

Pay.gov Frequently Asked Questions: Access Control

This document expresses functionality expected to be available by mid-2003.

Table of Contents

1. What is access control?	2
2. What is a resource?	2
3. What is the role-based access control system that Pay.gov is implementing?2	
4. What are the advantages of a role-based access control system?	3
5. Why not use other, more sophisticated methods, like digital certificates?.....	4
6. If Pay.gov is not using digital certificates, can it still be said that transactions are electronically signed?	4
7. What information will you gather during the authentication process?	5
8. What about authentication as a representative of a business, agency, or other entity?	5
9. What is the ad hoc authentication component?.....	6
10. Does the verification service operate as a credit check?	8
11. As opposed to ad hoc authentication, what is entailed in direct access to the verification engine?	8
12. What is the Pay.gov usernames and password authentication component?8	
13. How does an end-user self-enroll to obtain a username and password?	8
14. How do administrators enroll end-users?.....	8
15. What are the differences between the various roles that Pay.gov offers?....	8
16. Can my agency set password expiration periods?	9
17. What is the agency authentication component?	9
18. What about privacy and security?	9

19. Why is Direct Debit the only collection method that could require access control?	10
20. Will Pay.gov be a partner in the e-authentication gateway?.....	10

1. What is access control?

As used in this document, access control refers to the process of determining whether an end-user should be allowed to perform a specific action with regard to a resource. It typically consists of authentication, or determining who is the end-user, and authorization, or determining what actions the end-user may perform.

2. What is a resource?

A resource is a particular Web page, be it a collections page, a form, a saved form, a bill, or a report, for instance.

3. What is the role-based access control system that Pay.gov is implementing?

Pay.gov uses a role-based access control system. As the name implies, a role-based access control system focuses upon roles. A role is simply a title given to a pre-determined grouping of permissions (allowable actions). Pay.gov will assign roles to end-users and will look to those roles at the time of transaction to determine the actions in which an end-user can engage with regard to a particular resource.

Pay.gov has developed a set of roles (set out in a separate roles-permissions matrix) from which an agency can choose in determining which roles will be available for the resources that are part of the agency's application. If the end-users for two or more resources are to have identical roles, Pay.gov will treat the resources as a "resource cluster" to ensure that they are treated identically. This information will be maintained in a "policy" for that resource, held in a "policy store."

Roles are assigned either by administrators or "on the fly" during the end-user's session. If assigned by a Pay.gov administrator, the end-user must have a Pay.gov username and password. If assigned "on the fly," the end-user can be authenticated in various ways, leading to Pay.gov's application of business rules based upon authentication attributes to determine whether to assign a role. The rules on whether and how a role can be assigned "on the fly" are also maintained as part of the policy.

At the time of transaction, an agency or other Pay.gov service will inform the access control service of the particular resource at issue and the permission that is sought, along with locations to redirect the end-user upon successful and unsuccessful results. Pay.gov will authenticate the end-user according to limitations set out in the policy for that resource maintained in the policy

store, unless the end-user has already been authenticated during the session. Once authenticated, the roles for that end-user will be looked up in the user store, or assigned on the fly if allowed by the agency. Finally, once the end-user's role for that resource is known, it can be determined whether to grant the end-user the sought-after access. The invoking entity will be given a yes or no response as to whether access is allowed, along with authentication attributes of the end-user, which can be used for pre-populating forms or providing finer-grained access by the invoking entity. The end-user will be redirected to a site of the agency's choosing.

Access control performs a function not entirely unlike that which a security guard performs in protecting the entrance to a building. When an unknown person enters the building, the security guard may need to know where the person is going (the resource) and the purpose for the visit (the sought-after permission). According to rules set out in advance (the policy), the security guard will authenticate the person and determine whether the person holds a role that allows access. For instance, a person may hold a role of employee, or that of visitor. Once the person's role is clear, the security guard can make a determination of whether to allow access.

In summary:

- Resource—An access control protected application or other Web page (e.g., form, bill, report), for which a policy exists. Two or more resources for which the same end-users can perform the same roles will be treated as a resource cluster.
- Policy—For a resource or resource cluster, indicates the available roles and the authentication needed to obtain a particular role. Policies are maintained in a policy store.
- Role—A title given to a pre-determined set of permissions. Pay.gov's roles are set out in a roles-permissions matrix document. Roles are associated with end-users in a user store and accessed during authentication or assigned "on the fly," according to rules set out in the policy for that resource.
- Permission—An allowable action concerning a resource.

