Department of the Army
Circular 25–06–1

Information Management:

Digital Signature

Headquarters
Department of the Army
Washington, DC
25 July 2006

UNCLASSIFIED

SUMMARY of CHANGE

DA CIR 25-06-1
Digital Signature

This new circular dated 25 July 2006--

- Establishes new policy for using digital signatures.

- Identifies tools to implement digital signature.

Headquarters
Department of the Army
Washington, DC
25 July 2006

Department of the Army Circular 25–06–1

Expires 25 July 2008

Information Management:

Digital Signature

By Order of the Secretary of the Army:

PETER J. SCHOOMAKER
General, United States Army
Chief of Staff

Official:

JOYCE E. MORROW
Administrative Assistant to the
Secretary of the Army

History. This is a new Department of the Army Circular.

Summary. This circular reviews the government initiatives establishing electronic signature policy and requirements, identifies available tools to aid the implementation of digital signature technology, and provides procedures and guidance to advance the implementation of digital signatures.

Applicability. This circular applies to the Active Army, the Army National Guard/Army National Guard of the United States, and the United States Army Reserve. This circular applies to Information Technology or Information Management Programs at all Army installations, activities, and communities. This circular is applicable during full mobilization unless otherwise stated.

Proponent and exception authority. The proponent of this circular is the United States Army, CIO/G–6. The proponent has the authority to approve exceptions or waivers to this circular that are consistent with controlling law and regulations. The proponent may delegate this approval authority, in writing, to a division chief within the proponent agency or its direct reporting unit or field operating agency, in the grade of colonel or the civilian equivalent. Activities may request a waiver to this circular by providing justification that includes a full analysis of the expected benefits and must include formal review by the activity's senior legal officer. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through their higher headquarters to the circular proponent. Refer to AR 25–30 for guidance.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to NETCOM EST–IA CAC/PKI Division, 2531 Crystal Drive, 6th Floor, Arlington, VA 22202.

Distribution. This publication is available in electronic media only and is intended for command levels A, B, C, D, and E for the Active Army, the Army National Guard/Army National Guard United States, and the United States Army Reserve.

Contents (Listed by paragraph and page number)

Chapter 1
Introduction, *page 1*
Purpose • 1–1, *page 1*
References • 1–2, *page 1*
Explanation of abbreviations and terms • 1–3, *page 1*
Responsibilities • 1–4, *page 1*
History • 1–5, *page 1*

Chapter 2
Scope and Focus, *page 4*
Scope • 2–1, *page 4*
Focus • 2–2, *page 4*

Chapter 3
Policy, *page 4*
Digital signatures • 3–1, *page 4*

UNCLASSIFIED

Contents—Continued

Electronic authentication • 3–2, *page 5*
Archiving • 3–3, *page 6*
Army point of contact • 3–4, *page 6*

Appendixes

A. References, *page 7*

B. Extract from E–Authentication Guidance for Federal Agencies (para 2–2 thru 2–5), *page 9*

Table List

Table 1–1: Identity assurance level matrix with paper and electronic approval implementation examples, *page 2*
Table B–1: Maximum Potential Impacts for Each Assurance Level, *page 10*

Figure List

Figure 1–1: Electronic Signature Continuum Table, *page 3*

Glossary

Chapter 1
Introduction

1–1. Purpose

This circular provides background information and guidance to advance the implementation of digital signatures.

1–2. References

Required and related publications and prescribed and referenced forms are listed in appendix A.

1–3. Explanation of abbreviations and terms

Abbreviations and terms used in this circular are explained in the glossary.

1–4. Responsibilities

The Chief Information Officer/G-6 (CIO/G-6) will implement the policy and procedures for electronic signature as mandated by Title 15, section 7001, United States Code (15 USC 7001), Electronic Signatures in Global and National Commerce Act (also known as the "E-Sign Act").

1–5. History

a. Private and commercial organizations have been seeking a "paperless office" for years. Requirements for handwritten signatures often represent the largest delay in an otherwise automated or electronic system. Public Law (PL) 104–13, Public Law 105–277, and Public Law 106–229 establish electronic signature policy and requirements for the Federal government. These statutes champion "paperless" activities as the most efficient method to conduct transactions, while not precluding the use of written signatures in areas where written signatures are still required. To support the migration to a "paperless office," the U.S. Government clearly acknowledged the importance of electronic signatures with the enactment of the Public Law 105–277. This act required agencies to provide for the use and acceptance of electronic signatures where practicable by October 21, 2003.

b. The term "electronic signature" is a universal term that can be confusing, so it is appropriate to clarify the term for the purposes of this document. According to Public Law 106–229, June 2000, an electronic signature is "an electronic sound, symbol or process attached to a record by a person with the intent to sign the record." A diverse pool of technology tools are used to create electronic signatures such as digitized signatures; passwords or Personal Identification Numbers (PINs); software-based Department of Defense (DOD) Public Key Infrastructure (PKI) certificates; and hardware-based DOD PKI certificates. Electronic signatures are generally divided into two separate categories - digitized signatures and digital signatures. The primary distinction between the two is the presence or absence of Public Key Cryptography (PKC). Digital signatures are the most secure type of electronic signature because of the services provided by asymmetric key pairs used within a PKI. PKI enables strong user authentication, maintains data integrity, and facilitates non-repudiation throughout a given process. Definitions of electronic signature, digitized signature, and digital signature are provided in the glossary with additional remarks for explanatory purposes. These definitions are consistent with those used in the commercial marketplace and DOD, and with the definitions used in Public Law 106–229. Based on these definitions, only PKC-enabled digital signatures offer information assurance features such as data integrity and non-repudiation required by DOD e-business and e-government practices.

