USE OF ELECTRONIC SIGNATURES IN FEDERAL ORGANIZATION TRANSACTIONS

Version 1.0

January 25, 2013

Executive Summary

This document was developed by the General Services Administration (GSA) and Federal Chief Information Officers (CIO) Council at the request of the Office of Management and Budget (OMB). In developing this document, GSA collaborated with the Department of Defense (DoD), Department of Justice (DOJ), and the National Institute of Standards and Technology (NIST). This document supplements guidance previously issued by OMB and DOJ and referenced in Appendix H of this document.

OMB is responsible for developing general standards and guidelines for the use of electronic signatures by federal organizations, subject to any special requirements adopted by regulations issued by specific federal organizations. This document focuses on the electronic signature requirements of the Government Paperwork Elimination Act of 1998 (GPEA), the Electronic Records and Signatures in Global and National Commerce Act (E-SIGN), and the Uniform Electronic Transactions Act (UETA), and is designed to assist federal organization officials in complying with the signing requirements of these statutes applicable to electronic transactions.

While this document provides general guidance with respect to compliance with the legal requirements for electronic signatures, it is unable to address all of the legal issues that might arise. Thus, federal organizations should consult with their legal counsel as necessary when questions arise regarding implementation of the guidance provided here, or with respect to other electronic signature issues not addressed here. This guidance has been prepared for use by federal organizations. It may also be used by nongovernmental organizations on a voluntary basis and is not subject to copyright.

Nothing in this document should be taken to contradict standards and guidance made mandatory and binding by specific regulations adopted by any federal organization. Nor should this guidance be interpreted as altering or superseding the existing authorities of any federal organization with respect to signature issues.

TABLE OF CONTENTS

TABLES

FIGURES

USE OF ELECTRONIC SIGNATURES IN FEDERAL ORGANIZATION TRANSACTIONS

A. INTRODUCTION AND SCOPE

This document provides general guidance for federal organizations regarding the use of electronic signatures in connection with electronic records and electronic transactions. It addresses the following basic questions:

- When should a federal organization use an electronic signature?
- What are the requirements for creating a legally binding electronic signature in electronic transactions?
- What factors should federal organizations consider when deciding which signing process to use?

The focus of this guidance is on the use of electronic signatures for **legal signing purposes** in the **context of electronic transactions**.

Because this guidance focuses on electronic signatures used for legal signing purposes in electronic transactions, it does not address the use of similar electronic processes solely for social, identification, technical, or security-related purposes (such as authentication or document integrity). Thus, when symbols or processes that can qualify as a legally binding electronic signature (if the requirements set out in Part D below are met) are used in a manner that is not intended to be a legally binding signature (e.g., intended merely to convey a social message, to identify the sender, or to provide some level of security) they are not covered by this guidance.

Likewise, this guidance focuses only on the use of legally binding electronic signatures in the context of electronic transactions – i.e., actions between two or more persons relating to the conduct of business, consumer, commercial, or governmental affairs.[1] It does not address the use of signatures or similar electronic processes in communications that do not constitute an electronic transaction, such as their use in a more informal setting like a social email.

Moreover, this guidance does not address any of the other requirements for a valid electronic transaction, such as requirements for the consent of the parties to conduct the transaction in electronic form or to receive documents in electronic form, requirements for contract formation processes, ensuring the ability to download and print, etc.[2] Also, this document does not address any specific privacy issues that may

[1] See generally E-SIGN, 15 U.S.C. § 7006(13) and UETA § 2(16) (definitions of "transaction").

[2] For guidance regarding some of those issues, see generally, Office of Management and Budget Memorandum M-00-10, Implementation of the Government Paperwork Elimination Act, April 25, 2000 (hereinafter "OMB M-00-10); Appendix II to OMB Circular A-130, November 2000; Office of Management and Budget Memorandum M-00-15, Guidance on Implementation of the Electronic Signatures in Global and National Commerce Act (E-SIGN), September 25, 2000 (hereinafter "OMB M-00-15"); U.S.

arise in connection with the use of electronic signatures. Individuals using this guidance should consult with their respective privacy offices and privacy counsel about any privacy issues.

This guidance is designed to assist federal organization officials in complying with the signing requirements of the primary statutes applicable to electronic transactions. It does not, however, address the question of determining which one of those statutes applies to any particular agency electronic transaction. Likewise, it does not address agency regulations that might impose additional signature requirements for particular types of electronic transactions. This document also does not address the use of electronic signatures (or other electronic mechanisms) in the legislative process.[3]

While this document provides general guidance with respect to compliance with the legal requirements for electronic signatures, it is unable to address all of the legal issues that might arise. Thus, federal organizations should consult with their legal counsel as necessary when questions arise regarding implementation of the guidance provided here, or with respect to other electronic signature issues not addressed here.

B. OVERVIEW OF THE LAW OF ELECTRONIC SIGNATURES

1. The Role of Signatures Generally

A signature, whether electronic or on paper, is the means by which a person indicates an intent to associate himself with a document in a manner that has legal significance (e.g., to adopt or approve a specific statement regarding, or reason for signing, a document). It constitutes legally-binding evidence of the signer's intention with regard to a document. The reasons for signing a document will vary with the transaction, and in most cases can be determined only by examining the context in which the signature was made. Generally, however, a person's reason for signing a document falls into one of the following categories:

- Approving, assenting to, or agreeing to the information in the document or record signed (e.g., agreeing to the terms of a contract or inter-agency memorandum);[4]

Department of Justice, Legal Considerations in Designing and Implementing Electronic Processes: A Guide for Federal Agencies, November 2000.

[3] Cf. Memorandum for the Counsel to the President from Jonathan G. Cedarbaum, Deputy Assistant Attorney General, Office of Legal Counsel, *Re: Whether Bills May Be Presented by Congress and Returned by the President by Electronic Means* (May 3, 2011); Memorandum Opinion for the Counsel to the President from Howard G. Nielson, Jr., Deputy Assistant Attorney General, Office of Legal Counsel, *Re: Whether the President May Sign a Bill by Directing that His Signature Be Affixed to It* (July 7, 2005).

[4] With respect to contracts, for example, many courts note that: "The purpose of a signature on a contract is to show mutual assent . . . ." See, e.g., *Southern Elec. Servs. v. Cornerstone Det. Prods*., 2010 U.S. Dist. LEXIS 54313, *13 (W.D. Va. June 3, 2010); *NeighborCare Pharm. Servs. v. Sunrise Healthcare Ctr., Inc*., 2005 U.S. Dist. LEXIS 34404, *6 (D. Md. December 20, 2005); *Taylor v. First N. Am. Nat'l Bank*, 325 F. Supp. 2d 1304, 1313; 2004 U.S. Dist. LEXIS 13671, (M.D. Ala. July 16, 2004); 17A Am. Jur. 2d Contracts § 34.

- Certifying or affirming the accuracy of the information stated in the document or record signed (e.g., certifying that the statements in one's tax return are true and correct);
- Acknowledging access to or receipt of information set forth in the document or record signed (e.g., acknowledging receipt of a disclosure document);
- Witnessing the signature or other act of another (e.g., notarization); or
- Certifying the source of the information in the document or record signed (e.g., certifying data in a clinical trial record, certifying an inventory count, etc.)

Thus, a signature is used to provide evidence of a person's intent to approve or adopt a statement in, or reason for signing, a document in a legally binding way.

2. The Law Governing Electronic Signatures

The use of electronic signatures in transactions involving federal organizations will be primarily governed by one of the following laws ("E-Transaction Laws"):

- **Government Paperwork Elimination Act** ("GPEA")[5] a federal law enacted in 1998 that is applicable to governmental transactions and other transactions involving certain federal organizations;
- **Electronic Signatures in Global and National Commerce Act** ("E-SIGN"),[6] a federal law enacted in 2000 that largely preempts inconsistent state law (although in certain cases state law may still control)[7] and that is applicable to commercial, consumer, or business transactions involving federal organizations;
- **Uniform Electronic Transactions Act** ("UETA"),[8] a uniform state law that was finalized by the National Conference of Commissioners on Uniform State Laws ("NCCUSL") in 1999 and subsequently adopted by 47 states[9] and

[5] Government Paperwork Elimination Act (hereinafter "GPEA"), 44 U.S.C. § 3504.

[6] Electronic Signatures in Global and National Commerce Act (hereinafter "E-SIGN"), 15 U.S.C. § 7001 et. seq., effective October 1, 2000. E-SIGN preempts all inconsistent state legislation, other than state enactments of the Uniform Electronic Transactions Act in the form promulgated by the National Conference of Commissioners on Uniform State Laws (per 15 U.S.C. § 7002).

[7] E-SIGN permits UETA (as well as certain other state laws specifying alternative procedures or requirements for the use and/or acceptance of electronic records or electronic signatures that are "consistent" with E-SIGN) to modify, limit, or supersede the provisions of Section 101 of E-SIGN. See E-SIGN Section 102 (15 U.S.C. § 7002). E-SIGN also provides that the provisions of Section 101 "shall not apply" to records to the extent that they are governed by certain other state laws, including laws governing the creation and execution of wills, laws governing adoption, divorce or other family law matters, and certain provisions of the UCC. See, E-SIGN, 15 U.S.C. § 7003(a).

[8] Uniform Electronic Transactions Act (hereinafter "UETA"), approved by the National Conference of Commissioners on Uniform State Laws (NCCUSL) on July 23, 1999. NCCUSL is now known as the Uniform Law Commission. See www.nccusl.org.

[9] As of November, 2011, 47 states and the District of Columbia had enacted UETA. Illinois, New York, and Washington have not adopted UETA, but have enacted some form of law governing e-signatures.

which may be applicable to commercial, consumer, or governmental affairs transactions involving federal organizations in certain cases.[10]

Which E-Transaction Law will apply to any particular transaction involving a federal organization will depend on the nature of the transaction. Whether a particular electronic transaction by a federal organization is covered by GPEA, E-SIGN, and/or UETA can be a "complicated question."[11] Thus, federal organizations should consult with their legal counsel as necessary when questions arise regarding applicability of a specific E-Transaction Law, and its impact on the guidance provided here.

Nonetheless, while there are some differences in the electronic signature requirements of each of these E-Transaction Laws, they are all generally consistent.[12] The guidance set forth here is designed to address electronic signature requirements in a manner that satisfies the requirements of all of the E-Transaction Laws.

3. Legal Approach to Electronic Signatures

The E-Transaction Laws establish the general principle that a signature may not be denied legal effect, validity, or enforceability solely because it is in electronic form.[13] They also specify the requirements that must be satisfied to create an electronic signature that is considered equivalent to a handwritten signature. Of course all signatures, both paper and electronic, are subject to challenge for other reasons, such as claims of mistake, forgery, duress, etc. And the E-Transaction Laws do not require the use of an electronic signature in most cases.[14] It is up to the participants to determine the value of any particular transaction and, therefore, what level of security is required to reduce the risk of malfeasance or fraud.

[10] See E-SIGN, 15 U.S.C. § 7002.

