-Business environment, is greatly increased. It is within this realm that the intermediate levels of authentication, as addressed in the Executive Summary, and in paragraph 3.0 of this response, would be particularly attractive.

- The development of an ARL profile could provide a common framework for private sector suppliers of Web services to build their own authentication systems, thereby establishing industry wide standards that are more efficient, secure, and simple for the end user. The development of a "branded" ARL profile (that would be more "trusted" in theory) could be developed by the E-Auth Gateway and integrated by private sector partners to boost consumer confidence in the security of online transactions and services.

Issues:

- If privacy policy issues surrounding the use of credential information can be resolved (or perhaps waived by individual users) and there is broad application across commercial markets that should generate a number of credential validation services desiring to enter the market space.
- There is a vast difference between “credential validation”, “authentication requirements levels” and true, bona fide authentication of a user. The former merely validate database entries and confirm registration entries. The latter is a stand-alone system requiring an interface.
- The Gateway would have more intrinsic value if the Government could serve as the credential provider and commercial industry could use those credentials.
- The value depends on a finely grained ARL that can meet government, commercial, and, potentially, international user needs and requirements. Therefore, there must be a fine balance between specificity and flexibility –this may not be possible in the short or long term.
- A non-centralized Gateway would allow user communities (e.g., States, financial institutions, health care, etc.) to define ARLs that would be most appropriate for their specific applications and business needs. It may not be possible to craft a set of ARLs that meet the needs of all users.

Divergent Responses/Outliers:

- It is not clear that the introduction of ARL profiles to the commercial marketplace would generate sufficient cost savings to displace this method, that the introduction of authentication levels relative to transaction types are desired or required in the commercial space, or that users would tolerate the necessarily stringent process to verify their identity for use by commercial applications. Accordingly, we believe that the appeal of ARL profiles is of uncertain commercial value to all but the largest commercially web-based application providers.
- The tone of the RFI and the specific questions asked suggest that the government is again seeking industry “partners” who can shoulder the upfront investment to get an e-Authentication system going, in hopes of some later payout. Based on past experience on similar programs, and on the changed economic climate of the last two years, we find this very unlikely.
- The application by the Federal Government of the e-Authentication Gateway components should follow the same path to application by state and local governments. However, it is unlikely to see a similar migration to the commercial sector at this time. This is because the e-Authentication Gateway does not create any new technologies.
- The E-Authentication gateway architecture is similar to many current gateway implementations. However, it is difficult to quantify the commercial value of the gateway components at this time. It is evident that the authentication requirement level profile and credential evaluation and mapping scheme components have a need in the commercial sector, but the need is limited to select applications. As more applications require these capabilities in the future, the value of the gateway components can more easily be determined.
- It is not clear that the ability to dynamically map credentials to individual services or have the ability to access a large number of credential types are desired or required in the commercial space
- There is a vast difference between “credential validation”, “authentication requirements levels” and true, bona fide authentication of a user. The former merely validate database entries and confirm registration entries. The latter is a stand-alone system requiring an interface.

6.2.b. In what ways can Government leverage that value with industry?

Convergent Responses:

In general, respondents indicated that the Government could establish various bases for fee charging that would reduce/leverage up-front investment and ongoing operational costs for the e-Authentication Gateway.

- The Government could set up an authentication service that would be made available to industry. The credential bridge concept could also be made available. Fees could be collected from private companies that wish to use these services. However, the fees must be small enough to encourage participation
- The implications of the e-Authentication Gateway are vast. State and local governments could employ the model and be charged back for access. All federal agency compliance could be dictated through the gateway to client systems reducing infrastructure size and cost