c. Digital signature capabilities are required to meet legislative, DOD and Department of the Army (DA) policy mandates for non-repudiation, e-commerce and paperless processing. Senior leaders have become increasingly aware of these requirements as PKI deployments have demonstrated digital signature capabilities for messaging. Use of digital signatures in support of all automated business processes is viewed as the logical next step. Through adoption of Electronic Data Interchange (EDI), Extensible Markup Language (XML), and web-based business processes, government and industry widely recognize the value-add of electronic signatures which replace processes that were previously limited to manual staffing modes.

d. Public Law 106–229 established a statutory framework that ushered in the digital age of electronic government and transformational initiatives. Paperless transactions are the cornerstone to efficiency within administrative and warfighting environments. Streamlining processes that required traditional written (or "wet") signatures and replacing them with electronic signatures, strengthens these processes by strongly authenticating users to the DA's virtual communities, workplaces, and systems.

e. As indicated in Table 1–1 and Figure 1–1, several electronic signature techniques are available. Army Regulation 25–1 mandates Army commands use DOD PKI certificates stored on the Common Access Card (CAC) for all applications requiring digital signatures; however, it does not preclude the use of other electronic signature techniques on an "as necessary" basis. The level of care and trust within the integrated DOD PKI–CAC system is significantly higher than other electronic signature techniques. As such, the guidance provided in this document establishes baseline criteria for the use of digital signatures, and applies to those digital signatures generated under the trust of the DOD PKI–CAC system.

Table 1–1
Identity assurance level matrix with paper and electronic approval implementation examples

Identify Assurance Level: 1
OMB M-04-04 E-Authentication Guidance (required confidence level): Little or no confidence in the asserted identity's validity
NIST 800-63 Electronic Authentication Guideline (electronic authentication requirements): No identity proofing is required at this level. Although an authentication mechanism provides some assurance that the same claimant is accessing the protected transaction, there is not a requirement at this level to use FIPS-approved cryptographic techniques.
Paper Implementation: Faxed signature.
PKE electronic approval implementation: ePersona with a self-signed internal CAC DOD certificate (an approved ID must be shown to an authorized representative when obtaining the ePersona).
PKI applicability: Optional

Identify Assurance Level: 2
OMB M-04-04 E-Authentication Guidance (required confidence level): Some confidence in the asserted identity's validity.
NIST 800-63 Electronic Authentication Guideline (electronic authentication requirements): Authentication requires that the claimant prove through a secure authentication protocol that they control the token. Level 2 requires identity proofing, but does not require FIPS-approved cryptography. It allows any of the token methods of levels 3 and 4, as well as passwords and PINs.
Paper Implementation: Original signature.
PKE electronic approval implementation: ePersona with a self-signed internal CAC DOD certificate (an approved ID must be shown to an authorized representative when obtaining the ePersona).
PKI applicability: Yes.

Identify Assurance Level: 3
OMB M-04-04 E-Authentication Guidance (required confidence level): High confidence in the asserted identity's validity.
NIST 800-63 Electronic Authentication Guideline (electronic authentication requirements): Level 3 authentication requires cryptographic strength mechanisms that protect the primary authentication token against compromise. Relying parties must determine which data requires authentication or confidentiality protection, and are not required to authenticate or encrypt all data transferred. Authentication requires that the claimant prove through a secure authentication protocol that they control the token.
Paper Implementation: Notary.
PKE electronic approval implementation: ePersona with a CAC DOD certificate, private key, and CRL check (at some point in the process).
PKI applicability: Yes.

Identify Assurance Level: 4
OMB M-04-04 E-Authentication Guidance (required confidence level): Very high confidence in the asserted identity's validity.
NIST 800-63 Electronic Authentication Guideline (electronic authentication requirements): Requires strong cryptographic authentication of all parties and all sensitive data transfers between parties. Strong, FIPS-approved cryptographic techniques are used for all operations.
Paper Implementation: Medallion Signature Guarantee (The application of a Medallion Signature Guarantee provides the authentication of the guarantor that the endorser of a certificate is the registered owner and has the legal authority to sign the certificate. The guarantor must know the endorser and stand behind its guarantee.)
PKE electronic approval implementation: ePersona with a CAC DOD certificate, private key, and CRL check (at some point in the process).
PKI applicability: Yes.