[11] OMB M-00-15, at p. 14.

[12] See, e.g., OMB M-00-10, (noting that the definition of electronic signature in GPEA "is consistent with other accepted legal definitions of signature" and that UETA "contains a similar definition"). Note also that, the electronic signature requirements of E-SIGN and UETA are virtually identical.

[13] GPEA Section 1707; E-SIGN, 15 U.S.C. § 7001(a); UETA Section 7(a). UETA also expressly states that "If a law requires a signature, an electronic signature satisfies the law." UETA Section 7(d). According to the comments, this is just "a particularized application" of Section 7(a). UETA Section 7, Comment 3.

[14] See UETA Section 5(a) ("This [Act] does not require a record or signature to be created, generated, sent, communicated, received, stored, or otherwise processed or used by electronic means or in electronic form"); E-SIGN 15 U.S.C. § 7001(b)(2) ("This title does not . . . require any person to agree to use or accept electronic records or electronic signatures, other than a governmental agency with respect to a record other than a contract to which it is a party"); and OMB M-00-10 (which indicates that GPEA does not require a federal organization to accept electronic records or signatures where it determines that using electronic mechanisms is not feasible).

(a) Functional Equivalence

The E-Transaction Laws essentially answer the basic question: If a law requires a "signature," how can an electronic transaction satisfy that requirement? They do this by adopting what is referred to as the "functional equivalence approach" with respect to electronic signatures. This approach considers the purposes and functions of the traditional paper-based requirement for a signature, and specifies how those purposes or functions could be fulfilled in an electronic context. The goal is to specify criteria which, once met by an electronic signature, enable such electronic signature to enjoy the same level of legal recognition as a corresponding handwritten signature.

Thus, the E-Transaction Laws set forth the requirements that must be satisfied by an electronic signature to establish functional equivalence to the paper-based requirement for a "signature." In adopting this approach, they reject the notion that the concept of functional equivalence requires imposing on users of electronic signatures more stringent standards of security than required for handwritten or other forms of signatures in a paper-based environment. This functional equivalence approach also allows enforcement of electronic signatures in accordance with existing laws without requiring the wholesale removal of the paper-based requirements themselves or disturbing the legal concepts and approaches underlying those requirements.

(b) Technology Neutrality

In addressing the requirements for electronic signatures, the E-Transaction Laws also adopt the principle of "technology neutrality." This principle holds that the law should not discriminate between different forms of technology (i.e., the rules should neither require nor assume a particular technology).[15] The goal of technology neutrality is important from the standpoint of not stifling development of any technology or unfairly favoring one technology over another. Thus, GPEA, E-SIGN, and UETA adopt "neutral" requirements for electronic signatures; that is, they neither require nor presuppose the use of particular types of technology and can be applied to the signing of all electronic records regardless of the technology used.

4. Electronic Signatures Compared to Digital Signatures

The core concern of the E-Transaction Laws is: (1) electronic documents, referred to as "records" or "electronic records," and (2) "signatures" that are created, communicated, and stored in electronic form.[16] The E-Transaction Laws refer to these

[15] This does not necessarily mean, however, that all technologies will be acceptable in all cases. But by specifying requirements rather than specific technologies, GPEA, E-SIGN and UETA all seek to maximize freedom of choice in selecting among current and future appropriate technologies. See also, OMB M-00-10 noting that "the final guidance maintains the basic policy of technology neutrality for automated transactions while recognizing that agencies should select an alternative relative to the risk of the application, and calls on agencies to consider all of the available electronic signature technologies (including the advantages of public key technology) as part of their assessments."

[16] The formal definitions of the terms "electronic," "record," "electronic record," and "electronic signature," as set forth in the E-Transaction Laws and as used in this memo, are set out in the Glossary (Part F).

signatures as "electronic signatures." However, the common use of another term -- "digital signature" – has created considerable confusion. Thus, it is important to understand these terms as they relate to the legislation:

- "*Electronic signature*" is the term used in all of the E-Transaction Laws for the electronic equivalent of a handwritten signature. It is a generic, technology-neutral term that refers to the universe of all of the various methods by which one can "sign" an electronic record. Although all electronic signatures are represented digitally (i.e., as a series of ones and zeroes), they can take many forms and can be created by many different technologies. Examples of various forms of electronic signatures are noted in Section D.1 below.

- "*Digital signature*" is the term used to describe the small segment of encrypted data produced when a specific mathematical process (involving a hash algorithm and public key cryptography) is applied to an electronic record.

  The digital signature can be created in a manner so that it can be used to authenticate the identity of the person who created the digital signature, and/or to verify the integrity of the electronic record on which the digital signature is based. The encrypted data constituting the digital signature, like other electronic forms of signature *can also be applied* as a legally binding electronic signature, provided it is used in a manner that satisfies all of the requirements for a legally binding electronic signature outlined in Part D below. In fact, like any other electronic form of signature, a digital signature is not a legally binding electronic signature *per se* (notwithstanding its name), although it has properties that make it particularly well suited for use as a legally binding electronic signature where it is expressly intended for that purpose.

  Thus the encrypted data constituting the digital signature is sometimes used as a legally binding electronic signature, is sometimes used as part of a process to authenticate a person or device, is sometimes used to verify the integrity of the record, and is sometimes used for all three purposes. The term "digital signature" is not, however, used in the E-Transaction Laws, given that those laws are technology neutral and digital signatures are technology driven. Where a digital signature is intended to be used as a legally binding signature, it is simply considered to be one form of an electronic signature.

Basically, any sound, symbol or process, including a digital signature, *can* qualify as a legally binding electronic signature, provided it satisfies all of the requirements for a valid electronic signature outlined in Part D below. In some cases a sound, symbol or process is used only as a social, identification, or security procedure (with no legal signing impact), whereas in other cases it is used in the context of a signing process and may be legally binding. <u>But in all cases it is important to recognize that the mere fact that the term "electronic" or "digital" appears before the word "signature" does not automatically bestow on it any legal significance. A sound, symbol or process (including</u>

a digital signature) will not qualify as a legally binding electronic signature under the E-Transaction Laws unless it is applied in a manner that satisfies all of the requirements for a valid electronic signature outlined in Part D below.

5. Relationship between an Electronic Signature, a Security Procedure, and a Signing Process

It is important to distinguish an electronic *form of signature* (i.e., the sound, symbol, or process that comprises one of the five requirements for a valid electronic signature outlined in Part D below) from an indication of identity in a business or social setting or a *security procedure*, and to understand the concept of a *signing process* which may incorporate each. While they are all related, and sometimes can be somewhat interchangeable, at their core they are different concepts and must be treated accordingly.

An electronic signature is used to indicate a person's intent to associate himself in some way to information or to a reason for signing (e.g., agreeing to the terms of a contract, acknowledging receipt of information, etc.) with legal effect. As discussed in Section D.1 below, any sound, symbol, or process that is made or adopted by a person with intent to sign a document can be used as the **form of signature** for purposes of creating an electronic signature. This includes, for example, a typed name, clicking on an "I Agree" button, or a cryptographically created digital signature. But the mere use of any such sound, symbol, or process does not necessarily create a legally binding electronic signature. Thus, for example, one can type a name, or click a button, or apply a cryptographically created digital signature for many reasons having nothing to do with an electronic signature. None of the foregoing symbols or processes is, *per se*, an electronic signature. It is only when such symbols or processes meet the other requirements for a legally binding electronic signature outlined in Part D below that it constitutes an electronic signature.

A **security procedure**, by contrast, is employed for the purpose of verifying that an electronic record, signature, or performance is that of a specific person (attribution) or for detecting changes or errors in the information in an electronic record (integrity), among other purposes.[17] As described above, a digital signature is frequently used as part of a security procedure where the digital signature is applied automatically. But note that, in some cases a digital signature can be used as both a security procedure and as a legally binding form of signature (e.g., as a *process* made or adopted by a person with intent to sign a document). Thus, it is important that the context make clear whether the digital signature was intended merely for purposes of attribution and/or integrity, or whether it was also intended to be a legally binding electronic signature.

In many cases, a particular technology or process can be used as an electronic form of signature, as a security procedure, or as both at the same time. For example, a handwritten name can be used at the top of a lengthy paper contract to identify a party,

[17] See, e.g., UETA Section 2(14).

at the end of the contract as that party's signature agreeing to its terms, and at the bottom of each page to help verify the integrity of the document. Similarly, a digital signature can be used to increase the security by providing the identity of a person seeking access to a network or sending an email, the integrity of an electronic record, or as the form of signature for purposes of signing an electronic record. In some cases it is used for all three of these purposes, whereas in other cases it is used for only one or two of these purposes.

A **signing process** is the overall set of actions, steps, and elements that is used to create a valid and enforceable electronic signature, and includes both the application to an electronic record of a form of signature (i.e., the sound, symbol, or process) to be used as the electronic signature, and one or more processes or security procedures to address the other signature requirements listed in Part D below (including identifying and authenticating the signer and ensuring integrity of the electronic record). While some forms of electronic signature can directly address those security requirements, some of those requirements can also be met by the use of independent security procedures or through other means separate from the form of electronic signature used.

A security procedure can be used either as part of the signing process, or in a manner unrelated to any signing process. As noted above, when used as part of the signing process, a security procedure can be used as the form of signature, as another part of the signing process, or as both. For example, within the process for signing a contract, a security procedure might be used as the form of signature (Requirement D.1 below), as a method to identify and authenticate the signer (Requirement D.4 below), as a method to verify the integrity of the signed record (Requirement D.5 below), or as all three. Conversely, outside of the signing process, the same security procedure might be used to verify the integrity of a draft contract, or to verify the identity of the person who sent a draft contract, even though such person is not legally bound to the terms of the contract because he or she has not yet signed it.

Currently, the digital signature might be the best example of a process that can be used in such a variety of ways. A digital signature is often used to provide a security procedure for identification and authentication of a party, and/or ensuring the integrity of an electronic record in situations that do not involve a signature of any type. But it can also be used as part of a signing process, in one of two different ways. First, a digital signature might be used as part of the signing process in conjunction with a separate electronic form of signature, such as clicking a button or typing one's name. In such a case, the digital signature is not used as the form of signature in the legal sense, but rather is a security procedure that is used to satisfy the identification and authentication requirements and the record integrity requirements of a signing process that uses a different form of signature (e.g., clicking an "I Agree" button). Alternatively, a digital signature might be used as both the form of signature itself and as the means to satisfy the identification and authentication requirements and the record integrity requirements of the signing process.

Accordingly, it is important to distinguish between the use of a technology or process as a form of signature, and the use of that same technology or process to satisfy some security requirement applicable to a transaction but unrelated to a legally binding signature. Where security is critical to an electronic transaction, such security can be provided via the use of certain electronic forms of signature, or by other means, i.e., there is no requirement that security be provided by the form of signature itself. Moreover, the need for security does not necessarily translate into the need for an electronic signature.