- Bi-lateral agreements could be developed to enable authenticated linking between the e-Authentication Gateway and industry partners with higher traffic volume in order to increase usage of Government services.
- Membership fees could be charged to industry partners who choose to implement ARL profile compliant authentication systems to help defray the cost of operating the e-Authentication Gateway services.
- Value added services provided by private sector industry partners could be integrated into the E-Auth Gateway in order to ensure a better user experience and wider scope of functionality by placing authenticated links to selected service providers.
- Incentive programs could be developed including discounts for consumers that access the services of industry partners through the E-Auth Gateway.
- There is no doubt that the development and implementation of an E-Authentication Gateway will provide value to the e-Gov applications that use it. The measurement of that dollar value to the applications being served is a task that has not yet been addressed. We recommend that the value to the applications be understood and quantified as a step in the implementation of the overall e-Authentication Initiative. This understanding would be the basis for cost sharing, fee for service, subscription fees, or other approaches that GSA could negotiate with the Agencies using the e-Authentication Gateway.
- By providing a range of alternatives across the authentication spectrum, the potential to offer the availability of such products to smaller organizations that cannot afford the full implementation of PKI, but are nonetheless concerned about security in an e-Government or e-Business environment, is greatly increased.
- Credential Evaluation and Mapping services could effectively be made commercially available on a fee for service basis, whereby a user would purchase the validation to allow access. This could potentially lower GSA's overall cost for operation of the Gateway since the validation service contractor would be funded in part by user fees.
- A fee for service model would be the most efficacious for government and industry. This is an assured and efficient way the government will realize its goals for the e-Authentication initiative. A fee for service model will have attractive features for industry and government. Industry will operate the infrastructure for the e-Authentication Gateway that it may also use to provide services commercially. Government will realize economies of scale inherent in the model where it receives a service that is provided from an infrastructure.

Divergent Responses/Outliers:

- The existing services (Passport and Liberty Alliance) do not generally charge for their services. The real value is the expanded use of the web resources that are accessed via these systems and the revenue impact of expanded access.

6.2.c. 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?

Few responses were received for this question. In general, respondents cited contractual and sub-contractual relationships as the basis for Government and industry to relate in the development and administration of the Gateway. Some respondents recommended outsourcing the Gateway completely as a managed service. Others offered variations on contractual relationships.

6.2.d. What is the value proposition for such relationships partnership? What is the value to the government? What is the value to industry?

Value proposition to Government:

- Defrayed costs of system administration and management.
- Wider scope of accessible services through the E-Authentication Gateway beyond the government services.
- Greater awareness of E-government services and more frequent usage of the E-Authentication Gateway by consumers and businesses.
- Increased involvement by citizens in government activities due to ease of access and improved efficiencies.
- Shared traffic from higher volume private sector web sites and services.
- Continued movement towards the establishment of industry standards for online identity and authentication.
- Establishment of a unified authentication platform for partners to work with government agencies thereby allowing the government to more easily utilize the expertise and technology of private sector service providers.
- common infrastructure, policies, and business practices for identity management and authentication services.
- The government can take advantage of a mature set of products that have a proven track record in private industry as well as the experience of integrators with documented success stories. There is no need to develop a GOTS product.
- Involvement in industry efforts to develop products.
- The real value proposition of such a relationship is ultimately the ease of use and access to services afforded the end-user.
- Ability to leverage industry's experience in Gateway development and administration. Experience in the development and administration of Gateway services that has taken years for industry to develop can be transferred to government in months and accelerate speed to market within the 24-month time frame.
- Provide joint visibility to both Industry and Government organizations of evolving commercial and government requirements.
- Lower deployment and on-going operational costs for the government.

- Expedite definition of emerging standards and policy relative to E-Authentication. This has the widespread benefit of expediting the achievement of the President's Management Agenda and the PMC E-Gov Strategy in the public sector.
- Government will be able to leverage an industry-leading model that will have application in and outside the government.