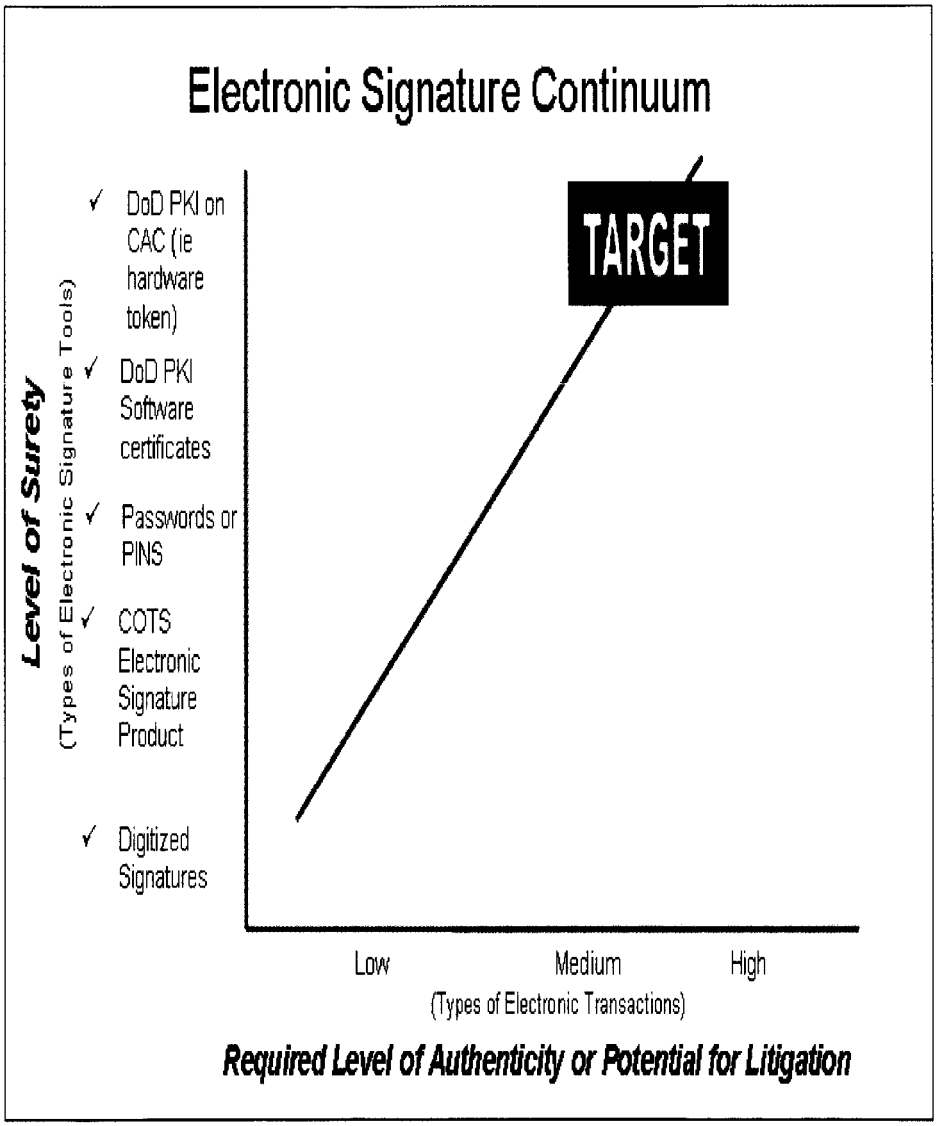

Figure 1–1. Electronic Signature Continuum Table

f. CAC and PKI provide a valuable framework for the "paperless office." An enterprise solution is required to facilitate the Public Key Enabling (PKE) of applications that require digital signatures and fully derive the benefits of this infrastructure; as such the Army has procured an enterprise license for a desktop and server-based electronic solution which is the Army standard for digital signatures. This electronic signature solution is included on the Army Gold Master (AGM) CD, and is available for download through the Army Small Computer Program (ASCP).

Chapter 2
Scope and Focus

2–1. Scope

The scope of this guidance is on Army business systems and forms, not tactics or weapon systems. This circular provides guidelines when implementing digital signature technology. It also reviews regulatory and technology standards pertinent to DOD and discusses how those standards affect interoperability. The Army has selected an enterprise digital signature solution which meets articulated requirements and capabilities and provides the ability to meet interoperability, policy, and regulatory requirements.

2–2. Focus

This guidance focuses on electronic signature tools that are used within the DA to provide non-repudiation and confidentiality to transactions, while critically linking the benefits of digital signatures with mandated requirements and strongly authenticated users to Internet-based systems (AR 25–1, para 5–1). Functional managers and system owners will determine the appropriate electronic signature tool for each type of electronic transaction (for example, financial, confidential, privacy-act related and more). For those transactions that require high levels of assurance, have a high potential for litigation, or have a high monetary value, digital signature tools with increased levels of surety are more appropriate. An extract from Executive Memorandum M–04–04 has been included in appendix B to help guide functional managers and system owners in selecting appropriate levels of assurance for each of their transactions. Figure 1–1 (Electronic Signature Continuum) provides theoretical guidelines to assist Army organizations with those determinations. Table 1–1 lists each of the four identity assurance levels as defined by OMB and National Institute of Standards and Technology (NIST), and provides examples of paper and desktop and server based electronic signature solutions for electronic approval implementations. Whether low, medium or high value transactions, the DA's vision is to eventually steer the vast majority of our electronic signature needs to level 3, those digital signatures provided by DOD PKI certificates stored on the CAC, no matter if these signatures are used for leave requests, travel vouchers, official correspondence, or other business processes.

Chapter 3
Policy

The following policies, procedures, and guidance apply solely to all unclassified Army business processes, network applications, and systems.

3–1. Digital signatures

a. Several policy and regulatory documents have been developed to support technology interoperability and ensure that DOD components are implementing secure information technology (IT) systems. Some of these documents focus on digital signatures, while others only reference the use of this technology. The DOD 8500 series of instructions places stringent requirements on products that support digital signature technology and invoke additional requirements mandated by other organizations. In this section, we reference key policy and regulatory documents and describe how the guidance in those documents affects the Army's use of digital signature technology.

b. As mandated by Joint Task Force Global Network Operations (JTF–GNO) Communications Tasking Order dated 17 January 2006, Subject: Global Network Operations Communications Tasking Order (CTO) 06–02, Tasks for Phase 1 of the Accelerated Public Key Infrastructure (PKI) Implementation, and in accordance with Public Law 106–229 Section 101 (a), Public Law 105–277 section 1703 (a), AR 25–1, paragraph 6–4m(3), and AR 25–2, paragraph 4–20f1(f), it is Army policy that within the unclassified environment:

(1) Digital signatures (whether single or multiple) should be used in place of written signatures for all For Official Use Only (FOUO) information, financial information, Privacy Act information, Unclassified Nuclear Control Information (UNCI), technical/contract data information, proprietary information, directions to subordinates, industry information, and foreign government information. Digital signatures may also be used for other functions, that is, personnel, legal (confidential), and so forth.

(a) Exception #1. This policy does not include DD Form 4/1 (Enlistment/Reenlistment Document Armed Forces of the United States), DD Form 1 (Officer's Commission), SF 61 Appointment Affidavit (federal civilian employment agreement), DD Form 214 (Certificate of Release or Discharge from Active Duty), and NGB Form 22 (Report of Separation and Record of Service). The first three will be the DA's authoritative initial source of an individual's written signature. A written signature will continue to be required for these forms until otherwise directed.

