United States
Department of Agriculture

Office of
the Chief
Information
Officer

DR 3610-001

USDA eAuthentication Service

USDA eAuthentication Service

TABLE OF CONTENTS

U.S. Department of Agriculture
Washington, D.C.

DEPARTMENTAL REGULATION	**NUMBER:** 3610-001
SUBJECT: USDA eAuthentication Service	**DATE:** November 4, 2004
	OPI: Office of the Chief Information Officer

1 PURPOSE

The USDA eAuthentication Service is a strategic component of USDA's eGovernment vision and USDA's Enterprise Architecture to provide common authentication and authorization services for Web-based applications. This Departmental Regulation documents USDA's eAuthentication policy, framework, roles and responsibilities. Policies in this Departmental Regulation are defined around USDA's enterprise architecture and investment strategies.

2 POLICY

The USDA eAuthentication Service provides authentication and authorization services for USDA Web-based applications. Authentication confirms a person's identity, based on the reliability of his or her credential; authorization identifies the person's user permissions.

USDA agencies will use the USDA eAuthentication Service to implement authentication and authorization capabilities for all Web-based applications. This policy applies only to web-based applications. It does not apply to client/server, mainframe, desktop, network or other legacy application architectures.

3 USDA eAUTHENTICATION SERVICE

The USDA eAuthentication Service supports the following concepts: Credential Assurance Levels; Authentication Risk Assessment; Credential Management; Site Protection; Records Management; Privacy Protection; Training; and Waivers.

a Credential Assurance Levels:

Four identity authentication assurance levels, as defined by OMB and NIST, shall be used for USDA electronic government services. These are:

(1) Level 1 – Single-factor, login and password. User is not identity-proofed and there is no assurance that the user is who he/she claims to be.
(2) Level 2 – Single-factor, login and password. User must be identity-proofed through the presentation of identifying materials or information. Identity-proofing may occur either through approved "in-person" or "on-line" methods that are approved by the Office of the Chief Information Officer (OCIO).
(3) Level 3 - Multi-factor Public Key Infrastructure (PKI) soft or hard tokens. User must be identity-proofed through the presentation of identifying materials or information. Identity-proofing may occur only through approved "in-person" methods approved by the OCIO.
(4) Level 4 - Multi-factor PKI hard tokens. User must be identity-proofed through the presentation of identifying materials or information. Identity-proofing may occur only through approved "in-person" methods approved by the OCIO.

b Authentication Risk Assessment:

USDA agencies are responsible for determining the required level of assurance for authentication for each business transaction. Authentication risks with potentially higher consequences require higher levels of assurance. This determination is accomplished through an authentication risk assessment for the system or transaction. Agencies shall conduct this risk assessment through:

(1) The USDA Integrated Reporting Tool to determine risks and tie the outcomes to an authentication level, and/or
(2) A risk-mitigation process to determine whether mitigating controls (management, operational or technical) can offset risks and thus lower the authentication assurance level,
(3) Completing a system Certification and Accreditation (C&A), as appropriate.

Within the process defined above, final decisions on the appropriate level of assurance to be used for a business transaction are delegated as follows:

- Agency specific applications - the required authentication assurance level will be the sole decision of the Agency that owns the business process.

- Department-wide or multi-agency applications – the required assurance level will be a joint decision between the agency that owns the business process and the USDA Office of the Chief Information Officer (OCIO.)

c Credential Management:

The USDA eAuthentication Service will adhere to credential management processes that have been assessed at a particular Assurance Level as described in the Office and Management and Budget (OMB) and the National Institute of Standards and Technology (NIST) guidance. Accordingly, for all USDA Web-based applications, users will utilize the credentials provided and/or approved by the USDA eAuthentication Service. These credentials include:

(1) Levels 1 & 2 UserIDs and passwords for employees, customers and affiliated users.
(2) Levels 3 & 4 PKI credentials for employees issued by NFC.
(3) Levels 3 & 4 PKI credentials for customers and affiliated users issued by credential service providers that are approved by the General Services Administration and the OCIO.