Value proposition to Industry:

- Acceptance/endorsement of commercial products for use in the E-Authentication Gateway.
- Ability to defray some of the costs of developing internal gateways by providing some of the components, infrastructure or lessons learned to the Federal government.
- Industry partners can leverage their existing human and technical resource pool to provide 7 X 24 support and leverage some of the costs of training and maintaining around the clock operation on multiple clients.
- Industry partners will need to remain at the forefront of the technology and will be in a better position to ensure that new or evolving standards, technologies and protocols are supported and being incorporated on a continuous basis, as part of an on-going maintenance and capability improvement program.
- Expedite definition of emerging standards and policy relative to E-Authentication, which will make standards available in the private sector that will simplify and accelerate the use of commercial e-Authentication initiatives, which will in turn reinforce and lower the cost of e-Authentication in the public sector.
- The value to industry is that the same robust platform that is used for the commercial customer base will be leveraged for the government customer. This will be an incentive for industry to commit a healthy R&D investment in the provisioning of these services.

Issues:

- One of the major commercial concerns regarding implementing the Authentication Gateway is vendor liability. The RFI does not mention this issue and we believe that the government must immediately begin to develop a liability mitigation strategy and proposal for the commercial sector. Any commercial vendor choosing to participate in this initiative, whether during development or operations, is exposed to a significant amount of financial liability for the data it is certifying, exchanging, validating, authorizing and/or maintaining. Because of the large scale of users, applications, functions, transactions, and other components of this system, a participating vendor is at significant risk if the government does not address this issue quickly. The government must be proactive in proposing creative and appropriate liability mitigation approaches in order to minimize the exposure commercial partners will face.
- It seems likely that certain major industry domains (finance, energy) will determine their own e-Authentication solutions. As an analogy, the Federal Government did not define its own credit card standard. Rather, it evolved its payment processes to include the use of credit cards by Federal Government employees. Similarly, commercial enterprises did not devise their own clearance

requirements. Rather, enterprises adopted policies and procedures that were set by the DOD. The same is likely to be true for electronic authentication. It is anticipated that the Financial Services Industry will define its own solutions. If the Federal Government wants to leverage that infrastructure for Government purposes, the Federal Government should expect to adopt the processes and procedures the Financial Services Industry develops, and participate in the development of the Financial Services Industry infrastructure. The use of commercial DCP's in the E-Authentication Gateway affords one mechanism for this sort of participation.

6.2.e. Are there any particular alliances, consortia or standards bodies that the government should be participating in? If so what are they?

The majority of respondents indicated that the Federal government should participate in the existing technology forums/standards groups of the Liberty Alliance and OASIS (Organization for the Advancement of Structured Information Standards). Additional specific recommendations are listed below:

- American Bar Association initiatives for authentication and identity management PKI Forum,
- Computing Technology Industry Association (CompTIA),
- Computer and Communications Industry Association (CCIA),
- CREN (Corporation for Research and Educational Networking),
- EDUCAUSE,
- Electronic Industries Association (EIA),
- Indentrus,
- Institution for Electrical and Electronics Engineers (IEEE)
- International Electrotechnical Commission (IEC),
- International Security Trust and Privacy Alliance (ISTPA),
- International Telecommunication Union (ITU),
- Internet Engineering Task Force (IETF)
- Internet 2 Shibboleth initiatives
- National Automated Clearinghouse Association (NACHA)
- Open Web Application Security Project (OWASP)
- Software Productivity Consortium (SPC)
- Software Engineering Institute (SEI) at Carnegie Mellon University
- Universal Description, Discovery and Integration (UDDI) project that creates a platform-independent, open framework for describing services, discovering businesses, and integrating business services using the Internet.
- W3C (World Wide Web Consortium).

Question 6.4 Credential Evaluation and “Mapping”

6.4.a. 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.

Credential Evaluation and Mapping Scheme. The government envisions that it will be necessary to develop and administer a scheme for evaluation, “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.

Summary Analysis

1. There is wide support of the federated approach.
2. There is wide support for incorporation of PIN/PW and digital certificate.
3. There is general agreement that the E-Authentication Gateway is a viable approach.
4. Several respondents expressed support for some use of biometrics.

Summary of Convergent Responses

A. Identity Mapping

1. Support for federated approach.
2. Several citations of XNS.
3. Many citations of SAML to communicate security information.

B. Credential Mapping

1. Most responses included PIN/PW and digital certificate.

C. Policy Mapping

1. Several referred to use of pre-established policies, and mapping of those, implying or stating that the mapping would be controlled by one or more Policy Authorities.