4. What are the advantages of a role-based access control system?

Use of a role-based system has several advantages. In particular, it reflects the structure of organizations, in which a person's actions are attached to the person's title. It serves as a "translation layer" to permissions, allowing for Pay.gov to add, change, or delete permissions at once, rather than separately for each individual. What authentication components are you offering?

Pay.gov will use several tools in determining the identity of the end-user. These tools will include accepting authentication:

- Through information provide by end-users at the time of transaction (ad hoc authentication); and
- Through usernames and passwords issued by Pay.gov after ad hoc authentication or creation of an end-user by an administrator (Pay.gov credentials authentication); and

- Through agencies (agency authentication).

We want to provide authentication components that agencies and end-users are willing to use and that keep costs down for the Government, while providing sufficient proof of authentication for the Government's needs. Because the sufficiency of proof may vary depending on the transaction, it is necessary for us to offer more than one means of authentication.

5. Why not use other, more sophisticated methods, like digital certificates?

Some may question why we are not planning to more extensively use digital certificates or other sophisticated authentication credentials, instead of relying upon usernames and passwords. Digital certificates and other advanced authentication credentials hold promise for the secure authentication of end-users; however, various real or perceived issues with installation, portability, interoperability, privacy, ease of use and cost have kept these technologies from gaining wide acceptance with the public. Furthermore, even these technologies will not always eliminate an end-user's fraudulent attempts to repudiate a transaction. In reality, no form of authentication—electronic or otherwise—is foolproof. Handwritten signatures can be forged, checks can be altered, and identification cards can be counterfeited. These factors and others have caused us to view digital certificates or other advanced authentication credentials not as a universal solution for authentication, but as one tool in a authentication toolbox that is appropriate for some transactions but perhaps less so for others. When we see the need for digital certificates—as expressed to us by our Federal agency customers—then we look to make greater use of them.

6. If Pay.gov is not using digital certificates, can it still be said that transactions are electronically signed?

The authentication services offered by Pay.gov will be used for the creation of electronic signatures that take the place of handwritten signatures. The Electronic Signatures in Global and National Commerce Act recognizes and gives broad scope to the concept of an electronic signature. The Act states: "The term 'electronic signature' means an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record." The GPEA includes a similar definition, especially as interpreted by OMB guidance published to implement that Act. Furthermore, both Acts require that an electronic record or signature is not to be denied effect as a writing or signature solely because the writing or signature are in electronic form. The providing of authentication evidence helps show the necessary intent to sign and, presuming any authorization requirements also are met, can constitute a "signed" debit authorization for various rules and regulations that require that direct debit (debit ACH) authorizations be "signed or similarly authenticated."

Digital certificates are needed for digital signatures, which are a sophisticated subset of electronic signatures. It is possible to have an electronic signature without use of a digital certificate, though non-repudiation of the transaction is more difficult if this is the case.

7. What information will you gather during the authentication process?

With the exception of agency authentication, Pay.gov divides information obtained during the authentication process into three categories:

- General identity (authentication) attributes are data elements that will identify an end-user in general terms, such as the end-user’s name or address. These attributes will be made available across agency applications.
- Resource-specific (authorization) attributes are data elements that identify an end-user with regard to a particular agency application, such as an agency-assigned identifier or a role. These will be made available only for particular agency applications.
- Assurance Level attribute is a data element that summarizes the strength of the authentication process used to authenticate a particular end-user.

For Pay.gov credentials, Pay.gov will place these authentication attributes into the user store. Because general identity attributes may by definition be used across agency applications, we reserve the right to impose baseline standards of the identity proofing used by administrator to justify the issuance of Pay.gov usernames and passwords.

Figure 1. Authentication Attributes

General Identity Attributes	Assurance Level Attribute	Resource-Specific Attributes
Name: John Doe SSN: 479-XX-XXX Address: 1702 Madeup Lane, Arlington VA 22201 Personal phone: (703)XXX-XXXX Personal fin. inst. account:123456789 0987654321	Administrator-entered	Role: Agent Agency-assigned entity identifier(s): 76441, 74432 Agency-assigned individual identifier: 776433

8. What about authentication as a representative of a business, agency, or other entity?

There often is a need to authenticate an end-user both as an individual and as a representative of an entity, which is often the case when an end-user is acting on behalf of a business. In determining whether a person is sufficiently authenticated, some agencies may rely entirely upon evidence of an end-user’s individual identity, especially if the risk of the transaction is low. In more sensitive transactions, the agency may require proof of the end-user’s identity as an individual and proof of the end-user’s identity as a representative of the business, which can be

done by verifying a confidential entity (business) identifier issued by the agency. In some instances, the agency will rely upon the entity identifier entirely, ignoring any need to authenticate the individual. This last point—authenticating an end-user as a representative without authenticating the end-user as an individual—is an important one because we recognize that an end-user should be able to communicate with Pay.gov without always requiring proof of the end-user’s identity.