Management of credentials will include all "end-to-end" activities for the credential including registration, issuance, use, modification, and revocation. The USDA eAuthentication Service is responsible for establishing procedures to ensure continued compliance with the OMB and NIST guidance. Additionally, USDA agencies will be responsible for implementing the procedures to ensure currency and accuracy of user information.

The E-Authentication Presidential Initiative has adopted a Federated Architecture for authentication. This architecture will allow for trusted credentials from trusted Credential Services from other Federal Agencies and external Industry Credential Services to be used at any participating application. USDA's eAuthentication Service will be an important part of the Federal government's architecture for authentication. Once integrated, USDA credentials will be valid at integrated agency applications across the government. Conversely, external credentials which have been approved by the General Services Administration (GSA) may be used to access USDA applications.

Integration with the Federated Architecture will be handled centrally through USDA's eAuthentication service. Agencies shall not perform any integration with the Federated Architecture, but should integrate their applications with eAuthentication.

d Site Protection:

As stated above, authentication is the process for confirming a person's identity, while authorization is the process for identifying the person's user permissions. The USDA eAuthentication Service addresses coarse-grained authorization services based on user attributes and roles stored in the USDA eAuthentication Service (e.g., the user is authorized to access the application if "agency = FNS"). Fine-grained authorization, usually business-specific information, will need to be addressed by the agency application (e.g., the user is authorized to access the application if "loan role=FSA loan approver").

Accordingly, USDA agencies will:

(1) Integrate web-based applications requiring authentication with the USDA eAuthentication Service to provide user authentication functionality,
(2) Leverage the USDA eAuthentication Service to provide coarse-grained authorization when appropriate attributes/roles exist,
(3) Create fine-grained authorization controls in the agency application when required by the business function.

Roles implemented as part of bullet (2) above will be documented and implemented according to approved USDA eAuthentication Service procedures. The procedures include data definitions, administration of the role and auditing of the role.

e Records Management:

The USDA eAuthentication Service is responsible for maintaining a record of the facts of registration and logons of users for a period beyond expiration or revocation of a user's credential. This time period varies with the assurance level of the credential and is as follows:

(1) Level 1 credentials – no minimum retention period,
(2) Levels 2 and 3 credentials – seven years and six months, and
(3) Level 4 – ten years and six months.

Agencies are responsible for maintaining a record of the application access and transactions conducted (data entered, modified or deleted) through their applications. Agency applications will use the USDA eAuthentication Service's "eAuth Internal ID" to identify the user in the application's audit trail.

Agency applications are also responsible for ensuring that the user explicitly confirms his/her intent to commit a transaction. This may be

accomplished by directing the user to a "confirm and submit" type function that is time-stamped and recorded by the application.

f Privacy Protection:

The USDA eAuthentication Service will use credential information only in the manner in which individuals have been notified it will be used (as stated in the system's Privacy Statement). This information includes user credentials, personal information regarding the user, logon information and audit log information.

USDA agencies are responsible for complying with the Privacy Act with respect to transaction information associated with the user.

g Training:

The USDA eAuthentication Service will be responsible for the development of USDA eAuthentication Service specific training (and in some situations, certification) curriculums for agency personnel interfacing with the service, including program managers, application developers, registration authorities and others. USDA agencies are responsible to ensure that the training is delivered and completed as intended.

h Waivers:

This regulation directs all applications requiring authentication to integrate with USDA's eAuthentication Service. However, in some cases Agencies may request a waiver for ephemeral or low impact internal applications. In order to be considered for a waiver, an application must meet all of the following requirements:

(1) Results of a Risk Assessment must show that the application requires only Level 1 authentication assurance:
(2) The application is accessible only through the USDA Intranet: and
(3) The application supports internal users only.

In addition, the application should fall into one or more of the following categories:

- A very small user population accesses the system.
- The application has a short life span (e.g., a pilot or demonstration system).
- The application has a pre-existing authentication method (a waiver granted for a pre-existing authentication method will only be valid

for a short time, the application will be expected to create and implement an eAuthentication integration plan.)