(b) Exception #2. This policy does not include any documents that are covered as "exemptions" or "exceptions" within Public Law 106–229.

(c) Exception #3. This policy does not include any document that requires a notary.

(2) Digital signatures may be used for documents that require witnesses; however, commands must be cognizant of the fact that DOD PKI credentials are only provided to active duty military personnel, selected reserve personnel,

civilians, eligible contract support personnel, select Foreign Military, eligible Foreign Nationals, and those industry partners that conduct business with the DOD.

(3) Commands should review transactions that they want to convert to digital rather than written signatures to make sure there are no conflicting foreign laws, foreign regulations, or treaties, when appropriate.

(4) Commands will ensure that all of their applications, systems, and business processes that use digital signatures:

(a) Prior to an individual digitally signing a transaction, provide an opportunity for that individual to review the information that is about to be digitally signed. This could be accomplished via a warning or message advising an individual that they are about to digitally sign a transaction. The warning must allow the individual to cancel or exit, prior to signing or proceeding with the transaction. Additionally, an acknowledgement statement outlining the associated legal ramifications for digitally signing this transaction must be provided.

(b) Provide a mechanism such that individuals who digitally sign documents and/or forms could (if desired) transition those digital transactions to paper copies. In the event an individual desires paper copies, the capability should exist to include indications or distinctive marks on the paper copies that the documents and/or forms were digitally signed. The indication capabilities should minimally include:

1. Verbiage to confirm the document or form was digitally signed.

2. Name of the individual who digitally signed the document or form.

3. DOD Electronic Digital Interchange Person Identifier (EDI PI) of the individual who digitally signed the document or form.

4. Certificate policy identifier associated with the certificate of the individual who digitally signed the document or form.

5. Date and time transaction was signed.

(c) Ensure the integrity of a digitally signed transaction in such a manner that records can be determined to be authentic and reliable by tracking the chain of custody and any changes that may occur (authorized or unauthorized).

(d) Ensure that implementations of digital signatures sign over the data and document containing it (for example, the blank form or document). This will provide the proper context and assists in establishing intent when a user signs a particular transaction.

(e) Ensure the validity of the DOD PKI certificate used to digitally sign and/or authenticate by checking revocation status and performing path processing of the certificate issuance chain.

(f) Archive digitally signed transactions in accordance with existing records management policies and procedures. Paragraph 3–3 addresses archiving.

3–2. Electronic authentication

a. The Army will continue to make significant progress in enabling unclassified Army networked workstations and Web sites to support the DOD PKI. The key to attaining a substantial level of assurance, as well as functionality, from the use of PKI and digital signatures is trust. Trust entails relying parties (applications/system owners) believing that the individuals requesting virtual access to services or digitally signing transactions are who they say they are. The designers of the integrated DOD PKI–CAC system have gone to great lengths to ensure the level of trust and assurance is sound in binding an individual's identity to their certificates and associated key pairs. Supporting measures include the use of strong hardware-based cryptography, a controlled Defense Enrollment Eligibility Reporting System (DEERS)/Real-time Automated Personnel Identification System (RAPIDS) issuing infrastructure, and verification by the National Security Agency's (NSA) security assessment resources.

b. Executive Memorandum M–04–04, and National Institute of Standards and Technology Special Publication 800–63, outline several requirements for authenticating users of Federal Internet-based systems. In order to ensure the Army is in compliance with each of these requirements:

(1) All Army commands are directed to conduct risk assessments for all existing Internet-based Army systems requiring user authentication.

(a) These risk assessments will be completed using OMB's "E-authentication Risk and Requirements Assessment" tool and guide, found at www.cio.gov/eauthentication/era.htm.

(b) Results are to be reported through the appropriate chain-of-command to the Deputy Director, Army CAC/PKI Division, Network Enterprise Technology Command/9th Army Signal Command, Enterprise System Technology Activity, Information Assurance Program (NETCOM ESTA IAP).

(2) When authenticating users that are active duty military, selected reserve military, civilian, industry partners, select Foreign Military, eligible Foreign Nationals, and eligible support contract personnel, all Army Internet-based systems will either integrate or use DOD PKI client-side authentication services through the Army Knowledge Online (AKO) Portal or independently as mandated in AR 25–1, paragraph 6–4n(2).

(3) When authenticating users outside the population identified in subparagraph 3–2b(2), all Army Internet-based systems should be prepared to use the appropriate authentication method from NIST's electronic authentication guidance.

(4) All Army commands should be preparing to incorporate the processes and guidance in subparagraphs 3–2b*(1)*, *(2)* and *(3)*, into all emerging and new Army Internet-based systems.

c. A digital signature, whether created by a subscriber, an authentic message or by a certification authority to authenticate its certificate should be time-stamped by an Internet Engineering Task Force (IETF) Request for Comments (RFC) 3161 Time Stamp Protocol (TSP) application.

3–3. Archiving

The Army signature policy requires commands to archive the digitally signed transactions in accordance with Records Management Guidance for PKI Digital Signature Authentication and Secure Transaction Records, National Archive and Records Administration (NARA) Federal Public Key Infrastructure Steering Committee Legal/Policy Working Group, 11 March 2005, and Implementation of the Army Records Information Management System, Chief Information Officer/G-6, Memorandum of 27 June 2005. The Army signature guidance also requires the responsible organization to "ensure the integrity of a digitally signed transaction in such a manner that records can be determined to be authentic and reliable by tracking the chain of custody and any changes that may occur (authorized or unauthorized)." This guidance is consistent with a NIST recommendation (see NIST Special Pub 800–25, paragraph D5.12): "All of the information required to validate a digital signature after the relevant certificates have expired should be available. This includes the expired certificates and the certificate revocation lists (CRLs) or other information showing that the certificates were valid at the time the signature putatively (supposedly) was made." This could also include e-mails or workflow history related to digitally signed transactions. Archiving a copy of the e-mail or associated workflow history showing the digitally signed document was sent to you from the signer adds confidence in the identity of the signer. This provides an additional layer of surety because the document is coming from their personal e-mail or from a password protected workflow system.