Pay.gov captures some employer information as part of the general identity attributes. However, other business information is non-standard and so will be captured as resource-specific information. This information can include unique agency identifiers that are used to identify a person not only as an individual, but also as a representative of an entity. Up to a half-dozen such identifiers will be captured in the end-user’s profile. This information will be passed to the application by access control when the end-user attempts to access a resource; this information can then be used by the application for pre-population or other purposes.

Pay.gov currently has no method of authenticating representative end-users “on the fly” at the time of transaction, although it is investigating possibilities. Identifiers relating to a representative end-user generally will be captured by administrators when creating or editing an end-user’s profile. The one exception would be self-enrollment in Pay.gov’s billing service, if allowed by an agency. In this instance, the end-user could provide one or more confidential identifiers necessary to tie the end-user to particular bills. Again, this information will be passed to the application by access control when the end-user attempts to access a bill; the billing service will take the identifier(s) to determine which bill(s) to show to the end-user.

9. What is the ad hoc authentication component?

One way that Pay.gov will authenticate end-users is by verifying items of shared knowledge that end-users provide, a process referred to as “ad hoc authentication.” Pay.gov will use a verification service to accomplish this verification. The information that an end-user will be asked to provide will consist of the following:

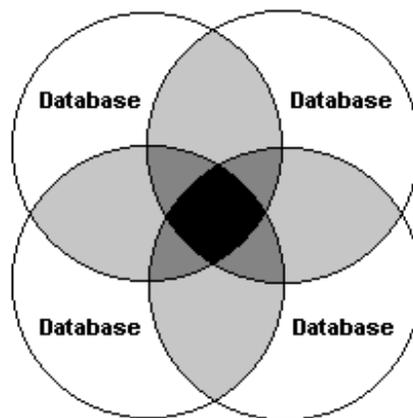
- Name
- Address
- Home telephone number
- Social Security number (SSN)
- Driver’s license number
- Date of birth (DOB)
- Personal financial institution account
- Amount of a recent payment from the Treasury

The end-user will be required to provide their Social Security number only when so allowed under the Privacy Act.

The information will be passed to Pay.gov’s verification service (described below) for confirmation. The agency will determine the extent to which the person needs to be authenticated, on an overall basis and also based on individual data elements. For instance, an agency that is shipping goods is likely to be much more concerned with verification of the end-user’s address than an agency that is simply receiving a fee from an end-user.

The verification service will compare the information provided it to records held in multiple, independently sourced databases. These databases will include our own databases and those of third parties, which primarily will be commercial in nature. By checking multiple databases—which often will have overlapping scope of coverage—the verification service will facilitate the online authentication process and will reduce the possibility of inaccurate results.

Figure 2. Increasing the Verification Service’s Accuracy



The verification service will account for the various ways in which information is stored, otherwise known as “fuzzy matching.” For instance, if a name to be verified is “Robert,” the verification service also will check for “Robby,” “Rob,” “Bobby,” and “Bob.”

The verification service only will query databases to determine the accuracy of information voluntarily provided to Pay.gov by end-users. The commercial databases will not be allowed to retain information passed to those databases from us, or vice versa.

At the completion of the verification process, the verification service will reply back and the access control service can determine whether authentication was successful.

10. Does the verification service operate as a credit check?

No. The verification service will not perform credit checks. Pay.gov will not reject an end-user's authentication request because of poor credit history. Ironically, such an end-user may be more likely to succeed in authentication, because poor credit histories are reported in several databases and so more authentication information will exist as a result. However, if an end-user lists a known closed financial institution account, this may hurt the end-user's ability to be authenticated.

11. As opposed to ad hoc authentication, what is entailed in direct access to the verification engine?

Agencies that want the most powerful access into the verification service can host the pages used to obtain information from the end-user and then pass the elements directly to the verification service using a script-based, XML interface. Agencies should be aware that the verification service interface and methods of calculation will change from time to time. However, without using the pages hosted by Pay.gov, agencies will have to accommodate such changes. These agencies will use a more sophisticated interface than those agencies that simply allow Pay.gov to host the pages used to gather information from end-users. If the pages are hosted by Pay.gov, agencies will use a simplified interface that insulates the agencies from changes to the verification service itself.