6. Impact of Enabling Automatic Digital Signing with PIN Caching

Some federal organizations implement a process whereby a digital signature is automatically applied to all emails and other messages when they are sent out. This is done as a security procedure to identify the sender and to ensure that the integrity of the message can be verified by the recipient, and typically is not intended to be a legally binding electronic signature.

In such cases, access to the system is restricted by a two-factor authentication process, requiring the user to insert his or her smart card (e.g., PIV or CAC card) into the device and enter the PIN associated with that card to activate it. Once the smart card is inserted into the device, and the proper PIN entered, the system will allow PIN caching for a limited period of time (in accordance with a defined security policy) thereby allowing the system to automatically apply a digital signature to each email sent during a defined time period. The purpose of such a PIN caching service is to enable users to use the smart card without entering the PIN for every card operation (e.g., every email sent out), while preserving the security of the smart card solution.

The end result is that for a pre-determined period of time after the smart card is inserted and the PIN properly entered, the system will automatically apply a cryptographic digital signature process to every email the user sends out, regardless of the content of the email, and without the need for the user to reenter his or her PIN to initiate the process.

Federal organizations that use such processes should pay close attention to the need to distinguish between the standard use of the PIN-cache-enabled digital signature as a security procedure, and the occasional need to use the PIN-cache-enabled digital signature as the form of signature for a legal electronic signature. Because the PIN caching process described above facilitates the automatic application of a digital signature, it is unlikely that the requisite intent will normally be present to render such digital signature as a legally binding electronic signature.[18]

[18] The intention with which a symbol is made is critical to determining whether or not it qualifies as a signature. Thus, for example, when a fax machine is programmed to automatically include the originating sender's name, phone number, date and time at the top of each faxed page, such symbols would in most cases not qualify as a signature, since they are automatically created by the fax machine that sends them, and thus are not appended to a specific message by the sender with intent to sign same. See, for example, *Parma Tile Mosaic & Marble Co. v. Estate of Fred Short 2 No. 20*, 87 N.Y.2d 524, 663 N.E.2d 633 (N.Y. Ct. App., 1996). See discussion regarding the intent requirement in Part D.2 below.

Thus, it is recommended that federal organizations note the following:

- For those situations where PIN caching is used to facilitate the automatic application of digital signatures to all e-mail messages solely as a security procedure to identify the sender and to ensure that the integrity of the message can be verified by the recipient (i.e., where the digital signature is NOT intended to be a legally binding electronic signature), it is important that the information received by the recipient (or as viewed by a subsequent third party) not appear as if the digital signature was applied with the intent to a legally binding electronic signature.

- For those situations where the digital signing process is intended to be used as a legally binding electronic signature:

    - From the sender's perspective it is important to build into the applicable signing process an additional step to alert the sender to the need for a legally binding signature and to appropriately evidence the sender's intent that the application of the digital signature constitutes a legally binding signature. This can be accomplished, for example, through the use of a pop-up box notifying the sender that a legally binding signature is required, and the use of a check box whereby the sender indicates his or her intent to use a digital signature to legally sign the communication; and
    - From the recipient's perspective, it is important that the document received makes clear that the digital signature applied to that document is intended as a legally binding signature (and not just as a security procedure, as in most cases). This might be accomplished, for example, on a PDF document through the use of (i) a standard signature line in conjunction with text evidencing intent (such as "I agree to the foregoing"), and (ii) text appearing on that signature line when the document is viewed indicating that the document was digitally signed by a certain person on a certain date and time.

- Another approach to help distinguish the use of a digital signature for security purposes from the use of a digital signature as a legally enforceable electronic signature is to include two cryptographic keys (ideally with two different PINs) on the sender's PIV or CAC card – one key for digitally signing the record solely for security purposes (e.g., the PIN-cached automatic process), and the other key for digitally signing the record as a form of signature used to create an electronic signature (e.g., via an additional step to alert the sender to the need for a legally binding signature and to appropriately evidence the sender's intent that the application of the digital signature constitute a legally binding signature).

- In addition, whenever PIN caching is used along with a mechanism (such as the pop-up box described above) to indicate that the digital signature is intended to be a legally binding signature, the parties must recognize that the PIN caching

process can facilitate another person (e.g., an assistant) signing the document in the name of the person whose digital signature is applied. This might occur, for example, if the person whose PIN is cached steps away from the machine for a few minutes but leaves his or her smart card inserted in the machine. Federal organizations should understand that in such case applicable law may hold the named signer responsible for the signature, even if it was unauthorized, but this remains to be adjudicated. Accordingly, appropriate education, training, and policies should be put in place to minimize the risk of such an occurrence. Furthermore, having PINs cached on a network may raise the risk of cyber attack and if implemented poorly reduces the security of the system.

In all cases, it is important that a digital signature (or other form of signature used as a security procedure) not be confused for a legally binding electronic signature where no signature was intended, or conversely, that it not be interpreted as merely a security procedure with no legal signing effect where in fact a legally binding electronic signature was intended.

C. DETERMINING WHETHER AN ELECTRONIC SIGNATURE IS NECESSARY

When evaluating whether an electronic signature is required for any particular federal organization transaction, it is important to clarify the scope of the question. The issue is determining whether an electronic signature is required or recommended for the purpose of legally binding an individual to the transaction (such as when a person requests the electronic deposit of Social Security Administration (SSA) benefits into a specific bank account). This section will outline the factors that federal organizations should consider in determining whether a legally enforceable electronic signature is necessary.

1. Legal Requirement for a Signature

In many cases, a transaction is governed by a law or regulation that requires the presence of a signature before it will be considered legally effective. In fact, there are thousands of federal, state, and local statutes and regulations that require certain types of transactions to be "signed." The statute of frauds (which requires contracts for the sale of goods in excess of $500 to be "signed") is a good example of such a law. Likewise, the Federal Acquisition Regulations (FAR) require the signature of a contracting officer on contracts made on behalf of the United States.[19]

Thus, as a first step, federal organizations must review the law applicable to each proposed transaction to determine if it requires that the transaction be "signed." If the applicable law or regulation requires a signature, then to conduct the transaction in electronic form requires an electronic signature.

2. Transaction-Based Need for a Signature

If there is no legal requirement for a signature on a particular type of transaction, it is recommended that federal organizations undertake a further analysis to evaluate the desirability of nonetheless incorporating a signature requirement into the transaction. An electronic signature may be desirable, even when not legally required, where there is a:

- Need for Emphasizing the Seriousness of the Transaction. In many cases, a signature serves to reinforce the significance of the undertaking to the party involved. It gives the transaction a more formal tone, and helps to drive home to the signing party the seriousness of what is being undertaken. In essence, it performs a cautionary function. For example, in the case of a commercial contract under $500 (which can be legally binding without a signature under common law), while it is clear that a party need not read the contract terms in order to be bound by them, it is also helpful to give such party some signal that he is entering into a legally binding transaction so that he knows to read

[19] See Federal Acquisition Regulations Section 4.101 ("Only contracting officers shall sign contracts on behalf of the United States.")

the offered terms. A signature provides that signal. The same can be said for a document used by a person to provide information to a government agency, such as a tax return or a passport application. Thus, requiring a signature provides a signal to the persons filling out such form that the document in front of them is important and that they should be cautious about agreeing to it.[20]

- Need for Binding a Party to the Transaction. If the transaction involves an intent element (e.g., agreement, approval, acknowledgment, receipt, witnessing, etc.), a signature may be useful to help formally bind a person to that reason for signing and make it more likely to be enforced – e.g., to mitigate concerns regarding repudiation. Likewise, where there is a risk of fraud, a signature might be useful for enforcing enhanced criminal penalties. Thus, where evidence of a party's intent is important to the transaction, a signature can provide evidence of deliberation and informed consent.

Where either of these needs is present,[21] it is important to consider the significance of the transaction to determine whether an electronic signature is necessary to satisfy these needs. See Section E.2 (Risk Analysis) below.

*** * ***

The analysis for determining whether an electronic signature is necessary for an electronic transaction is summarized in Table C-1.

Table C-1 Determining Whether an E-Signature is Necessary

	Signature Required by Law or Regulation Governing Transaction	**Signature NOT Required by Law or Regulation**
There is a Need for Emphasizing the Seriousness of the Transaction	Electronic Signature Required	Electronic Signature Recommended
There is a Need to Bind a Party to a Specific Intent Transaction	Electronic Signature Required	Electronic Signature Recommended
All Other Transactions	Electronic Signature Required	Electronic Signature Not Needed

[20] See, e.g., Robert A. Hillman & Jeffrey J. Rachlinsk, Standard-Form Contracting in the Electronic Age, 77 N.Y.U.L. Rev. 429 (May 2002), at p. 481.

[21] Note, however, that a requirement to authenticate the identity of a party, or to ensure the integrity of the electronic record, does not necessarily mandate the use of an electronic signature. These are requirements for security that can be addressed by a variety of security procedures. For example, allowing someone to access their Social Security records requires authenticating their identity, but does not require a signature.

D. REQUIREMENTS FOR LEGALLY BINDING ELECTRONIC SIGNATURES

Where an electronic signature is required by law or otherwise deemed desirable, it is critical that the electronic signature and the associated signing process satisfy all of the applicable legal requirements.

Those legal requirements are derived from a combination of the E-Transaction Laws and applicable evidentiary requirements for admissibility, and are intended to ensure that the electronic signature is functionally equivalent to a handwritten signature. The statutory requirements for an electronic signature vary slightly among the E-Transaction Laws[22] but are essentially equivalent.[23] This section will set forth requirements for the signing process that will satisfy all of the E-Transaction Laws. Generally, when the statutory requirements are combined with the overall evidentiary requirements it becomes clear that creating a valid and enforceable electronic signature requires satisfying the following signing requirements:

1. A person (i.e., the signer) must use an acceptable electronic ***form of signature***;
2. The electronic form of signature must be executed or adopted by a person with the ***intent to sign*** the electronic record, (e.g., to indicate a person's approval of the information contained in the electronic record);
3. The electronic form of ***signature must be attached to or associated with the electronic record*** being signed;
4. There must be a means to ***identify and authenticate*** a particular person as ***the signer***; and
5. There must be a means to preserve the ***integrity of the signed record***.