Summary of Divergent Responses

A. Identity Mapping

1. Some responses said there would be one method for modern applications and another for legacy applications. Other responses said one method would work for both.

B. Credential Mapping

1. Some respondents said many (or “all”) types of credentials should be supported by the Gateway. Others said the Gateway should be limited to a few types (e.g., PIN/PW and digital certificate), e.g., to assure successful implementation.

2. Some respondents citing biometrics mentioned one or more particular types (e.g., fingerprint) or uses, but others cited them only as a general class without detail.

3. One respondent argued for a scoring method to assess the strength of presented credentials, and said this approach allows for combining credentials of all types in generating a score for an individual’s submission to the Gateway. (This is cited as an outlier in the Detailed Analysis.)

C. Policy Mapping

1. The scoring method (see B.3. just above) would substitute for mapping of one policy to another. However, each policy that is incorporated into the operation of the Gateway would have to be mapped into a score initially. (And how to do that is problematic.)

2. Another respondent (see first paragraph of Policy Mapping, in the Detailed Analysis) suggested a strategy whereby credential requirements would be mapped into “roles”, but did not explain how this would reflect policy.

Summary -- Issues

1. Scalability is an obvious issue, and was included in the RFI as part Q6.3. Scalability is an issue for evaluation and mapping of a user’s credential(s) as it is for other aspects of the Gateway architecture and operation. One respondent, for example, suggested that authentication (and possibly authorization) information about evaluated credentials be stored in a geographically distributed database similar to that of DNS.

2. Is Credential Mapping necessary, i.e., is it necessary to make use of combinations of credentials for a user? Alternatively, can different types of credential (e.g., PIN/PW as one type, and digital certificate as another type) be kept categorically separate in the operation of the Gateway, such that an authentication requirement would be defined in terms of one type of credential or another, but not a combination of dissimilar types? If combinations of dissimilar types of credentials are necessary, how can those be combined in a meaningful way?

3. Besides an ordered series of discrete Levels of Assurance, is there a workable alternative of a continuous Assurance Scale, by which multiple credentials could be combined to produce a composite Level of Assurance located on that Assurance Scale?
4. Is there a practical use of a biometric as an identifier or credential presented to the Gateway (in contrast to the use of a biometric used to unlock a different type of credential for presentation to the Gateway)? If so, how would that work? How would the necessary scalability and privacy be achieved?
5. Are two types of credential – PIN/PW, and digital certificate – sufficient, at least for the initial version of the Gateway, or are there other types that are necessary?

Scope

The electronic credentials here are those that can be used to authenticate users (individuals, businesses). “Authenticate” in this context means to conclude based on satisfactory evidence (see the second following paragraph) that the person (or other entity) using an identity is the rightful possessor of that identity. This authentication includes two components: (1) using an identity, and (2) authenticating that identity by use of the credential (i.e., by use of authenticating information that makes the identity credible) and possibly other information. A user may have different identities for different Agency applications (AAs) and different identities from different credential providers. For example, a user might have the following identities: Albert Bruce Citizen, albertc, alcitizen, alcit01, abcitizen, acitizen, abc789, citizen_ab. The contemplated Gateway architecture provides for a user to authenticate with one of his/her/its identities, and thereby to gain access to multiple AAs (i.e., multiple accounts, or applications, or processes), even though those accounts know the user by different identities. Hence, there is a need for mapping such identities for the same user, one to another. This may be called “Identity Mapping”.

The authenticating information associated with an identity consists of one or more elements that only the rightful possessor of that identity is presumed to know, have or be. Examples are: PIN/password, secret key, private key (something the user knows), fingerprint or other biometric (something the user is). (As to something the user has, see the next paragraph.) There is a need for the Gateway to accommodate different types of authenticating information. Hence, there is a need to establish relationships or equivalences among these different types; this may be called “Credential Type Mapping” or more simply “Credential Mapping”.