3–4. Army point of contact

Both electronic authentication and signatures are key tools in the transformation of the DA's virtual environments and business processes. We recognize and appreciate the efforts to date and solicit your support and cooperation in continuing to lead the Federal sector in implementing practical eGovernment and identity management solutions. Forward questions concerning the interpretation of guidance provided in this circular to the Army point of contact, the Deputy Director, Army CAC/PKI Division, NETCOM ESTA IAP.

Appendix A
References

Section I
Required Publications

Office of Management and Budget
e-Authentication Risk and Requirements Assessment tool. (Cited in para 2–2.) (Available at http://www.cio.gov/euathentication/era.htm.)

Section II
Related Publications
A related publication is a source of additional information. The user does not have to read it to understand this publication

AR 25–1
Army Knowledge Management and Information Technology.

AR 25–2
Information Assurance.

DA Pam 25–1–1
Information Technology Support and Services.

Chief Information Officer/G–6 Memorandum of 27 June 2005
Implementation of the Army Records Information Management System (ARIMS). (Available at http://www.army.mil/ciog6/references/policy/docs/RecordsManagement.pdf.)

Executive Memorandum M–04–04
E–Authentication Guidance for Federal Agencies. (Available at http://www.whitehouse.gov/omb/memoranda/fy04/m04–04.pdf)

Federal Information Processing Standards (FIPS) – 199
Standards for Security Categorization of Federal Information and Information Systems. (Available at http://csrc.nist.gov/publications/fips/fips199/FIPS–PUB–199-final.pdf)

Joint Task Force Global Network Operations WARNORD 06–16
Global Network Defense Warning Order (WARNORD) 06–16 Specified Tasks for Phase I of the Accelerated Public Key Infrastructure (PKI) Implementation.

National Archives and Records Administration (NARA) Federal Public Key Infrastructure Steering Committee Legal/Policy Working Group, March 11, 2005
Records Management Guidance for PKI Digital Signature Authenticated and Secured Transaction Records. (Available at http://www.archives.gov/records-mgmt/policy/pki.html)

National Institute of Standards and Technology (NIST) Special Publication 800–30
Risk Management Guide for Information Technology Systems. (Available at http://csrc.nist.gov/publications/nistpubs/800–30/sp800–30.pdf.)

National Institute of Standards and Technology (NIST) Special Publication 800–63
Electronic Authentication Guideline. (Available at http://csrc.nist.gov/publications/nistpubs/800–63/SP800–63v6_3_3.pdf)

15 USC 7001
General rule of validity. (Available at http://www.gpoaccess.gov.uscode.)

18 USC 1029
Fraud and related activity in connection with access devices. (Available at http://www.gpoaccess.gov.uscode.)

18 USC 1030
Fraud and related activity in connection with computers. (Available at http://www.gpoaccess.gov.uscode.)

Public Law 104–13
Paperwork Reduction Act of 1995. (Available at http://thomas.loc.gov/bss/)

Public Law 105–277
The Government Paperwork Elimination Act. (Available at http://thomas.loc.gov/bss/)

Public Law 106–229
Electronic Signatures in Global and National Commerce Act. (Available at http://thomas.loc.gov/bss/)

Section III
Prescribed Forms

This section contains no entries.

Section IV
Referenced Forms

DD Form 1
Officer's Commission.

DD Form 4/1
Enlistment/Reenlistment Document - Armed Forces of the United States.

DD Form 214
Certificate of Release or Discharge from Active Duty.

SF 61
Appointment Affidavit.

NGB Form 22
Report of Separation and Record of Service.

Appendix B
Extract from E–Authentication Guidance for Federal Agencies (para 2–2 thru 2–5)

B–1. Risks, potential impacts, and assurance levels

a. While, this guidance addresses only those risks associated with authentication errors, NIST Special Publication 800–30, "Risk Management Guide for Information Technology Systems," recommends a general methodology for managing risk in Federal information systems. In addition, other means of risk management, (for example, network access restrictions, intrusion detection, and event monitoring) may help reduce the need for higher levels of authentication assurance.

b. To determine the appropriate level of assurance in the user's asserted identity; agencies must assess the potential risks, and identify measures to minimize their impact. Authentication errors with potentially worse consequences require higher levels of assurance. Business process, policy, and technology may help reduce risk. The risk from an authentication error is a function of two factors:

(1) Potential harm or impact.

(2) The *likelihood* of such harm or impact.

c. Categories of harm and impact include:

(1) Inconvenience, distress, or damage to standing or reputation.

(2) Financial loss or agency liability.

(3) Harm to agency programs or public interests.

(4) Unauthorized release of sensitive information.

(5) Personal safety.

(6) Civil or criminal violations.

d. Required assurance levels for electronic transactions are determined by assessing the potential impact of each of the above categories using the potential impact values described in Federal Information Processing Standard (FIPS) 199, "Standards for Security Categorization of Federal Information and Information Systems." For the purposes of this document, the impact value not applicable may apply to the categories of harm. The three potential impact values are:

(1) Low impact.

(2) Moderate impact.

(3) High impact.

e. The next section defines the potential impacts for each category. Note: If authentication errors cause no measurable consequences for a category, there is "no" impact.

B–2. Determining potential impact of authentication errors

a. Potential impact of inconvenience, distress, or damage to standing or reputation:

(1) Low–at worst, limited, short-term inconvenience, distress or embarrassment to any party.