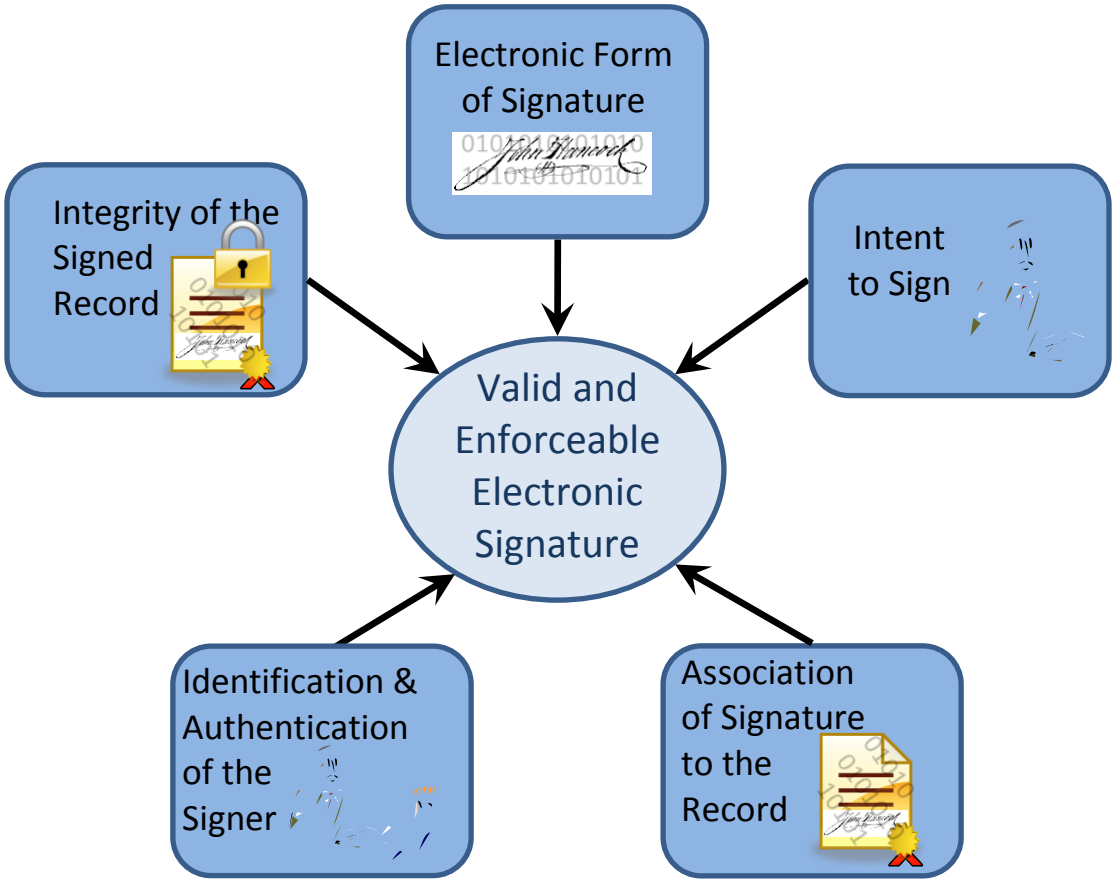
Because electronic signatures are functionally equivalent to handwritten signatures, these requirements are not unique to electronic signatures and also apply to handwritten signatures on paper documents.

---

[22] GPEA defines an electronic signature as "a method of signing an electronic message that-- (A) identifies and authenticates a particular person as the source of the electronic message; and (B) indicates such person's approval of the information contained in the electronic message." GPEA (Section 1710). E-SIGN defines an electronic signature as "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" E-SIGN, 15 U.S.C. § 7006(5), and the definition in UETA is virtually identical. UETA § 2(8).

[23] Both GPEA and E-SIGN/UETA are similar and consistent. See, e.g., Office of Management and Budget Memorandum M-00-10, Implementation of the Government Paperwork Elimination Act, April 25, 2000, (noting that the definition of electronic signature in GPEA "is consistent with other accepted legal definitions of signature" and that UETA "contains a similar definition").

Figure D-1 Requirements for Legally Binding Electronic Signatures



Taken together, the five signing requirements listed above must be ***as reliable as is appropriate*** for the purpose of the transaction.[24] (See Part E)

Satisfying the signing requirements outlined above requires the use of a signing process[25] that may involve multiple steps, processes, or procedures. As noted in Section B.5 above, in some cases the electronic form of signature that is used can satisfy most of these requirements,[26] whereas in other cases additional security procedures and processes must be used to ensure that all of the signing requirements are addressed.[27] Thus for example, while the overall signing process must identify and

[24] GPEA at Section 1703(b)(1)(C). See also OMB M-00-10, (noting that OMB must "develop procedures for Executive agencies to follow in using and accepting electronic documents and signatures . . . with due consideration of . . . ensuring that electronic signatures are as reliable as appropriate for the purpose in question").

[25] GPEA uses the term "method of signing" to refer to this signing process.

[26] Although no electronic form of signature can satisfy all of these requirements.

[27] The GPEA requirement for a "method of signing," for example, recognizes that the signing process can include the use of multiple steps, processes, or procedures. Thus, while GPEA requires that the method

authenticate the person signing, the specific symbol used as the electronic form of signature need not do so, as long as the issue is addressed by some portion of the overall process.

This is particularly noteworthy, because it allows separating from each other the means by which the various requirements for functional equivalence with a handwritten signature are satisfied, and thereby greatly enhances the flexibility of the federal organizations with regard to approaches that will satisfy the signing requirements. Thus, for example, a party might log into a system using a very secure process to verify his or her identity (such as a PIV card public key encryption process), and then use a separate and very different process (such as clicking on an "I Agree" button) as the electronic form of signature to indicate his or her approval. So long as the overall signing process sufficiently links the two activities, it addresses the requirement to identify and authenticate a specific person as the source of the signature.

1. Electronic Form of Signature

In a paper-based transaction, the most commonly used form of signature is a person's name, written with ink and in their own handwriting. But many other forms of signature are also acceptable for signing paper documents. These include a typewritten name;[28] initials;[29] a firm's name printed on a confirmation statement;[30] a name on letterhead;[31] a faxed signature;[32] and use of an account number as an endorsement on

---

of signing must both (i) identify and authenticate a particular person as the source of the electronic message, and (ii) indicate such person's approval of the information contained in the electronic message (discussed below), GPEA does not require that these two signature requirements be satisfied by a single set of data or a single electronic form of signature, or accomplished in the same step of the method. Stated differently, the focus of GPEA on a *method* (rather than an *object or item* that constitutes an electronic form of signature) implies that the step (or process) of identifying and authenticating the party, and the step (or process) of indicating the party's approval, can be separated (even though they may be viewed as part of an overall method) – e.g., they need not be part of the data element comprising the electronic form of signature itself.

[28] See, e.g., *Benedict v. Lebowitz*, 346 F.2d 120 (2nd Cir. 1965) (typed name); *Hillstrom v. Gosnay,* 188 Mont. 388, 614 P.2d 466 (1989) (name typed on telegram); *Franklin County Coop. v. MFC Services*, 441 So.2d 1376 (Miss. 1983); *Hideca Petroleum Corp v. Tampimac Oil Int'l Ltd.,* 740 S.W.2d 838 (Tex. Ct. App. 1987) (name typed on telex); *Watson v. Tom Growney Equip. Inc.,* 721 P.2d 1302 (N.M. 1986) (name typed on a purchase order); *Matter of Save On Carpet of Arizona, Inc.,* 545 F.2d 1239 (9th Cir. 1976) (typewritten name on a UCC financing statement); *A & G Const. Co. v. Reid Bros. Logging Co.,* 547 P.2d 1207 (Alaska 1976) (typed name); *Hesenthaler v. Farzin*, 388 Pa. Super 37 (1989); *McMillan Ltd v. Warrior Drilling & Eng Co.,* 512 So. 2d 14 (Ala. 1986) (name on Western Union Mailgram). See also 71 Comp. Gen. 109 (No. B-245714, December 13, 1991).

[29] Ohl & Co. v. Smith Iron Works, 288 U.S. 170, 176 (1932), as cited in 71 Comp. Gen. 109 (No. B-245714, December 13, 1991).

[30] *Kohlmeyer & Co. v. Bowen*, 126 Ga. App. 700, 192 S.E.2d 400 (1972) (court found that securities brokerage firm's name printed on a confirmation statement for the sale of securities was intended as authentication, and met the signature requirement under the statute of frauds).

[31] *Associated Hardware Supply Co. v. Big Wheel Distrib. Co.,* 355 F.2d 114 (3d Cir. 1966).

[32] *Bogue v. Sizemore,* 241 Ill.App.3d 250, 608 N.E.2d 1246 (4th Dist. 1993); *Madden v. Hegadon*, 565 A.2d 725 (N.J. Super. 1989), ***aff'd*** 571 A.2d 296 (N.J. 1989).

a check.[33] As early as 1951, the Comptroller General of the United States recognized that a signature does not have to be handwritten and that "any symbol adopted as one's signature when affixed with his knowledge and consent is a binding and legal signature."[34]

The E-Transaction Laws similarly recognize that electronic signatures can take many forms, and can be created by many different technologies.[35] No specific technology or form of signature is required. Generally, any electronic "sound, symbol, or process" can be used as the form of signature,[36] so long as the signing process satisfies the other requirements identified above and further described in Sections 2 - 5 below. Examples of commonly used electronic forms of signature include:[37]

- Symbols such as –
  - A typed name (e.g., typed at the end of an e-mail message by the sender, or typed into a signature block on a website form by a party);[38]
  - A digitized image of a handwritten signature that is attached to an electronic record;
  - A shared secret (e.g., a secret code, password, or PIN[39]) used by a person to sign the electronic record;
  - A unique biometrics-based identifier, such as a fingerprint, voice print, or a retinal scan; or
  - A digital signature;[40]
- Sounds such as –
  - A sound recording of a person's voice expressing consent;

---

[33] *Spevak, Cameron & Boyd v. National Community Bank Of New Jersey,* 291 N.J. Super. 577, 677 A.2d 1168 (App. Div. 1996) (According to the court, "in this computer age the use of numbers as a means of identification has become pervasive. Indeed, numbers are more readily recognized and handled than signatures.")

[34] 71 Comp. Gen. 109 (No. B-245714, December 13, 1991) (citing to B-104590, Sept. 12, 1951).

[35] See, e.g., OMB M-00-10, (noting that "These flexible definitions permit the use of different electronic signature technologies, such as digital signatures, personal identifying numbers, and biometrics.").

[36] E-SIGN and UETA require a "sound, symbol, or process;" GPEA requires a "method of signing."

[37] Note that GPEA requires OMB to "develop procedures for the use and acceptance of electronic signatures by Executive agencies" and that such procedures "shall be compatible with standards and technology for electronic signatures that are generally used in commerce and industry and by State governments."

[38] See, e.g., *Stevens v. Publicis*, S.A., 50 A.D.3d 253, 854 N.Y.S.2d 690, 2008 N.Y. App. Div. LEXIS 2834 (N.Y. App., 2008)**;** *Polyad Company, v. Indopco Inc*., 2007 U.S. Dist. LEXIS 71925 (N.D. Ill. Sept. 25, 2007); *Rosenfeld v. Zern*, 2004 N.Y. Slip Op. 24143 (2004); *Shattuck v. Klotzbach*, 2001 Mass. Super. LEXIS 642 (December 11, 2001)

[39] See, e.g., *United States v. Miller,* 70 F.3d 1353, 1355 (D.C. Cir. 1995), (Court held that unauthorized use of a PIN number to withdraw funds from an ATM machine was forgery, because such unauthorized use of the PIN number was "tantamount to cashing a check with a forged signature.")

[40] See 71 Comp. Gen. 109 (No. B-245714, December 13, 1991) (approving use of digital signatures).