Credentials may be stronger or weaker, according to the type of credential (i.e., the type of authenticating information), the issuing basis (whether an in-person appearance was required, what kinds of source documents or other credentials were used in the credentialing process, how such identity proofing evidence was evaluated, and so on). The strength of a credential also depends on how hard it is for someone to discover the authenticating information and the physical form in which it is stored and protected (e.g., whether a token of some type – something the user has – is used). In general, the strength of a credential depends on the policy for its issuance and management, and that policy is the operational definition of “satisfactory evidence” at a named (or implicit and unnamed) Level of Assurance. Different AAs have different requirements for the strength of credential, depending on the level of risk, the sensitivity of information, or the value of transaction. These requirements may be expressed as a required score (according to some particular scoring algorithm) or as a selected Level of Assurance. Although the authorization control for a user’s access to an AA is outside the scope of this analysis (see the second paragraph below), the Gateway will accommodate credentials based on

different policies for their issuance and management (i.e., Levels of Assurance). The relationships and equivalences among credentials based on different policies may be called “Policy Mapping”.

The scope of this analysis includes Identity Mapping, Credential Mapping and Policy Mapping. (Credential Mapping and Policy mapping are separate for purposes of analysis, but in the design of the Gateway the former may be folded into the latter.)

Per RFI Section 5.1.5, this analysis assumes that the Gateway will know the level of authentication required for each AA. Further, it is assumed here that this information includes the type of credential if the AA has such a requirement (and this would be part of the policy defining the Level of Assurance). Therefore, a credential presented by a user will be pre-screened by the Gateway to determine that it is of an acceptable Level of Assurance for the particular AA, before the validation step. Presumably, if a credential has been validated for one AA and then the user wants to use it for access to another AA, the first validation will suffice for subsequent AAs during the same session unless, possibly, a time-out has been reached. The scope of this analysis does not include authorization methods (e.g., use of individual identity vs. group identity, or use of supplemental authenticating information for a particular AA), nor does it include the selection of a Level of Assurance for a particular AA, since authorization is in the domain of the AAs. However, a credential such as a digital certificate may include authorization information, and such a credential (when authenticated) can be passed to the AA. And, an authorization proxy, acting on behalf of one or more AAs, can be incorporated into a gateway.

Many respondents mentioned standards in connection with Q6.4, such as SAML and LDAP, but the standards are more thoroughly treated under 6.3 and so are not dwelt upon in this analysis. Similarly, there are several mentions of alliances, consortia or standards bodies (e.g., Liberty Alliance and XNS.org) in responses to Q6.4, but these are more thoroughly dealt with under 6.2.

The scope does not include credential validation services, except as they may be reflected in Policy Mapping. (Validation is covered primarily under Question 6.3. However, the policy underlying a Level of Assurance will (or might) include requirements relating to validation.) The scope does not separately address the physical forms of credentials (e.g., smart card, USB token) but they may be reflected in Policy Mapping. It does not separately address the forms of source documents and other elements of identity proofing for issuance of a credential, since these are included in Policy Mapping. However, if such a document is to be used electronically as an identifying and authenticating credential (e.g., if a user keys or scans in an account number and keys in a password), then that electronic submission is a credential for purposes of this analysis. A biometric submitted to the Gateway or associated credential validation service is also included as an identifier and/or as authentication information.

Detailed Analysis -- Convergent Responses

Identity Mapping

- A respondent described an enterprise-level credential provisioning system using its own markup language, Directory Access Markup Language (DAML), which has been offered as the basis for a forthcoming Service Provisioning Markup Language (SPML) from OASIS. This would provide a common language for provisioning services, thus facilitating identity mapping.
- Another respondent described a suite of COTS products including an identity manager to which a user authenticates by means of a unique credential that describes the user as known to the system registry. Following that, the system builds a credential to access a particular application.

Apparently the system is not suited for a federated identity environment. However, it includes a customizing tool that can be used to allow an external authentication mechanism to be used for clients that are not in this system's registry.