(2) Moderate–at worst, serious short term or limited long-term inconvenience, distress or damage to the standing or reputation of any party.

(3) High – severe or serious long-term inconvenience, distress or damage to the standing or reputation of any party (ordinarily reserved for situations with particularly severe effects or which affect many individuals).

b. Potential impact of *financial loss*:

(1) Low – at worst, an insignificant or inconsequential unrecoverable financial loss to any party, or at worst, an insignificant or inconsequential agency liability.

(2) Moderate – at worst, a serious unrecoverable financial loss to any party, or a serious agency liability.

(3) High – severe or catastrophic unrecoverable financial loss to any party; or severe or catastrophic agency liability.

c. Potential impact of harm to agency programs or public interests:

(1) Low – at worst, a limited adverse effect on organizational operations or assets, or public interests. Examples of limited adverse effects are: (i) mission capability degradation to the extent and duration that the organization is able to perform its primary functions with *noticeably* reduced effectiveness, or (ii) minor damage to organizational assets or public interests.

(2) Moderate – at worst, a serious adverse effect on organizational operations or assets, or public interests. Examples of serious adverse effects are: (i) significant mission capability degradation to the extent and duration that the organization is able to perform its primary functions with *significantly* reduced effectiveness; or (ii) significant damage to organizational assets or public interests.

(3) High – a severe or catastrophic adverse effect on organizational operations or assets, or public interests. Examples of severe or catastrophic effects are: (i) severe mission capability degradation or loss of to the extent and duration that the organization is unable to perform one or more of its primary functions; or (ii) major damage to organizational assets or public interests.

d. Potential impact of *unauthorized release of sensitive information*:

(1) Low – at worst, a limited release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in a loss of confidentiality with a low impact as defined in FIPS PUB 199.

(2) Moderate – at worst, a release of personal, U.S. government sensitive or commercially sensitive information to unauthorized parties resulting in loss of confidentiality with a moderate impact as defined in FIPS PUB 199.

(3) High – a release of personal, U.S. government sensitive or commercially sensitive information to unauthorized parties resulting in loss of confidentiality with a high impact as defined in FIPS PUB 199.

e. Potential impact to *personal safety*:

(1) Low – at worst, minor injury not requiring medical treatment.

(2) Moderate – at worst, moderate risk of minor injury or limited risk of injury requiring medical treatment.

(3) High – a risk of serious injury or death.

f. The potential impact of *civil or criminal violations* is:

(1) Low – at worst, a risk of civil or criminal violations of a nature that would not ordinarily be subject to enforcement efforts.

(2) Moderate – at worst, a risk of civil or criminal violations that may be subject to enforcement efforts.

(3) High – risk of civil or criminal violations that are of special importance to enforcement programs.

B–3. Determining assurance level:

a. Compare the impact profile from the risk assessment to the impact profiles associated with each assurance level, as shown in Table B–1 below. To determine the required assurance level, find the lowest level whose impact profile meets or exceeds the potential impact for every category analyzed in the risk assessment (as noted in step 2 below).

Table B–1
Maximum Potential Impacts for Each Assurance Level

Assurance Level Impact Profiles				
Potential Impact Categories for Authentication Errors	1	2	3	4
Inconvenience, distress or damage to standing or reputation	Low	Mod	Mod	High
Financial loss or agency liability	Low	Mod	Mod	High
Harm to agency programs or public interests	N/A	Low	Mod	High
Unauthorized release of sensitive information	N/A	Low	Mod	High
Personal Safety	N/A	N/A	Low	Mod High
Civil or criminal violations	N/A	Low	Mod	High

b. In analyzing potential risks, the agency must consider all of the potential direct and indirect results of an authentication failure, including the possibility that there will be more than one failure, or harms to more than one person. The definitions of potential impacts contain some relative terms, like "serious" or "minor," whose meaning will depend on context. The agency should consider the context and the nature of the persons or entities affected to decide the relative significance of these harms. Over time, the meaning of these terms will become more definite as agencies gain practical experience with these issues. The analysis of harms to agency programs or other public interests depends strongly on the context; the agency should consider these issues with care.

c. In some cases (as shown in table B–1), impact may correspond to multiple assurance levels. For example, table B–1 shows that a moderate risk of financial loss corresponds to assurance levels 2 and 3. In such cases, agencies should use the context to determine the appropriate assurance level.

B–4. Determining assurance levels and selecting authentication solutions using risk assessment

Agencies will use the following steps to determine the appropriate assurance level:

a. Step 1: Conduct a risk assessment of the e-government system.

(1) Guidance for agencies in conducting risk assessments is available in A–130, Section 5 of OMB's GPEA guidance and existing NIST guidance. The risk assessment will measure the relative severity of the potential harm and likelihood of occurrence of a wide range of impacts (to any party) associated with the e-government system in the event of an identity authentication error.

(2) Note: An E-government system may have multiple categories or types of transactions, which may require separate analysis within the overall risk assessment. An E-government system may also span multiple agencies whose activities may require separate consideration.

(3) Risk analysis is to some extent a subjective process, in which agencies must consider harms that might result from, among other causes, technical failures, malevolent third parties, public misunderstandings, and human error. Agencies should consider a wide range of possible scenarios in seeking to determine what potential harms are associated with their business process. It is better to be over-inclusive than under-inclusive in conducting this analysis. Once risks have been identified, there may also be ways to adjust the business process to mitigate particular risks by reducing the likelihood that they will occur (see step 4).

b. Step 2: Map identified risks to the required assurance level.

(1) The risk assessment should be summarized in terms of the potential impact categories in section B–1.b.