- Processes such as –
  - The process of using a mouse to click a button (such as clicking an "I Agree" button);[41]
  - The process of using a private key and applicable software to apply a "digital signature;" or
  - The process of scanning and applying a fingerprint.

This is not an exhaustive list of the forms of signature that one can use to electronically sign a record. But it illustrates the variety of options available for use as the electronic form of signature.[42]

2. Intent to Sign

In electronic transactions, merely applying a sound, symbol, or process that is commonly used as a form of signature does not make it a legally binding signature. It must be applied with intent to sign.

In paper-based transactions, there are many situations in which someone might write his or her name in ink. These include, for example, identifying oneself (e.g., when filling out a form requiring name and address), adding one's name to a list, and making a legal commitment (e.g., when agreeing to a contract). Whether a handwritten name appearing in ink on any particular document constitutes a legally binding signature depends on whether it was made with the intent to sign.

The same requirement exists in the case of an electronic signature. That is, in order for an electronic form of signature (i.e., a sound, symbol, or process) to be legally effective as an electronic signature, it must be executed or adopted by the signer with an intent to sign.[43] Intent is the critical component of any legally binding signature.[44]

---

[41] By including the term "process" as part of the definition of an electronic signature, both E-SIGN and UETA make clear that the "process" of clicking a mouse can qualify as a signature if the other applicable requirements are also present. As noted in the Reporter's notes to UETA, "this definition includes as an electronic signature the standard Webpage click-through process. For example, when a person orders goods or services through a vendor's web site, the person will be required to provide information as part of a process which will result in receipt of the goods or services. When the customer ultimately gets to the last step and clicks "I agree," the person has adopted the process and has done so with the intent to associate the person with all the record of that process." UETA § 2, comment 7.

[42] More detailed information regarding some of the foregoing electronic forms of signature can be found at OMB M-00-10.

[43] E-SIGN and UETA expressly require that the signer execute or adopt the sound, symbol, or process with the *intent to sign* the record. GPEA requires that the method of signing indicate the signer's "*approval of the information contained in the electronic message*." These requirements are essentially identical, however, as the intent to use a particular symbol as a signature (under E-SIGN) is the same as using a particular symbol to indicate one's approval of information contained in a document (under GPEA) – i.e., indicating one's approval of information in a document is accomplished by a signature.

[44] See *Buckles Management LLC. V InvestorDigs, LLC.,* 2010 U.S. Dist. LEXIS 73000, *13 (D. Col. July 20, 2010) (holding that electronic record was not signed where the alleged signature was not "executed or adopted by a person with the intent to sign the record"). See also, *Pepco Energy Services, Inc. v. Geiringer,* 2010 U.S. Dist. LEXIS 4651, 2010 WL 318284 (E.D. N.Y. 2010) (ruling that under E-SIGN, 15

The intent requirement recognizes that the act of applying a sound, symbol or process to an electronic record could have differing meanings and effects. For example, one might type his or her name on a website in order to fill out an application form, to provide shipping information, or to agree to the terms of a contract. Merely applying a person's name, a digital signature, or any other sound, symbol, or process to an electronic record does not necessarily qualify it as a legally-binding signature. Whether that sound, symbol, or process is an electronic signature, a security procedure, or just a data element depends on the intent of the person who applied it. The essential attribute of a signature involves applying a sound, symbol or process with an intent to do a legally significant act.[45]

Intent to Sign vs. Reason for Signing. When designing a signing process to evidence an intent to sign, it is important to distinguish "intent to sign" from the "reason for signing" (which can vary from one transaction to another). The reason someone signs a document is typically stated in the document itself (such as in a statement right above the signature line) or as part of the process by which the signing occurs (such as a statement on a web page). Reasons for signing can include, for example: to signify agreement to be bound to the terms of a contract, to certify the truth of the statements made in the document, to approve or authorize an activity, to attest to the act of signing by a party to the transaction, to confirm that the signer has read and reviewed the contents of a document, to indicate that the signer was the author of a document, or to certify that the contents of a document have been shown to the signer and that he or she has had an opportunity to review them. But whatever the reason for signing, the sound, symbol or process used to indicate agreement to or approval of that reason must be applied with intent to sign the record."[46]

While intent to sign and reason for signing are distinct, a signing process must be able to provide documentation demonstrating both. The reason for signing is typically

---

U.S.C. § 7006(5), the parties' intent is crucial, and where there was ample evidence that the sender did not intend for the attached letter to be "executed" by virtue of his including his name on the email itself, the typed name on the email was deemed to not be equivalent to a signature).

[45] See, e.g., UETA, Section 2, Comment 7. See also *Parma Tile Mosaic & Marble Co. v. Estate of Fred Short 2 No. 20*, 1996 WL 73828 (N.Y. Ct. App. Fed. 20, 1996) (holding that a sender's phone number (i.e., a symbol) appended to a faxed document *could* qualify as a signature, but that under the facts of that case, it was not a signature since it was automatically applied by the fax machine that sent the fax, and was not appended by the sender with *intent* to sign the particular fax in issue); and *Kohlmeyer & Co. v. Bowen*, 126 Ga. App. 700, 192 S.E.2d 400 (1972) (holding that where a securities brokerage firm's name was printed on a confirmation statement for the sale of securities, the printed name was intended as authentication, and met the signature requirement under the statute of frauds).

[46] E-SIGN, 15 U.S.C. 7006(5); UETA Section 2(8); GPEA Section 1710(1). GPEA expresses this intent to sign requirements as a requirement that the method of signing must indicate "such person's approval of the information contained in the electronic message." This is, in effect, a requirement to approve the statement of the reason for signing set forth in the document – e.g., to approve a statement such as "I agree to the contract," "I acknowledge receipt of the document," or "the statements in the document are true and correct." It is another way of requiring intent to sign (with the reason for signing being set forth in the information being approved).

demonstrated by the content of the document and any corresponding attestations/certifications/warnings. For example, where the reason for signing is to acknowledge receipt, that reason might be evidenced by text in the document stating "By signing I acknowledge receipt of a copy of this document," or by text on a webpage stating "Click 'Sign' to acknowledge receipt of a copy of this document." Intent to sign, on the other hand, is usually demonstrated by the signing process itself – often the act of applying the requested signature in the context of the stated reason.

Evidencing Intent to Sign. The existence of intent to sign is determined based on what a signer would have reasonably believed under the circumstances when the electronic form of signature was applied, assuming that he or she was not being coerced.

A person's intent to sign is often inferred from his or her approval of the ***reason for signing*** as stated in the text of either: (i) the electronic record being signed or (ii) the surrounding signing process. For example, words appearing immediately above a blank signature line on a draft contract document might state "By signing below I agree to the foregoing contract terms." That statement indicates both the reason for signing (agreement to the contract) as well as the means by which a person can indicate an intent to sign (i.e., by applying the form of signature where indicated). Thus, a person indicates his or her intention to sign, for the reason stated, by signing on the applicable blank line. Likewise, text on a website might state that "By checking this box I agree to the terms of use." A person indicates his or her intention to sign, for the reason stated, by checking the box on the website.

As with a handwritten signature, the sound, symbol, or process that is used as the electronic form of signature typically does not, by itself, indicate any intent to sign.[47] Thus, it is important that the record, and/or process by which a person applies an electronic form of signature to the record, be designed to indicate the means by which the signer can indicate his or her intent to sign the record. This is usually accomplished by the context in which the form of signature is applied, such as by the words that precede the signature in the document and set forth the conduct that will evidence an intent to sign – e.g., a line labeled "Signature," website text stating "click to agree," or a variety of other approaches. It requires making clear to persons that they are being asked to sign a record – i.e., to engage in an act that has legal significance – and specifying or implying the conduct that will evidence that intent to sign.

In most cases, such intent to sign can be determined only by looking at the context in which the form of signature was made. For example, a person filling out an online tax return might type his name twice: First, at the top of the form to identify the person filing the tax return, and second, at the bottom of the form to certify, under penalty of perjury, that he has examined the return and accompanying schedules and statements, and that to the best of his knowledge and belief, they are true, correct, and

[47] An exception might be a voice signature wherein the signer recites intent to sign by stating the reason for signing – e.g., "I agree to this contract" or "I approve this expenditure).

complete. Both entries are identical, but the certification preceding the second entry establishes the intent to sign that makes clear that it is a signature.

Process to Establish Intent. Designing a signature process that establishes the intent to sign can be done through a variety of methods that provide a clear and conspicuous notice that a signature is being created and that it will be legally binding. Such notice information should be provided prior to signing and should include a description of the signature process, a clear statement of the reason for signing, and a statement that when completed it will constitute the signer's legally binding signature. The reason for signing can be set forth in the text of the document being signed (e.g., a statement that "I agree to the foregoing contract terms" set out immediately above a signature line), in the text of the on-screen signature process (e.g., a statement that "By checking this box I agree to the terms of use"), or in a process structured so that the purpose is evident.

The overall signing process should be designed to minimize the risk that signers could legitimately claim later that they applied an electronic form of signature without realizing its legal significance – i.e., without understanding the reason for signing and/or without an intent to sign. This might be accomplished, for example, by requesting a confirmation of the signer's signature, by acknowledging the signer's signature and then giving him the option to cancel or continue, or by following the signature step with a submission step whereby the signed records are not effective until submitted.

The key is that the overall signing process be set up in a manner designed to: (1) clearly identify the reason for signing (e.g., agreement to the contract terms; acknowledgement of receipt, etc.), and (2) clearly specify the conduct that will indicate an intent to sign for the purpose of agreeing to that reason. Often this is done by the ceremony surrounding the signing process.[48] Such ceremony can help the parties to understand what they are doing and its significance. For example, persons need to know whether they are clicking to get to the next screen in a process or clicking to agree to a contract. Likewise, they need to know whether they are using their private key to generate a digital signature for the purpose of making an electronic record tamper proof or for the purpose of attaching a legally binding signature.

3. Association of Signature to the Record

In a paper-based transaction, a document is typically signed by writing one's name directly on the document to be signed. Writing one's name on a blank sheet of paper, for example, will not qualify as a signature for any specific document. By its very

[48] See, e.g., OMB M-00-10, noting that: "It is also important to establish that the user of the digital signature or PIN/password is fully aware of obligations he or she is agreeing to by signing at the time of signature. This can be ensured by programming appropriate ceremonial banners into the software application that alert the individual of the gravity of the action she is about to undertake. The presence of such banners can later be used to demonstrate to a court that the user was fully informed of and aware of what he or she was signing."

nature, signing a document requires putting the signature directly on the document.[49]

The same requirement is carried over to electronic records. That is, to be functionally equivalent to a handwritten signature, the E-Transaction laws require that the electronic form of signature must be made a part of the record being signed and in accordance with acceptable recordkeeping requirements established by the National Archives and Records Administration (NARA). Specifically, it must be attached to, or logically associated with, the record being signed;[50] otherwise it is not legally significant. There are two aspects to this issue.