If an application meets these requirements, the Agency may submit a waiver request form to OCIO. The request will be reviewed for its validity and adherence to the requirements of this Regulation. In instances where a waiver is granted, it will have an expiration date. Extensions to the waiver must repeat the process.

4 AUTHORITIES AND REFERENCES

a USDA Strategic Plan and USDA eGovernment Strategic Plan;

b H.R. 2458, *E-Government Act of 2002*, December 17, 2002;

c Public Law 99-508, *Electronic Communications Privacy Act of 1986*, October 21, 1986;

d Public Law 100-235, H.R. 145, *Computer Security Act of 1987*, January 8, 1988;

e Public Law 105-277, Title XVII, *Government Paperwork Elimination Act (GPEA)*, October 21 1998;

f Public Law 106-222, *Freedom to E-File Act*, June 20, 2000 Public Law 106-229,

g *Electronic Signatures in Global & National Commerce Act*, June 30, 2000;

h H.R. 3802, *Electronic Freedom of Information Act Amendments of 1996*, January 3, 1996;

i U.S.C. § 552a, *The Privacy Act of 1974;*

j 29 U.S.C. § 794(d), *Section 508 of the Rehabilitation Act of 1973*, August 7, 1998;

k Office of Management and Budget (OMB) Circular A-123, *Management Accountability and Control*, June 21, 1995;

l Office of Management and Budget (OMB) Circular A-127, *Financial Management Systems*, July 23, 1993;

m Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, November 28, 2000;

n Office of Management and Budget (OMB) Memo 00-10, *Implementation of the Government Paperwork Elimination Act*, April 25, 2000;

o National Institute of Standards and Technology (NIST) Special Publication 800-9, *Good Security Practices for Electronic Commerce, Including Electronic Data Interchange*, December 1993;

p National Institute of Standards and Technology (NIST) Special Publication 800-14, *Guide for Developing Security Plans for Information Technology Systems*, September 1996;

q National Institute of Standards and Technology (NIST) Special Publication 800-25, *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*, October 2000;

r National Institute of Standards and Technology (NIST) Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems,* August 2001;

s Federal Information Processing Standards (FIPS) 102, *Guidelines for Computer Security Certification and Accreditation,* September 1983;

t National Security Telecommunications and Information Systems Security Committee (NSTISSI) 4009, *National Information Systems Security (INFOSEC) Glossary,* September 2000;

u NIST Federal Information Processing Standards Publication 199, "*Standards for Security Categorization of Federal Information and Information Systems*" promulgated under the E-Government Act of 2002;

v National Institute of Standards and Technology (NIST) Special Publication 800-63, *Electronic Authentication Guideline,* June, 2004;

w Office of Management and Budget (OMB) Memo 04-04, *E-Authentication Guidance for Federal Agencies,* December 16, 2003; and

x *Homeland Security Presidential Directive HSPD-12,* August 27, 2004.

5 ROLES AND RESPONSIBILITIES

a **Chief Information Officer (CIO), Deputy CIO, and Associate CIOs** will provide leadership for the implementation, enhancement, and maintenance of the eAuthentication Service, including:

(1) The management and operations of the USDA eAuthentication Service.

(2) The review of agency domain name requests for applications that are best served using eAuthentication services by:

(a) The coordination of the agency domain name requestor and the OCIO evaluation of the agency application; and
(b) The approval of domain names only after eAuthentication evaluation has been completed.

(3) The creation and facilitation of a project-level Change Control Review Board to advise OCIO on USDA eAuthentication Service functional and technical issues.

b **Agency and Staff Office Executives, CIOs, DAMs and Agency Contracting Officials.** USDA agencies are responsible for supporting USDA's eAuthentication Initiative for Department and Government-wide authentication and authorization. Agencies are responsible for implementing procedures necessary to ensure compliance with this Departmental Regulation.

c **USDA eAuthentication Service Change Control Review Board**

The eAuthentication Service Change Control Review Board is responsible for advising OCIO on eAuthentication functional and technical issues. It is constituted of various USDA stakeholders that have decision authority from their respective agencies.

End