- Another respondent named two methods as viable for identity processing: (1) use the Gateway as a central uid/password issuer, and (2) the Liberty model.
- Another described how a federated architecture works. Another described how its product could support a federated environment such as .NET Passport or Liberty.
- A respondent described (in considerable detail) the Extensible Name Service (XNS), designed to allow identity services such as single sign-on authentication to operate on a federated basis. Respondent is a provider of products based on that protocol. The authentication service enables a user to prove they are the rightful controller of an XNS identity. XNS identity documents contain links to other identity documents. XNS identity documents can be globally distributed as DNS identities are, thus achieving scalability like that of DNS. This technology appears to be potentially important.
- A respondent explained a preference for a role-based method, rather than rule-based, for federated identity management based on directory technology.
- Liberty architecture can be used for federating identities. But for legacy applications, mapping of multiple identities could be done via a simple SSO adaptation layer that accesses application-specific credentials stored in the Gateway.
- Two respondents described their own designs for identity services based on the Liberty model, primarily from the point of view of public key credentials.
- One respondent described an enterprise identity manager with a capability to auto-discover user identities, and map them to create a user's virtual identity, but did not explain how this works.

Credential Mapping

- Several respondents described products that can handle multiple types or all types of credential, or stated an opinion that many types will have to be accommodated.
- A few respondents urged that the number of credential types be kept small, to keep the design simple and achievable.
- Most responses included passwords and digital certificates. One response seems to be oriented solely to passwords, but could use one (strong) password to protect access to the passwords for multiple applications. However, through the use of Pluggable Authentication Modules (PAM), it's possible that biometrics could be included, although the respondent didn't make this claim. Another described a master authentication credential consisting of email address, password and PIN.

- One respondent advocated that passwords be combined with PKI to provide two intermediate types of credential: hardened password and soft PKI, and cited a COTS single sign-on product.
- Biometrics were sometimes mentioned for possible use with other types of credential, without clearly stating whether they would be used as adjuncts to protect access to another credential (e.g., private key) or would be used as standalone credentials to be presented to the Gateway. One respondent gave a description of biometric templates as an example of an authenticating credential by use of PAM. Another described a technology and service that uses voice as a biometric for validation of a credential or as an identity credential. And another stated that biometrics are suitable for identity proofing prior to issuance of a credential (as essential for preventing people from registering for multiple identities, i.e., for reducing identity theft), but not for authentication. One respondent described the use of behavioral monitoring (as compared to the user's behavioral profile from past experience) to watch for evidence of fraud and to adjust the amount of information to be supplied for authentication on a particular occasion.
- The same respondent proposed a confidence scoring approach as a way of allowing all types of credential to be incorporated into a composite (see Policy Mapping below).

Policy Mapping

- One respondent described a strategy that would calculate a confidence score by combining credentials that have been given weights. Rules of combining can provide for multiple types of credential to be required and for alternative types to be permitted. If a higher score were required for access to a resource, the user would be asked to provide additional authenticating information. Thus, the approach is technology agnostic as to types of credential (see Credential Mapping, above). (See Outliers, below.) Another respondent described a way of defining authentication requirements as combinations of commonly possessed credentials (driver's license, bank cards, and so on), but did not explain how an internally consistent series of levels would be achieved nor how these requirements would be related to existing levels of assurance.
- A respondent advocated a policy mapping scheme modeled on the Federal Bridge, and incorporating the ACES and ECA programs. It would use a small set of trust levels that are easily understood. Guidance would be provided to agencies for mapping their applications' requirements to these trust levels. A hybrid approach tested at NIH was described.
- A respondent noted that the Liberty architecture offers additional functionality in that the level of authentication required by an application can be specified dynamically at runtime rather than only in offline agreements.
- Another respondent described a runtime authentication engine that would normalize the policies of the various credential providers and would issue its own credential in the form required by the particular application. In this way it would allow credentials from many different sources to be used with many different applications.