First, it must be clear to the signer exactly what it is that he/she is signing. In a paper environment, the document is in front of the signer, and the signature is applied directly by the signer to the document, so that the signer can know exactly what is being signed. Similarly, in an electronic environment the signer must have an opportunity to review the record before signing it, and to clearly understand the parameters of the record he or she is signing.[51] Because an electronic signing process can apply one's electronic signature to something other than what is displayed on a screen, it is also critical that the signing process be established in a manner to ensure that the signer's electronic signature is applied only to what the signer can see and review – nothing more or less.[52]

[49] In some cases, such as with an allonge, the signature on a separate piece of paper is attached to or related to the document signed.

[50] E-SIGN and UETA expressly require that the electronic signature be "attached to or logically associated with a record." E-SIGN 15 U.S.C. Section 7006(5); UETA Section 2(8). This requirement is not expressly stated in GPEA, but is implied by the GPEA requirement that the method of signing must indicate "such person's approval of *the information contained in the electronic message*" (emphasis added). A method of signing cannot indicate approval of information contained in a message unless it is somehow attached to or logically associated with the message being signed.

[51] See, e.g., *Specht v. Netscape Communications Corp.*, 306 F.3d 17, 30 (2d Cir. 2002).

[52] Note that E-SIGN and UETA also require that certain records be capable of printing and downloading by the parties involved. See, e.g., E-SIGN 15 USC Section 7001(e) and UETA Sections 8(a) and 8(c).

Second, the electronic form of signature applied by the signer must be linked to the record being signed. In a paper transaction, the handwritten name used by a party as his signature is written directly on the document being signed (e.g., the classic signature at the end of a long contract), and anyone later reviewing the document can readily determine that it has been signed. Likewise, for an electronic signature to be functionally equivalent to a handwritten signature on a paper document, the sound, symbol, or process that constitutes the electronic form of signature must be in some way attached to, or associated with, the electronic record being signed. And this must be done in a manner that allows someone to later determine that the record has been signed. This is particularly important for electronic records, since they might otherwise be communicated separately from any physical media (for example, a storage disk) on which they may exist at any point in time.[53]

Satisfying this requirement requires storing the data constituting the electronic form of signature, and doing so in a way that permanently associates it with the electronic record that was signed. Where the electronic form of signature consists of a symbol or a sound (such as a typed name, a digitized image of a handwritten name, a PIN, a digital signature, a voice recording, etc.), the data representing the symbol or sound must be saved. Where the electronic form of signature consists of a process (such as clicking on an "I Agree" button), the system must be programmed so that completion of the process generates some specific data element to indicate completion of the signing process, or some other procedure (such as generation of a log record or audit trail) to record the act of signing.

It is also recommended that the following additional data elements be appended to or associated with the signature data provided privacy considerations have been taken into account:

- Identity of the signer or a link to the source of identifying information, such as a validated UserID, a digital certificate, a biometric database, etc.;
- Date and time of the signature;
- Method used to sign the record; and
- An indication of the reason for signing

The signature data must then be attached to, or logically associated with, the record being signed. Thus, must be done at the time of signing.

Associating the signature with the document can be accomplished using various approaches. The signature data can be embedded within, or directly appended to, the electronic record that was signed. Using this approach, the electronic signature becomes a part of, and is stored with, the electronic record being signed. Alternatively,

[53] See UETA, § 2(8), comment 7. This is consistent with the approach taken by the Food and Drug Administration in its regulations on electronic signatures set forth at 21 CFR Part 11 (March 20, 1997). § 11.70 of those regulations also require that electronic signatures "shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means."

the data representing the electronic signature can be stored separately from the document signed, so long as a demonstrably reliable and provable process is in place (which might include a relational database or a digital signature algorithm) to associate the electronic signature with the electronic record so that it can be established (in court if necessary) that a particular electronic signature was applied to a specific electronic record (by a specific person, at a specific time) with an intent to sign that electronic record. However, using the latter process may increase the risk that the transaction cannot be validated later.

Other approaches are also feasible. However, whatever the approach, it requires implementing an electronic recordkeeping process that, in the future, can provide evidence that a specific electronic signature was applied to or used in connection with a specific electronic record. Federal organizations should review their Privacy Impact Assessments (PIAs) and System of Record Notices (SORNs) to see: i) if they already have one covering electronic recordkeeping processes; ii) if the current PIAs and/or SORNs cover any new approach that might be implemented; and iii) if they need to develop a new PIA and/or SORN.

4. Identification and Authentication of the Signer

By definition, a signature must be the act of a specific signer. If the alleged signer denies signing, the signature will usually be unenforceable unless there is proof that the alleged signer did do the signing. Thus, if it is ever necessary to prove the validity of an electronic signature in court, it will be necessary to prove "who" signed. Meeting this burden of proof requires establishing a link between an identified person and the signature – i.e., attribution.

In a paper environment, signer attribution is typically accomplished by a variety of means such as the testimony of witnesses ("I saw him sign it"), notarization, circumstantial evidence suggesting the alleged signer actually did sign the document, or handwriting analysis. Some of these approaches (other than handwriting analysis) may also work in the electronic environment,[54] although more commonly alternative processes will be necessary. However, as a threshold matter, it is important to note that it is not necessary, in either the paper or electronic environment, for the form of signature itself to establish the identity of the signer.

Just as an electronic form of signature must be associated with a record, it must also be associated with a person (or at least capable of such association, if needed). Accordingly, ensuring the validity of any electronically signed record begins with identification and authentication of the signer.[55] That is, it requires evidence of "who"

[54] One commonly used form of circumstantial evidence is where a party cannot access a web-based process without clicking "I Agree" to the Terms of Use. In such case, evidence that the party actually accessed the web-based process is often accepted by courts as evidence that he/she agreed to the terms of use.

[55] GPEA requires that the method of signing "identifies and authenticates a particular person as the source of the electronic message." GPEA Section 1710(1)(A). E-SIGN and UETA do not expressly

the electronic form of signature belongs to, as well as evidence that the identified person is actually involved with the transaction. Identity and authentication are thus critical elements of the "signing process."[56]

While authentication of the signer's identity is an important part of the signing process, it may or may not be the electronic form of signature that provides proof of identity. Many forms of signature do not contain or directly link to the identity of the person making them (such as clicking an "I Agree" button), or if they do provide evidence of identity, such identity may not be reliable (e.g., a typed name). However, it is not necessary that the signer's identity, or the ability to authenticate that identity, be part of the form of the signature itself.[57] Other security procedures may be used to accomplish this objective. For example, the signer's identity may be authenticated as part of an overall process of obtaining access to a website or electronic resource that includes the record to be signed. If the act of signing is performed during the session authorized by the authentication process, the signature itself is attributed to the signer because the person accessing the record for signing has been duly authenticated. As long as the overall signing process addresses identity and authentication, it is acceptable.[58]

There are, of course, numerous ways to identify a person, and the level of confidence with respect to such identification will often depend on the needs of the transaction. Likewise, once a person's identity has been established, there are numerous ways to authenticate such person's identity over a remote system, and the level of confidence with respect to such authentication will often depend on the needs of the transaction. For additional information on electronic authentication of identity, see Office of Management and Budget Memorandum M-04-04, E-Authentication Guidance for Federal Agencies (December 16, 2003),[59] and National Institute of Standards and

---

require identification or authentication of the signer, but such requirement is implied by the language in both statutes stating that an electronic signature is a sound, symbol, or process, that is "executed or adopted *by a person*". E-SIGN 15 U.S.C. § 7006(5), UETA Section 2(8). Satisfying that requirement presumably requires identifying and authenticating "a person." Moreover, such identification and authentication is presumably required for the admissibility of evidence of an electronic signature in a court proceeding.

[56] See, e.g., OMB M-00-10, noting that: "Agencies should develop well-documented mechanisms and procedures to tie transactions to an individual in a legally binding way."

[57] Likewise, it is not necessary that the electronic form of signature protect the signed record from alteration, although some types of signatures will protect a record's integrity. See Section D.5.

[58] GPEA requires that the overall "method of signing" must identify and authenticate the signer, but does not necessarily require that the specific data object or process that constitutes the signature include the identity element, so long at the overall method does. See GPEA Section 1710. E-SIGN does not directly impose such an identity requirement, but that the rules of evidence will likely require it to authenticate an electronically signed document.

[59] OMB M-04-04, available at http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf

Technology, Special Publication 800-63-1, Electronic Authentication Guidance (December 2011).[60]

In light of their technology neutral approach, the E-Transaction Laws do not require the use of any particular method to identify or authenticate a party, so long as the method selected satisfies the requirement that it be as reliable as appropriate for the purpose in question. As noted above, it need not be part of the same step or process that indicates the signer's intent, so long as the person's identity and intent can be reliably correlated.

5. Integrity of Signed Record

In the paper-based world, signed documents are stored in files, often coded in some manner to aid in retrieval. Their usability, admissibility, and provability of each such document is based on the continuing integrity of the document itself (legibility, no indication of alteration, etc.) and the preservation of the additional "chain of evidence" that proves the signature's validity, as discussed in Section D.4 above. The integrity of the document often relies on the ability of the storage process used to protect it from fire, water, and other environmental dangers, and to limit access to authorized persons.

Likewise, the usability, admissibility, and provability of a signed electronic record requires procedures be undertaken to ensure the continuing integrity of both the electronic record and its electronic signature following completion of the signing process. It is a matter of providing appropriate data security for both the record and the signature.

Data integrity is concerned with the accuracy and completeness of electronic information communicated over the Internet or stored in an electronic system, and with ensuring that no unauthorized alterations are made to such information either intentionally or accidentally. Ensuring "integrity" requires "guarding against improper information modification or destruction, for the full retention period of the record."[61]

The concern regarding integrity flows from the fact that electronic records are easily altered in a manner that is not detectable. In an electronic transaction of any significance, the parties to the transaction must be confident of the integrity of the information before they rely or act on the record.[62]

---

[60] NIST Special Publication 800-63, available at http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf

[61] Homeland Security Act of 2002 § 1001(b), amending 44 U.S.C. § 3532(b)(1)(A).

[62] Some courts have started requiring expanded proof of the integrity of stored electronic records before they will be admissible as evidence in the case. See, e.g., *American Express v. Vinhnee*, 336 B.R. 437; 2005 Banker. LEXIS 2602 (9th Cir. December 16, 2005); *Lorraine v. Markel*, 2007 U.S. Dist. LEXIS 33020 (D. Md. May 4, 2007); *Victory Med. Hosp. v. Rice*, 493 N.E.2d 117 (Ill. App. Ct. 1986).

Digital signatures provide evidence of data integrity as part of the signature validation process, but as with the attribution requirement, this function may be performed by other security process associated with the electronic form of signature or the signing process to achieve the same result.

E. SATISFYING THE SIGNING REQUIREMENTS

1. Overall Approach

In general, federal organizations have a great deal of flexibility when selecting and/or designing the processes to be used for the electronic signing of records. However, it is important to understand that the solution chosen must take into consideration all of the signing requirements set forth in Parts C and D above.