(2) To determine the required assurance level, agencies should initially identify risks inherent in the transaction process, regardless of its authentication technology. Agencies should then tie the potential impact category outcomes to the authentication level, choosing the lowest level of authentication that will cover all of potential impacts identified. Thus, if five categories of potential impact are appropriate for Level 1, and one category of potential impact is appropriate for Level 2, the transaction would require a Level 2 authentication. For example, if the misuse of a user's electronic identity/credentials during a medical procedure presents a risk of serious injury or death, map to the risk profile identified under Level 4, even if other consequences are minimal.

c. Step 3: Select technology based on the NIST e-authentication technical guidance. After determining the assurance level, the agency should refer to the NIST e-authentication technical guidance to identify and implement the appropriate technical requirements.

d. Step 4: After implementation, validate that the information system has operationally achieved the required assurance level. Because some implementations may create or compound particular risks, conduct a final validation to confirm that the system achieves the required assurance level for the user-to-agency process. The agency should validate that the authentication process satisfies the system's authentication requirements as part of required security procedures (for example, certification and accreditation).

e. Step 5: Periodically reassess the information system to determine technology refresh requirements. The agency must periodically reassess the information system to ensure that the identity authentication requirements continue to be valid as a result of technology changes or changes to the agency's business processes. Annual information security assessment requirements provide an excellent opportunity for this. Agencies may adjust the identity credential's level of assurance using additional risk mitigation measures. Easing identity credential assurance level requirements may increase the size of the enabled customer pool, but agencies must ensure that this does not corrupt the system's choice of the appropriate assurance level.

B–5. Assurance levels and risk profiles: descriptions and examples

a. Level 1. Little or no confidence exists in the asserted identity. For example, Level 1 credentials allow people to bookmark items on a web page for future reference.

(1) In some instances, the submission of forms by individuals in an electronic transaction will be a Level 1 transaction: (i) when all information is flowing to the Federal organization from the individual, (ii) there is no release of information in return, and (iii) the criteria for higher assurance levels are not triggered. For example, if an individual applies to a Federal agency for an annual park visitor's permit (and the financial aspects of the transaction are handled by a separate contractor and thus analyzed as a separate transaction, the transaction with the Federal agency would otherwise present minimal risks and could be treated as Level 1.

(2) A user presents a self-registered user ID or password to the U.S. Department of Education web page, which allows the user to create a customized "My.ED.gov" page. A third party gaining unauthorized access to the ID or password might infer personal or business information about the individual based upon the customization, but absent a high degree of customization however, these risks are probably very minimal.

(3) A user participates in an online discussion on the whitehouse.gov Web site, which does not request identifying information beyond name and location. Assuming the forum does not address sensitive or private information, there are no obvious inherent risks.

b. Level 2. On balance, confidence exists that the asserted identity is accurate. Level 2 credentials are appropriate for a wide range of business with the public where agencies require an initial identity assertion (the details of which are verified independently prior to any Federal action).

(1) A user subscribes to the Gov Online Learning Center (www.golearn.gov). The site's training service must authenticate the person to present the appropriate course material, assign grades, or demonstrate that the user has satisfied compensation-or promotion-related training requirements. The only risk associated with this transaction is a third party gaining access to grading information, thereby harming the student's privacy or reputation. If the agency determines that such harm is minor, the transaction is Level 2.

(2) A beneficiary changes the address of record through the Social Security Web site. The site needs authentication to ensure that the entitled person's address is changed. This transaction involves a low risk of inconvenience. Since official notices regarding payment amounts, account status, and records of changes are sent to the beneficiary's address of record, it entails moderate risk of unauthorized release of personally sensitive data. The agency determines that the risk of unauthorized release merits Assurance Level 2 authentication.

(3) An agency program client updates bank account, program eligibility, or payment information. Loss or delay would significantly impact him or her. Errors of this sort might delay payment to the user, but would not normally result in permanent loss. The potential individual financial impact to the agency is low, but the possible aggregate is moderate.

(4) An agency employee has access to potentially sensitive personal client information. She authenticates individually to the system at Level 2, but technical controls (such as a virtual private network) limit system access to the system to the agency premises. Access to the premises is controlled, and the system logs her access instances. In a less constrained environment, her access to personal sensitive information would create *moderate* potential impact for unauthorized release, but the system's security measures reduce the overall risk to *low*.

c. Level 3. Level 3 is appropriate for transactions needing high confidence in the asserted identity's accuracy. People may use Level 3 credentials to access restricted web services without the need for additional identity assertion controls.

(1) A patent attorney electronically submits confidential patent information to the US Patent and Trademark Office. Improper disclosure would give competitors a competitive advantage.

(2) A supplier maintains an account with a General Services Administration Contracting Officer for large government procurement. The potential financial loss is significant, but not severe or catastrophic, so Level 4 is not appropriate.

(3) A First Responder accesses a disaster management reporting Web site to report an incident, share operational information, and coordinate response activities.

(4) An agency employee or contractor uses a remote system giving him access to potentially sensitive personal client information. He works in a restricted-access Federal office building. This limits physical access to his computer, but system transactions occur over the Internet. The sensitive personal information available to him creates a moderate potential impact for unauthorized release.

d. Level 4. Level 4 is appropriate for transactions needing very high confidence in the asserted identity's accuracy. Users may present Level 4 credentials to assert identity and gain access to highly restricted web resources, without the need for further identity assertion controls.

(1) A law enforcement official accesses a law enforcement database containing criminal records. Unauthorized access could raise privacy issues and/or compromise investigations.

(2) A Department of Veteran's Affairs pharmacist dispenses a controlled drug. She would need full assurance that a qualified doctor prescribed it. She is criminally liable for any failure to validate the prescription and dispense the correct drug in the prescribed amount.

(3) An agency investigator uses a remote system giving her access to potentially sensitive personal client information. Using her laptop at client worksites, personal residences, and businesses, she accesses information over the Internet via various connections. The sensitive personal information she can access creates only a moderate potential impact for unauthorized release, but her laptop's vulnerability and her non-secure Internet access raise the overall risk.