Detailed Analysis -- Divergent Responses/Outliers

- One respondent described a product that is a biometric authentication engine, and suggested that with government R&D this model of authentication might have commercial value for authentication of users for access to multiple applications.
- Two others suggested biometrics as authenticating credentials (see Credential Mapping, above).
- One respondent described a strategy for use of scoring, augmented by behavioral monitoring (see Credential Mapping and Policy Mapping, above). But it's not clear how one would provide the weights to represent the relative strengths of different credentials such that as they are aggregated the resulting scores will be meaningful. Integrating the scoring plan with levels of assurance such as those defined for the Federal Bridge would be a major challenge. We would need to know much more about how the scoring plan would be set up, to understand it as a method.
- One respondent described a product that uses Internet spidering technology to build a database of the login requirements for both affiliated and unaffiliated sites. A front end allows users to store their credentials for various sites, and to access their credentials through a two-stage password+PIN procedure, said to be equivalent to a strong password with an expiration timeout. In addition, the respondent proposes that the Gateway offer a two-factor authentication method for applications requiring stronger authentication.
- Another respondent described a system that's designed for business applications where the users are already known. In effect this system puts the identity proofing and credentialing function at the application's organization. The organization can also outsource the identity proofing to the respondent. The system uses a proprietary chip with public key technology to provide a credential for a known user. This eliminates the CRL (and CRL checking) of traditional PKI. This product/service system is suitable for closed, stovepipe applications, but the respondent claims it can be re-purposed for the Gateway. Authentication can be supplemented by online identity proofing against financial databases at the time a user seeks access to an application. Respondent characterizes the approach as going outside of the traditional PKI concepts.

Question 6.5 Compliance with Government Mandates for Protection of Privacy Information

6.5a: Provide 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.

The majority of respondents indicated 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 indicated that they would be willing to specifically meet the requirements of the Privacy Act and other any other requirements that the Federal government specifies. Many of the responses indicated other requirements that they would be willing to comply with, such as the Computer Security Act, Security of Federal Information Resources, Critical Infrastructure Protection, Guide for Developing Security Plans for IT Systems - NIST, and the Government Information Security Reform Act to name a few. However, the respondents imply that they would be willing to comply with Federal privacy requirements or other related terms as a condition of a Government contract. This RFI question really wanted to know the willingness of industry to comply with Federal privacy requirements on a voluntary basis, absent a contractual requirements to do so. As such, it is not clear that respondents clearly understood the question that was being asked.

Convergent Responses:

- Most commercial entities already follow privacy protection practices due to the fact that citizens will often not use services that do not ensure the protection of their private personally identifiable information.
- Several responders suggested that there should be some form of a centralized management function to provide timely and quality service to customers.
- Several of the responses discussed the importance of composing a draft that would outline the privacy policies and practices for the gateway. They suggest that the government work with Computer System Security and Privacy Advisory Board, the International Security Trust & Privacy Alliance, Liberty Alliance and Johns Hopkins University when composing the privacy policy.

Divergent Responses:

- The responses that did not necessarily converge with the majority, but proposed interesting ideas and discussions, were the ones that covered both why they think agencies would follow

the requirements of the Privacy Act and why they think they would not. Some of the implications were that organizations might not want to meet the Privacy Act requirements because they do not want another ‘audit’ or do not want to be burdened with additional rules/regulations, which might create new liabilities, increase the cost of operations and diminish profit. Several respondents also mentioned the fact that personal information is becoming a valuable commercial commodity therefore it would be hard to assume that industry would not exploit personal information for profit. The same respondents also commented that industry would also welcome controls of complying with the Privacy Act and other Federal requirements because they would be necessary to achieve the trust of citizens.

- One other response that was an outlier from the rest stated that they felt the privacy requirements in the RFI were understated and there were other requirements that would need to be met such as HIPPA and COPPA. They also strongly suggest that the users of the gateway not be known by a single unique identifier due to the risk that an individual’s behavior can be traced throughout all entities in the system. They also felt that the importance of the federation to privacy has not been adequately recognized in the RFI. This specific organization believes that Liberty Alliance specifications are the best way of providing the protection under the Privacy Act and associated regulations.