The goal is to implement a signing process that is ***as reliable as is appropriate*** for the purpose in question.[63] The reliability of a signing process refers to the extent to which it supports enforcement of the resulting electronic signature in the face of attempts by the alleged signer (or an interested third party) to:

- **Repudiate** the electronic signature (e.g., a claim that "I didn't sign it")[64]
- **Deny any intent to sign** (e.g., a claim that "I didn't agree to that, it was just a draft," or a claim that "I may have done the act claimed to be a signature, but I did not intend (or understand) it to be a signature.")
- **Challenge the integrity** of the record or signature (e.g., a claim that "The record has been altered since I signed it" or "That isn't the record that I signed").

Stated differently, the reliability of a signing process is a function of the strength of the methods used by the federal organization to:

- **Identify and authenticate** the identity of the signer and attribute that identity to the particular electronic form of signature used in a particular case;
- **Associate the electronic form of signature** used to the electronic record being signed;
- Establish that the electronic form of signature associated with a record was executed or adopted by the identified signer with the requisite **intent to sign**; and
- Establish the continuing **integrity** of the signed record.

The reliability standard recognizes: (1) that there are many different processes that could be used and combined for a signing process, and (2) that the requirements for the strength of any particular process are relative, i.e., that they will vary with the nature of the transaction, the parties involved, and a variety of other factors. Thus in

[63] GPEA at Section 1703(b)(1)(C). See also OMB M-00-10 (noting that OMB must "develop procedures for Executive agencies to follow in using and accepting electronic documents and signatures . . . with due consideration of . . . ensuring that electronic signatures are as reliable as appropriate for the purpose in question").

[64] See e.g., *Kerr v. Dillard Store Services, Inc*., 2009 U.S. Dist. LEXIS 11792; 105 Fair Empl. Prac. Cas. (BNA) 1298; 92 Empl. Prac. Dec. (CCH) P43,483 (D. Kan. 2009).

ascertaining whether a proposed signing process is sufficiently reliable for the intended purpose, federal organizations must take into account a variety of factors other than just the specific technology used as the electronic form of signature.

With respect to the reliability analysis in a signing process, a digital signature created by a properly identified government signer through the use of his or her PIV card - if properly implemented - will normally satisfy the reliability standard for all of the signing requirements, except for the intent requirement (which must be addressed separately as outlined in Sections D.2 and E.4 (b) regardless of the technology used).[65]

For all other approaches to signing, determining whether a particular technology and set of procedures that comprise a signing process is "as reliable as is appropriate" for the intended purpose requires a risk analysis with respect to the enforceability of the resulting signature. Specifically, this requires an analysis of: (1) the risk that an alleged signer (or other interested third party) will be able to successfully repudiate the electronic signature, deny that it was made with an intent to sign, or challenge the integrity of the signed record, and (2) the loss, cost, or other impact of such a successful challenge to the enforceability of the signed record.

2. Risk Analysis

With respect to each of the potential challenges to the enforceability of an electronic signature noted above, a risk analysis should consider:

- the **likelihood of a successful challenge** to the validity of the electronic signature, and
- the **monetary loss, or other adverse impact**, that will result from such a successful challenge to the enforceability of the electronic signature.

Because reliable data regarding the likelihood of a successful challenge to a signature may not be available, or the resulting impact of a successful challenge may not be capable of measurement in dollars, it is recommended that a qualitative approach be taken with respect to the risk analysis. Using such an approach, the risk of a challenge being successful and having a significant impact is defined in more subjective and general terms such as high, moderate, and low. (See generally, National Institute of Standards and Technology, FIPS Pub. 199, Standards for Security Categorization of Federal Information and Information Systems.)[66] In this regard,

---

[65] Thus, for intra-governmental transactions where all potential signers possess a PIV card (and the associated card readers, software, and identity verification processes are in place), the use of a signing process that employs a digital signature created by the signer through the use of his or her PIV card is recommended, as it will allow federal organizations to leverage the highly secure PIV card technology and associated infrastructure already in place, and will provide the highest level of reliability for all of the signature requirements other than intent. Even where the PIV card is used, however, the intent element of the signing process must be adequately addressed as outlined in Sections D.2 and E.4 (b) of this Guidance.

[66] FIPS Pub. 199; available at http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

qualitative analyses depend more on the expertise, experience, and good judgment of the Federal managers conducting them than on quantified factors.[67]

In determining whether a signing process is sufficiently reliable for a particular purpose, federal organization risk analyses need at a minimum to consider the relationships between the parties, the value of the transaction, the risk of unauthorized alteration, and the likely need for accessible, persuasive information regarding the transaction at some later date. In addition, federal organizations should consider any other risks relevant to the particular process. Once these factors are considered separately, a federal organization should consider them together to evaluate the sensitivity to risk of a particular process, relative to the benefit that the process can bring.[68]

Once that determination is made, a signing process can be designed that takes into account the risk level determined by the risk assessment and the availability and cost of mitigating actions that could be taken.

(a) Evaluating Likelihood of Successful Challenge to Signature

The likelihood of a successful challenge to the enforceability of a signature is categorized as "Low," "Moderate" or "High" In alignment with FIPS Pub. 199.[69] Generally, the factors that should be taken into account in making that determination include the following:

(1) Parties to the Transaction

One key factor in evaluating the risk that an alleged signer will repudiate or otherwise challenge the electronic signature in a given transaction is the nature of the parties involved. Generally speaking, the closer the relationship and the more sophisticated the parties the lower the risk of repudiation.

For example, there is generally a very low risk of a party later repudiating the electronic signature in an inter- or intra-governmental transaction of a relatively routine nature. Similarly, transactions between a regulatory agency and a publicly traded corporation or other known entity regulated by that agency will often bear a relatively low risk of repudiation, particularly where the regulatory agency has an ongoing relationship with, and enforcement authority over, the entity. For the same reasons, risks tend to be relatively low within rulemaking contexts, as all parties can view the submissions of others so the risk of imposture is minimized.[70]

---

[67] OMB M-00-10

[68] OMB M-00-10

[69] See generally, FIPS Pub. 199; available at http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

[70] OMB M-00-10

Likewise, the more sophisticated the alleged signer, the lower the likelihood of repudiation. For example, the risk of repudiation is probably greatest with consumers, somewhat less with businesses (especially larger established businesses), and even less with other federal organizations.

Thus, for purposes of the risk analysis, federal organizations should consider whether the proposed transaction is:

- An intra-agency transaction
- An inter-agency transaction
- A transaction between a federal organization and a non-federal organization (state, or local)
- A transaction between a federal organization and a private organization – e.g., business, non-profit, association, etc. (G2B)
- A transaction between a federal organization and an individual – (G2C)
- A transaction between a federal organization and a foreign government.[71]

(2) Nature of the Relationship and Frequency of Transactions

The nature of the relationship and frequency of the transactions between the parties is also a relevant risk factor. Risks tend to be relatively low in cases where there is an ongoing relationship between the parties, particularly where they engage in frequent transactions. Conversely, the risk of signature repudiation or other challenges to the enforceability of the electronic signature are greater when the parties are strangers who have not previously dealt with each other, or only do so infrequently.

Other types of transactions, such as those involving an ongoing relationship between a federal organization and non-governmental entities and persons, can have varying degrees of risk depending on the nature of the relationship between the parties; the same would apply in the case of those federal programs in which the ongoing relationship is between entities that are acting on behalf of a federal organization and such non-governmental entities and persons -- e.g., transactions between a lender, guaranty agency, or other institution participating in a federal loan or financial aid program and another program participant or a member of the general public, such as a borrower or grant recipient.[72]

On the other hand, the highest risk of fraud or repudiation is for a one-time transaction between a person and a federal organization that has legal or financial implications. Federal organizations should also pay attention to transactions with non-federal entities, where the federal organization has a law enforcement responsibility but does not have an ongoing relationship. Transactions between a federal organization and a foreign entity may entail unique legal risks due to varying national laws and

[71] OMB M-00-10

[72] OMB M-00-10

regulations. In all cases, the relative value of the transaction needs to be considered as well.[73]

In addition, federal organizations should also consider whether the signing process will occur in-person (i.e., all parties in the same room) or remotely. Although remote signing processes may be more common, they also present greater risks that should be considered.

Thus, for purposes of the relationship and frequency risk analysis, federal organizations should consider whether the proposed transactions involve:

- An ongoing relationship between the parties
- A new relationship with a known party
- A new relationship with an unknown party
- One-time, occasional, or frequently reoccurring transactions
- An in-person signing or a remote signing.

(3) Value or Significance of the Transaction

The value or significance of the transaction can have a significant impact on the risk that an alleged signer will attempt to repudiate the signature. That is, the greater the value or significance, the greater the likelihood that a party who later finds it to be an undesirable transaction may want to repudiate it. While value is often measured in terms of the dollar amount involved, other factors are also relevant.

Federal organization risk analyses should attempt to identify the relative value of the type of transaction being automated and factor that against the costs associated with implementing technological and management security controls to mitigate risk. Note that the value of the transaction depends on the perspective of the federal organization and the transaction partner. In general, electronic signatures are least necessary in very low value transactions and need not be used unless specifically required by law or regulation. Where signature is necessary, the method of electronic signature should be appropriate to the level of risk.[74]

The value or significance of the transaction may be higher and hence the risk of a challenge to the enforceability of an electronic signature greater, in cases of –

- Transactions involving the transfer of funds
- Transactions where the parties commit to actions or contracts that may give rise to financial or legal liability

[73] OMB M-00-10

[74] OMB M-00-10

- Transactions involving information protected under state or federal law (e.g., privacy, national security, otherwise sensitive, etc.) – i.e., importance and value of the information involved
- Transactions where the party is fulfilling a legal responsibility which, if not performed, creates a legal liability (criminal or civil)
- Transactions where the party is certifying information or statements which, if not true or accurate, creates a legal liability (criminal or civil).[75]

Conversely, the value or significance of the transaction may be lower, and hence the risk of a challenge to the enforceability of an electronic signature lower, in the case of transactions where no funds are transferred, no financial or legal liability is involved and no privacy or confidentiality issues are implicated.

(4) Risk of Unauthorized Alteration or Other Compromise

The likelihood of signature repudiation or other challenges to the enforceability of an electronic signature also increases with the likelihood of a security intrusion to the transaction or the stored record, especially if such an intrusion affects the integrity of the signed record. The likelihood of such an intrusion can depend on the benefit to the potential attackers and their knowledge that the transaction will take place. For purposes of risk analysis, it should be noted that:

- Regular or periodic transactions between parties are at a higher risk than intermittent transactions because of their predictability, causing higher likelihood that an outside party would know of the scheduled transaction and be prepared to intrude on it.
- The value of the information to outside parties could also determine their motivation to compromise the information. Information relatively unimportant to a federal organization may have high value to an outside party.
- Certain federal organizations, because of their perceived image or mission, may be more likely to be attacked independent of the information or transaction. The act of disruption can be an end in itself.[76]

(b) Evaluating Extent of Resulting Loss or Adverse Impact

Determining the likelihood of successful signature repudiation or other challenges to the enforceability of an electronic signature is the first part of the risk analysis. Next, federal organizations must consider the extent of any financial loss or other adverse impact flowing from a successful challenge to the validity of the electronic signature. This is generally a function of the value or significance of the record signed, as compared to its value or significance without a signature.

