

Dated: July 8, 2003.

G. Martin Wagner,

Associate Administrator for Governmentwide Policy.

Draft E—Authentication Policy for Federal Agencies

Section 1: Introduction

Section 2: Assurance Levels

Section 3: Determining Assurance for Credential Service Providers

Section 4: Implementing an Authentication Process

Section 5: Effective Dates of Guidance

1. Introduction

1.1. Summary

- This guidance should be applied to all Federal electronic transactions requiring authentication, except those that are national security systems as defined in 44 U.S.C. 3542(b)(2).

- This guidance does *not* stipulate which technology solutions should be implemented for each assurance level. The Department of Commerce's National Institute for Standards and Technology (NIST) is developing complementary e-authentication technical guidance that will be used by agencies to determine appropriate technology solutions, based on the process described in this guidance.

- Agencies are required to review existing and categorize new electronic transactions to ensure that these transactions comply with this guidance.

- As detailed in Section 9c of OMB's GPEA guidance, agencies should continue to minimize the likelihood of denial or repudiation of the information individuals transmit electronically. As an element of assessing the risks that are relevant to the required assurance level, agencies must consider how they plan to minimize the likelihood of repudiation by ensuring the user's approval of the information transmitted in electronic transactions. General guidance on minimizing the likelihood of repudiation is included in Section 8c of the OMB Procedures and Guidance on Implementing GPEA.

- This guidance does not directly apply to authorization. Authentication focuses on establishing a person's identity, based on the reliability of the credential he or she offers; while authorization focuses on what actions that identity, at that level of assurance, is permitted to do. Decisions concerning authorization are and should remain the purview of the electronic business process owner.

- Authentication is an inherent part of an electronic signature; however this guidance does not cover "intent to sign," or when an agency uses authentication credentials as an electronic signature. For more information on electronic signatures, please consult OMB's guidance on implementing GPEA and the Electronic Signatures in Global and National Commerce Act (found at: <http://www.whitehouse.gov/omb/memoranda/m00-15.html>, September 25, 2000).

- Agencies should implement an e-authentication process using the following steps, described in Section 2.2: (1) Conduct

a risk assessment as explained in Part II of the GPEA guidance and Section 2 of this guidance, (2) match identified risks with assurance levels, and (3) determine implementation technology based on the e-authentication technical guidance.

- Each step of the authentication process—from identity proofing, to issuance of a credential, to technical and administrative management and use of the credential by an application, and ultimately to record keeping and auditing—influences whether the process conforms to the desired assurance level. There are many layers of risk related to authentication. This guidance document is intended to assist agencies in identifying and analyzing risks associated specifically with the improper authentication of users of electronic transactions. These risks are highly dependent on the type of application and transactions offered.

- This document does not address risks that are associated with the improper management of authentication controls or processes, or risks to the underlying authentication technical architecture or infrastructure. This document does not confer, and may not be used to support, any right on behalf of any person or entity against the United States or its agencies or officials.

- This guidance does not refer to the authentication of systems or between services (for example, security socket layer (SSL) authentication). Instead, it is focusing on the attribute or identity authentication of individuals who are authenticated for Government services online.

1.2. Overview

This document provides agencies with guidance on electronic identity and attribute authentication (or e-authentication). E-authentication is the process of establishing confidence in both identities and attributes after being electronically presented to an information system. Individual authentication is the process of establishing an understood level of confidence that an identifier refers to a specific individual. Attribute authentication is the process of establishing an understood level of confidence that an attribute applies to a specific individual. The process of e-authenticating an individual may involve establishing the individual's unique identity (identity authentication) or establishing that the individual is a member of a group (such as a military veteran or U.S. citizen) (attribute authentication). For a complete list of definitions, refer to the Report of the National Research Council "Who Goes There? Authentication Through the Lens of Privacy" (found at: <http://www.nap.edu/books/0309088968/html/>, March 31, 2003).

E-authentication is the first step in the related process of deciding what an individual ought to be allowed to do, called "authorization." Authentication focuses on establishing a person's identity, based on the reliability of the credential he or she offers; while authorization focuses on what actions that identity is permitted to do.

Agencies providing the e-government services need to determine how certain they need to be in the identity of an individual and identify the risks inherent in a particular

transaction. This guidance will provide the framework for the identified risks to be mapped to the desired assurance level that the authentication technology selected must satisfy.

As described in OMB Circular A-130, Management of Federal Information Resources, agencies must prepare and update a strategy that identifies and mitigates risks associated with each information system; Section 5 of the GPEA guidance detailed the risk factors agencies should consider in planning and implementing electronic transactions. This new e-authentication guidance expands on Section 5 by—

- Instructing agencies how to implement an e-authentication process by outlining a process for assessing risk, and determining the requisite level of identity assurance; and
- Describing four discrete (and increasing) levels of identity assurance.

2. Assurance Levels

2.1. Description of Assurance Levels

For the purposes of e-government transactions, this guidance describes four assurance levels for authentication. In this context, assurance is defined as how much confidence the relying party has that the electronic identity credential presented is done so by the person whose identity is asserted by the credential. These levels are each appropriate for different classes of electronic transactions. In general, informal or lower value transactions will require less stringent assurance levels. Higher value or legally significant transactions will require more stringent assurance levels.

2.2. How To Determine an Assurance Level

Step 1: Agencies should conduct a systematic risk assessment of the transaction. The risk assessment will determine the required assurance level and will measure the relative severity of the potential harm to the agency or user of the e-government application and other transaction participants in the event of an improperly validated or unauthorized authentication. Each of the 4 levels described in Section 2.4 contains a profile of consequential risks. The more severe the likely consequences, the more confidence required in the asserted electronic identity in order to engage in a transaction, and, therefore, the higher the assurance level required. The definition of each assurance level is directly correlated to the degree of confidence or certainty that the agency must have in the identity of the user. Assurance levels are the vital link between the risk assessments of applications and the selection of authentication solutions.

Agencies should consider a wide range of possible scenarios in seeking to determine what risks are associated with their business process. It is better to be over inclusive than under inclusive in conducting this analysis. Risk analysis is to some extent a creative process, in which agencies must consider harms that might result from, among other causes, technical failures, malignant third parties, public misunderstandings, and human error.

Step 2: Match identified risks with assurance levels. The results of the risk assessment should be summarized, and then