RFI Question 6.9 Response Synthesis

6.9a. Describe how the requesting agency application is authorized to receive the requested user information.

6.9b. Describe where that agency authorization information should be stored.

Convergent Responses:

The majority of the respondents did not respond to this question.

Of those that did respond, there was not a single common identifiable answer or recommendation. In general, respondents presented a combination of three solutions or locations for the storage of agency authorization information:

- central location at the gateway. Reasons for storing the information in a central location on the gateway are that it is a more manageable and secure location.
- maintained individually at the agency or agency application level (slightly more responses than the other two options). Reasons for storing personal information at the individual application agencies include:
 - that it provides scalability, simplicity, and flexibility in designing and organizing the security model;
 - it would be too complex for the gateway to keep current information on the agency users;
 - many agencies may have varying security policies about access to different levels of data and they may classify data in different ways/levels;
 - it would be easier and more viable for each AA to store this information
 - storing the information in a central location would subject this sensitive information to greater risk of attack, unauthorized disclosure, and could create a performance bottleneck for other applications and systems that rely on the authorization information.
- LDAP or LDAP-like directories. Respondents recommending an LDAP-based directory suggest that it could serve as a policy repository or provide the necessary linkage between storing the information locally with each AA, but also possess the capability to make the information accessible via the e-Authentication Gateway.

Divergent Responses/Outliers:

- Store the information in a federated model or a federated system of directories (something like a Liberty Alliance approach?)
- Deploy a SAML-based architecture, which has the advantage that permissions do not need to be stored in a centralized fashion, preferences regarding the dissemination of their private information are managed through agreements at their identity provider (storing information at each ECP and, potentially AA and sharing only the information agreed to in bi-lateral agreements).

Conclusion:

The majority of respondents recommended maintaining personal information at the individual agency applications, with some recommendations for federation and tailored approaches based on agreements among the parties.

Response Synthesis of RFI Question 6.9

6.9c. Identify how a user pre-authorizes release of user-selected private information.

Many of the respondents did not provide an answer to this question.

Convergent Responses:

Of those that responded, the majority answered in one of three ways:

- a form that the user can fill out that will outline the use of their personal information;
- an opt-in/opt-out capability if so desired/needed; and,
- through the use of a trust agreement with the gateway to agree on circumstances under which the user's private information may be shared. The user would have to give their consent to this (similar to opt-in/opt-out). Basically respondents indicated that users should be given choices up front and on an *on-going* manner as to how they can pre-authorize release of selected personal information.

In addition, many respondents recommended that the user have some kind of a manageable profile that users could have the capability to edit if needed.

Divergent Responses/Outliers:

The outlier responses did not present divergent responses, rather, they recommended additional of accomplishing this functionality. One suggested that another approach would be to request access to private information only when a user requests access to an application specifically requiring it. This coincides with pre-authorization of selected personal information when it is desired/needed. One respondent provided a good discussion on providing the user with a questionnaire to indicate what types of organizations their personal information may be disclosed to for these limited purposes. They suggest the questionnaire be filled out at the time the user requests a credential from the DCP. They also point out that personal information provided by users may need to be verified by a trusted third party because without such verification, relying parties may not be willing to rely on this personal information (a cross check of information).

6.9d. Describe situations where the user does not give pre-release authorization, yet agencies are permitted by law to share.

The majority of the respondents did not answer the question.

Convergent Responses:

Out of those that did answer the question, the majority recommended how could be handled:

- Most recommended a notice ("terms & conditions") to the individual advising that their personal information could be shared in certain lawful instances (tell them the instances) without their consent.
- Most also recommended that when this does happen the user needs to be notified at the earliest possible time.

- Out of those that actually gave examples of situations where this might happen, they suggest civil matters, criminal matters, and simply when they captured information from business dealings with the agency (ex. The IRS would have information from a tax return filed by the individual, the State Department would have information from a passport application, and so on).

Divergent Responses/Outliers:

The outliers were those few that stated that under no circumstances could personal information be shared without user's consent. If the user does not give pre-authorization up-front, then this should not happen.