

- A State or local law enforcement official accesses a law enforcement database containing information about the criminal records of individuals. Unauthorized access would violate the legal privacy rights of individuals or compromise investigations.

- A VA pharmacist dispenses a controlled drug. He/She would need full assurance that a qualified doctor had signed the prescription. In this case, the pharmacist's actions on the transaction carries criminal liability that the prescription was the correct drug(s), in the correct quantity, and that the prescription was validated before filling the prescription.

2.4. Additional Considerations

Each step of the authentication process—from identity proofing, to issuance of a credential, to management and use of the credential in a well-managed secure application, and ultimately to record keeping and auditing—influences whether the process conforms to the desired assurance level. The level of assurance achieved by each step of the process needs to be considered. The step that provides the lowest level of assurance may often determine the assurance level for the entire authentication process. Ideally each step in the authentication process should be consistent in its strength and robustness. A strong identity proofing process, combined with a strong credential and a robust management practice (including a strong archive and audit process) will contribute to the highest level assurance of identity. However, the best authentication process needs to be supported by well-engineered and tested user and agency software applications.

In making the risk assessment, the business process owner must consider all the direct and indirect consequences as presented in the definitions of the levels. Since each assurance level uses the terms “minimal”, “minor”, “significant”, or “considerable”, the business process owner will need to consider the terms in the context of the parties likely to be affected and their typical views. While it is realized that these terms are subjective, it is expected that these will be solidified through implementation and practice. For example, risk assessments have already been conducted on the E-Government Initiatives to determine their appropriate assurance levels.

As stated in OMB's GPEA guidance, properly implemented technologies can offer degrees of confidence in authenticating identity that are greater than a handwritten signature can offer. However, electronic transactions may in some circumstances affect the risk of criminal and civil violations, increase the harms associated with such violations, and complicate redressing such violations. Legal and law enforcement issues are discussed in the Department of Justice's Guide for Federal Agencies on Implementing Electronic Processes (found at <http://www.cybercrime.gov/e-commerce.html#GFA>, November 2000). Agencies should consider these issues in assigning transactions to particular assurance levels.

Violations of the law can present significant policy issues for an agency. The risk assessment process should consider the

potential effects of illegal activities or other process failures in light of the agency's enforcement priorities, the agency's programmatic interests, and such broader public interests as national security, the environment, and the proper functioning of markets. Some of these harms are specifically described in each level (such as financial loss or release of personal information); others will depend on a particular agency's programmatic interests.

The risk analysis reflects this issue by referring to risks of criminal or civil violations and harm to agency programs or the public interest. In assessing this risk and designing a process, agencies should take into account not just the effects of a single violation or other act, but the possibility of a pattern of actions that might affect agency programs. For instance, if sensitive information could be obtained from an agency website, the agency should consider the effects of a possible pattern of such activity, not just a single action, in assessing risk levels. (Note that unauthorized access to an agency website is itself a criminal offense, see, e.g., 18 U.S.C. 1029, 1030. Agencies should consider the effects and risks associated with such unauthorized access, rather than focusing on the unauthorized access itself, in assessing such risks.)

3. Determining Assurance for Credential Service Providers

Credential Service Providers (CSPs) are organizations, both governmental and non-governmental, that issue and in some cases may maintain electronic credentials. CSPs can handle several of the steps in the e-authentication process. Because the CSP's issuance and maintenance policy influences the trustworthiness of an e-authentication process, CSPs will also need to be assessed to determine the e-authentication level to which their credentials pertain. For example, if a CSP follows all process/technology requirements for authentication level 3, a user may use a credential provided by the CSP to authenticate himself for a transaction requiring authentication levels 1, 2, or 3. Additional information on CSPs will be included in both the E-Authentication technical guidance and in separate guidance issued by the E-Authentication E-Government Initiative.

4. Implementing an Authentication Process

4.1. Overview of the E-Authentication Process

When determining e-authentication needs, agencies must consider the entire e-authentication process. An agency cannot simply determine the level of credential that will be required to validate a user's identity without also determining how that credential will be processed by the agency business applications. They must determine the requirements for each step in the e-authentication/authorization process. This process includes the following steps:

- Initial enrollment.
- Repeat visits.
- Verification of identity.
- Transaction management.
- Long term records management.
- Periodic tests of the system.
- Suspension, revocation, reissue.

• Audit.

Each of these steps will be explained in more detail in the e-authentication technical guidance. Responsibility for these steps lies with the individual business process owners or designated agency or cross agency authority.

4.2. Use of Anonymous Credentials

Anonymous credentials may be appropriate when it is not necessary that authentication be associated with a known personal identity (as opposed to identity authentication). To protect privacy, it is important to balance the need to know who is communicating with Government with a citizen's right to privacy. This includes ensuring that information is used only in the manner in which individuals have been assured it will be used. In some cases, it may be desirable to preserve the anonymity of individuals and it may be sufficient for the purposes of an application to authenticate that—

- The user is a member of a group; and/or
- The user is the same individual who supplied or created information in the first place; and/or
- A particular user is entitled to use a particular pseudonym.

These anonymous credentials will have limited application. In some cases, individuals would have an anonymous as well as a non-anonymous credential. Anonymous credentials can be used up until level 3.

4.3. Information Sharing and the Privacy Act

When developing authentication processes, agencies must consider the requirements for managing security in the collection and storage of information associated with the process of validating a user's identity. As required by the E-Government Act of 2002 (Public Law 107-347), section 208, 44 U.S.C. § 3604, agencies are required to conduct privacy impact assessments for electronic information systems and collections, which includes when authentication technology is newly applied to an electronic information system.

The following information is captured in most e-authentication processes:

- Information regarding the individuals/businesses/governments using the E-Gov service.

- Electronic user credentials (i.e., some combination of public key certificates, user identifiers, passwords, and Personal Identification Numbers).

- Transaction information associated with user authentication, including credential validation method.

- Audit Log/Security information.

Some of this information includes personal information as defined by the Privacy Act and, systems that use the information are considered systems of records that must meet all requirements of the Privacy Act and the E-Government Act.

Data collected and stored during the authentication process should only be accessible routinely to systems administrators and to auditors. As required by the Privacy Act, access to the system of