B–6. Scope and elements of risk

a. When determining assurance levels, one element of the necessary risk assessment is the risk of denial (or repudiation) of electronically transmitted information. Section 9c of OMB's GPEA guidance states agencies should plan how to minimize this risk by ensuring user approval of such information. Section 8c of the OMB Procedures and Guidance on Implementing GPEA includes guidance on minimizing the likelihood of repudiation.

b. OMB's GPEA guidance states that properly implemented technologies can offer degrees of confidence in authenticating identity that are greater than a handwritten signature can offer. Conversely, electronic transactions may increase the risk and harm (and complicate redress) associated with criminal and civil violations. The Department of Justice's "Guide for Federal Agencies on Implementing Electronic Processes" discusses the legal issues surrounding electronic government. This guide is available at http://www.usdoj.gov/criminal/cybercrime/eprocess.pdf. Legal and enforcement needs may affect the design of an e-authentication system and may also entail generation and maintenance of certain system management documentation.

c. Legal issues can present significant policy challenges for agencies. Agencies should consider these issues when assigning transactions to assurance levels. Risk assessments should include the potential effects of illegal activities and process failures with respect to:

(1) Agency enforcement priorities.

(2) Agency programmatic interests.

(3) Broader public interests such as national security, the environment, and economic markets.

d. Some of these harms (for example, financial loss or release of personal information) are described in each assurance level; others depend on the agency's programmatic interests. The risk analysis process is necessarily highly contextual, and agencies should consider whether their systems present any distinctive risks.

e. The risk analysis incorporates this by discussing the risks associated with criminal and civil violations, and harm to agency programs or the public interest. Agencies should remember to consult appropriately with their counsel's office in their determination of this impact. When assessing this risk when designing a process, agencies should consider single acts or patterns of action that could affect agency programs. For example, if sensitive information is

available from an agency Web site, the agency should consider the effects of single acts and possible patterns of such activity when assessing risk levels. (18 USC 1029 and 1030)

f. Agencies may also decrease reliance on identity credentials through increased risk-mitigation controls. For example, an agency business process rated for Level 3 identity assertion assurance may lower its profile to accept Level 2 credentials by increasing system controls or 'second level authentication' activities. (See section 2–3, step 5 (B–4e, step 5))

g. Agencies are expected to follow all relevant guidance issued by the National Achieves and Records Administration (NARA) regarding the handling of electronic records. This guidance addresses implementation issues further in section 4.1 (Executive Memorandum M–04–04, E–Authentication Guidance for Federal Agencies).

Glossary

Section I
Abbreviations

AGM
Army gold master

AKO
Army Knowledge Online

ASCP
Army Small Computer Program

CAC
common access card

CIO/G-6
Chief Information Officer/G-6

CRL
Certificate Revocation List

CTO
communications tasking order

DA
Department of the Army

DEERS
Defense Enrollment Eligibility Reporting System

DOD
Department of Defense

EDI
electronic data interchange

EDI PI
electronic digital interchange person identifier

FIPS
Federal Information Processing Standard

GPEA
Government Paperwork Elimination Act

IETF
Internet Engineering task Force

IT
information technology

JTF-GNO
Joint Task Force Global Network Operations

NARA
National Archive and Records Administration

NETCOM ESTA IAP
Network Enterprise Technology Command/9th Army Signal Command, Enterprise System Technology Activity, Information Assurance Program

NIST
National Institute of Standards and Technology

NSA
National Security Agency

PIN
personal identification numbers

PKC
public key crytography

PKE
public key enabling

PKI
public key infrastructure

PL
public law

RAPIDS
Real-time Automated Personnel Identification System

RFC
request for comments

TSP
time stamp protocol

UNCI
unclassified nuclear control information

XML
extensible markup language

Section II
Terms

Asymmetric Key Pairs
A cryptographic system that consists of a personal private key and a public key. An individual has both a private key that is kept secret and a public key that everyone knows.

Authentication
The process in which users, systems, and devices identify themselves to virtual spaces, by using usernames with passwords, tokens, cryptographic keys, and other means.

Authorization
The process in which virtual spaces map authenticated users, systems, and devices to access their privileges.

Digital signatures
Designed to provide both a high degree of connection between a signer's identity electronic mark, as well as greater security and integrity of signed information through the use of advanced cryptography. Public Key Infrastructure (PKI) provides the mechanism for issuing and managing digital certificates that signers use to create digital signatures. Digital signatures do not attempt to reproduce a hand written signature, but they do provide non-repudiation and data integrity through the encryption of a unique electronic fingerprint of each document based on its contents.

Digitized signatures
A type of electronic signature that captures a digital picture of an individual's written signature, and places it within an electronic form or transaction package. (Also referred to as a "wet" signature.) There is no cryptography associated within this process. For example, commercial retailers and delivery services have customers accept transactions by signing on a digitizing pad using a stylus. This process captures a bit map image of the customer's signature that can be stored and is representative of a hand written signature.

Electronic signature
An electronic symbol or process attached to, or logically associated with, a record and used by a person with the intent to sign the record (reference (a)). A more sophisticated type of electronic signature is a digital signature.

ePersona
A digital identity consisting of an electronic image of their handwritten signature. Unique to each user, an ePersona is securely encrypted and can only be accessed via personal password.

Section III
Special Abbreviations and Terms
This section contains no entries.

USAPD

ELECTRONIC PUBLISHING SYSTEM
OneCol FORMATTER WIN32 Version 235

PIN:	083355–000
DATE:	07-25-06
TIME:	11:00:56
PAGES SET:	20
DATA FILE:	C:\wincomp\c25-06-1.fil
DOCUMENT:	DA CIR 25–06–1
SECURITY:	UNCLASSIFIED
DOC STATUS:	NEW PUBLICATION