12. What is the Pay.gov usernames and password authentication component?

Another of Pay.gov's authentication services will involve the issuance of usernames and passwords through Pay.gov. Stored with an end-user's username and password will be the authentication attributes described above. These attributes will be passed to the application at the time of transaction for pre-population purposes and for fine-grained access control purposes.

13. How does an end-user self-enroll to obtain a username and password?

An end-user may obtain a username and password upon completion of a Web application, which will ask for the same pieces of information as ad hoc authentication.

14. How do administrators enroll end-users?

Pay.gov and agency administrators may enroll end-users through a file or one at a time through a Web interface. A Pay.gov administrator generally will require completion of a paper form before enrolling an end-user.

15. What are the differences between the various roles that Pay.gov offers?

[Note: The roles used by Pay.gov are being revised for an upcoming release; this discussion reflects the expected changes, rather than current functionality.]

Pay.gov offers a variety of roles in transactional, reporting, administrator, and operator responsibilities. An administrator must assign all but the transactional roles. The availability of

and authentication needed for transactional roles is determined by the agency through the agency configuration template.

There are four transactional roles. These roles are available for forms, bills, and collections transactions performed by individual and business end-users. The roles include “Anonymous Guest,” “One-time Customer,” and “Recurring Customer-Limited” and “Recurring Customer-Full”. The roles are incrementally more powerful; an Anonymous Guest can fill out and print but not electronically submit forms; a One-time Customer can submit but cannot save forms; a Recurring Customer-Limited can save and submit forms and bills; a Recurring Customer-Full can save, submit, and route forms. It is up to the agency to determine which roles will be available and what authentication is necessary for an end-user to hold a role. It is possible for roles to be assigned “on the fly” based upon a person’s authentication attributes, so that an administrator need not have previously assigned a role to the end-user for the transaction to occur.

There are two reporting roles, those of “Summary Analyst” and “Detail Analyst.” As the names imply, the distinction between the two is that the Detail Analyst can view reporting information on individual transactions, whereas the Summary Analyst is limited to individual transactions. More importantly, the extent to which either type of analyst can view transactions is limited by the cash flows that are associated with the analyst’s username and profile, as controlled by an administrator.

An agency operator has the ability to administratively cancel or authorize certain collections.

Details of these roles are maintained in a separate roles-permission matrix.

16. Can my agency set password expiration periods?

No. A Pay.gov password does not have to be changed by the end-user. It will expire after two years of non-use. However, an agency can set the expiration period on roles for its resources, so that if an end-user does not log in to access a resource within that timeframe, the end-user will lose access privileges to that resource.

17. What is the agency authentication component?

Pay.gov will accept authentication information pushed to Pay.gov by the agency. Under this approach, the agency will authenticate an end-user on its site, then inform Pay.gov of the end-user’s identity. Pay.gov will use a standard script for such access, which will allow for some general identity attributes and resource-specific attributes that further identify the end-user as an individual or as a representative of an entity such as a business. This script will connect with agencies using much of the same architecture and security used by the scripts that allow an agency to invoke the collections service on its site.

18. What about privacy and security?

Pay.gov will follow a policy of confidentiality with regard to end-user information contained in its records. Furthermore, Pay.gov will follow a policy of openness about developments, practices

and policies with respect to personal data. Pay.gov will keep a page of such notices prominently linked to from pages on Pay.gov.

In addition, Pay.gov will offer a “Privacy and Security Control Panel” for Government-wide authentication credentials, which will provide end-users with the ability to:

- Opt-out of the authentication service at any time;
- Access, update, and control the disclosure of personal data associated with their username and password;
- View notices relating to privacy, security, and liabilities for financial transactions.

Financial agents and contractors are barred from using any information gathered for Pay.gov for any commercial purposes.

Finally, Pay.gov will obtain a review of Pay.gov’s authentication services.

19. Why is Direct Debit the only collection method that could require access control?

Financial institutions may accept direct debits solely based upon routing and account numbers; unlike many credit card transactions, there is no requirement to match the numbers to the name on the account. In addition, there is no approval passed back by the financial institution as to whether the transaction was successful, unlike credit cards; nothing is known until the item is actually collected or a return of some type is received.

20. Will Pay.gov be a partner in the e-authentication gateway?

The e-authentication gateway is managed by the General Services Administration and seeks to provide means, through various vendors and agencies, by which agencies can authenticate users. Pay.gov will offer its services to the gateway and will use services offered by it as our Federal agency customers request.