[75] OMB M-00-10

[76] OMB M-00-10

When evaluating such legal risks, federal organizations should consult with their legal counsel about any specific legal implications due to the use of invalid electronic signatures in electronic transactions or documents in the application in question.

As with the analysis of the likelihood of a successful challenge to the enforceability of a signature, the analysis of the cost or impact of an unenforceable signature should result in a "Low," "Moderate" or "High" determination. Generally, the factors that should be taken into account in making that determination include the following:

(1) Whether Lack of Signature Invalidates Transaction

In the case of transactions where a signature is required by law, a successful challenge to the enforceability of the signature will usually invalidate the entire transaction. That is, it will convert the document into an unsigned record. However, the significance of this result depends in part on the significance of the underlying transaction itself.

Conversely, in the case of a transaction where a signature is viewed as desirable, but is not legally required, the transaction may likely remain valid without a signature, but its enforceability may be weakened.

Thus, the impact on enforceability is generally much greater for transactions where signatures are required by law, but at the same time it is still important to consider the value or significance of the record signed and the overall transaction. It may well be that the weakened enforceability of a transaction that does not require a signature by law has a more significant impact in some cases than the complete unenforceability of other low value transactions where a signature is required by law.

(2) Damages and Other Non-Monetary Impact

Where the lack of an enforceable signature renders the entire transaction unenforceable, or even where it merely increases the difficulty of proving a transaction, the dollar value of the transaction or the resulting damages (where it is calculable) should be considered. Likewise, the non-monetary impact of the failed transaction should also be considered. For many transactions the dollar value of an unenforceable signature may not be readily calculable, yet the impact of the resulting non-enforceability or invalidity of the transaction may be significant.

(3) Need for Provable Electronically Signed Records at a Future Time

In some paper transactions requiring a party's signature, the signature both identifies the party and establishes that party's intent to submit a truthful answer. Sometimes a notary or other third party signs as witness to the signature. When converting these types of transactions to electronic processes, federal organizations

should ensure that the selected signing process is able to provide similar functions.[77] Transactions that need a provable record at a later time include transactions where:

- Transaction information may later be subject to audit or compliance;
- Transaction information will be used for research, program evaluation, or other statistical analyses;
- Transaction information may later be subject to dispute -
  - by one of the parties (or alleged parties) to the transaction;
  - by a non-party to the transaction;
- Transaction information may later be needed as proof in court or other forum;
- Transaction information will be archived later as long-term or permanently valuable records.

3. Overall Risk Level Determination

Both (i) the analysis of the likelihood of a successful challenge to the enforceability of a signature and (ii) the analysis of the cost or impact of an unenforceable signature should result in a "Low," "Moderate" or "High" determination[78]. Combining those determinations into a risk level matrix can be used to make an overall risk determination of "Low," "Moderate" or "High" (essentially by multiplying the likelihood of a threat event succeeding by the cost or impact of an unenforceable signature), as illustrated in Table E-1.

Table E-1 Risk Level Determination

	Likelihood of Threat Event Succeeding		
Impact of Unenforceable Signature	**Low Likelihood (1)**	**Moderate Likelihood (2)**	**High Likelihood (3)**
Low Impact (1)	Low Risk(1)	Low Risk (2)	Moderate Risk (3)
Moderate Impact (2)	Low Risk (2)	Moderate Risk (4)	High Risk (6)
High Impact (3)	Moderate Risk (3)	High Risk (6)	High Risk (9)

4. Acting on the Risk Assessment Results

The foregoing Risk Level determination (which categorizes the overall signature risk of the transaction as Low, Moderate, or High) will be used primarily to determine the options available for each of the five signature requirements discussed in Part D above. Selecting from the available options within the applicable Risk Level requires a further cost-benefit analysis as described in Section E.5 below.

[77] OMB M-00-10

[78] The four levels of assurance are defined in Office of Management and Budget Memorandum M-04-04, **E-Authentication Guidance for Federal Agencies**, December 16, 2003, available at http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf.

Depending on the Risk Level for the proposed transaction, the options for addressing each of the five signature requirements discussed in Part D above are as follows:

(a) Electronic Form of Signature

For **low risk transactions**, any electronic form of signature is acceptable, subject to the cost-benefit analysis discussed below. This includes clicking an on-screen button, checking an on-screen box, typing ones name, using a PIN number, or any other reasonable method, so long as it is clear to the signer that such act constitutes a signature, and is not being done for any other purpose (e.g., making it clear that the act of typing the signer's name is a signature and not filling out the name field in a form, or making it clear that clicking is a signature, and not simply a method to advance in an on-screen process).

For **moderate risk transactions**, any electronic form of signature is acceptable, subject to the cost-benefit analysis discussed below. This includes clicking an on-screen button, checking an on-screen box, typing ones name, using a PIN number, or any other reasonable method, so long as it is clear to the signer that such act constitutes a signature, and is not being done for any other purpose (e.g., making it clear that the act of typing the signer's name is a signature and not filling out the name field in a form, or making it clear that clicking is a signature, and not simply a method to advance in an on-screen process).

For **high risk transactions**, the only acceptable electronic form of signature is a cryptographically based digital signature created with a private cryptographic key that corresponds to the public key specified in a digital credential that is recognized by the Federal Bridge Certification Authority (FBCA) at Medium Hardware or High assurance, or by the COMMON Policy at the Common Hardware assurance level (at Level of Assurance [LOA] 3 or 4).

(b) Intent to Sign

For **low risk transactions**, evidence of intent to sign may be included either in the record being signed or in the on-screen signing process, as appropriate. While evidence of intent to sign must always be clearly provided, shorter or more cursory indicators of intent may be used as necessary to facilitate the signing experience, so long as it is reasonably clear to the signer that he/she is signing the record, not doing something else.

For **moderate risk transactions**, evidence of intent to sign may be included either in the record being signed or in the on-screen signing process, as appropriate. Clear evidence of intent to sign must be unmistakably provided. Shorter or more cursory indicators of intent should be avoided in favor of clearer evidence of intent to facilitate the signing experience, so that it is very clear to the signer that he/she is signing the record, not doing something else.

For **high risk transactions**, evidence of intent to sign must be included both in the record being signed and in the on-screen signing process. Such evidence of intent to sign must be clearly provided in both places, pursuant to an appropriate signing ceremony that makes it unmistakable to the signer (i) that he/she is signing the record (not doing something else) and (ii) the reason he/she is signing.

(c) Association of Signature to Record

For **low risk transactions**, any method may be used to associate the signature to the record being signed. This can include establishing a process that could not be completed unless a person has signed; using a process that appends signature data to the record signed; or establishing a database-type link between the signature data and the record signed.

For **moderate risk transactions**, any reasonable method may be used to associate the signature to the record being signed. This can include using a process that appends the signature data to the record signed, or establishing a database-type link between the signature data and the record signed. It cannot include relying solely on a process that could not be completed unless a person has signed.

For **high risk transactions**, the federal organization must use a cryptographic signing process whereby a hash of the content of the record being signed is incorporated into the signature data, so that there is an intrinsic relationship between the signature and the record signed. The signing data can then be either attached or appended to the record signed, or a database-type link can be established between the signature data and the record signed.

(d) Identification and Authentication of Signer

For **low risk transactions**, any approach to identification and authentication of the signer is acceptable, subject to the cost-benefit analysis discussed below. This includes self-assertion of identity by the signer.

For **moderate risk transactions**, the identification and authentication of the signer must be conducted at e-Authentication Level of Assurance 2 or higher. Any method at this Level of Assurance is acceptable, subject to the cost-benefit analysis discussed below.

For **high risk transactions**, the signer must be identified and authenticated by reference to a digital certificate issued at e-Authentication Level of Assurance 3 or 4 and containing the public cryptographic key that corresponds to the private cryptographic key used to create the digital signature for the record.

(e) Integrity of Signed Record

For **low risk transactions**, the federal organization's standard security procedures for ensuring integrity of low risk records are acceptable.

For **moderate risk transactions**, the federal organization's standard security procedures for ensuring integrity of moderate risk records are acceptable.

For **high risk transactions**, the record must be digitally signed using a digital signature process operating at Level of Assurance 3 or 4.

*** * ***

The foregoing Risk Level options are summarized in Table E-2.

Table E-2 Satisfying the Signature Requirements

	Low Risk	Moderate Risk	High Risk
Electronic Form of Signature	▪ Any electronic form of signature is acceptable, subject to a cost-benefit analysis. This includes clicking an on-screen button, checking an on-screen box, typing ones name, using a PIN number, or any other reasonable method appropriate to the intended transaction.	▪ Any electronic form of signature is acceptable, subject to a cost-benefit analysis. This includes clicking an on-screen button, checking an on-screen box, typing ones name, using a PIN number, or any other reasonable method appropriate to the intended transaction.	▪ The only acceptable electronic form of signature is a cryptographically based digital signature created with a private cryptographic key that corresponds to the public key specified in a digital credential that is recognized by the Federal Bridge Certification Authority at Medium Hardware or High assurance, or by the COMMON Policy at the Common Hardware assurance level (at Level of Assurance 3 or 4).
Intent to Sign	▪ Evidence of intent to sign may be included either in the record being signed or in the on-screen signing process, as appropriate. While evidence of intent to sign must always be clearly provided, shorter or more cursory indicators of intent may be used as necessary to facilitate the signing experience, so long as it is reasonably clear to the signer that he/she is signing the record, not doing something else.	▪ Evidence of intent to sign may be included either in the record being signed or in the on-screen signing process, as appropriate. Clear evidence of intent to sign must be unmistakably provided. Shorter or more cursory indicators of intent should be avoided in favor of clearer evidence of intent to facilitate the signing experience, so that it is very clear to the signer that he/she is signing the record, not doing something else.	▪ Evidence of intent to sign must be included both in the record being signed and in the on-screen signing process. Such evidence of intent to sign must be clearly provided in both places, pursuant to an appropriate signing ceremony that makes it unmistakable to the signer (i) that he/she is signing the record (not doing something else) and (ii) the reason he/she is signing.

	Low Risk	Moderate Risk	High Risk
Association of Signature to Record	▪ Any reasonable method may be used to associate the signature to the record being signed, including using a process that could not be completed unless a person has signed; using a process that merely appends signature data to the record signed; or establishing a database-type link between the signature data and the record signed.	▪ Any reasonable method may be used to associate the signature to the record being signed, including using a process that merely appends the signature data to the record signed, or establishing a database-type link between the signature data and the record signed. It cannot include relying solely on a process that could not be completed unless a person has signed.	▪ The federal organization must use a cryptographic signing process whereby a hash of the content of the record being signed is incorporated into the signature data, so that there is an intrinsic relationship between the signature and the record signed. The signing data can then be either attached or appended to the record signed, or a database-type link can be established between the signature data and the record signed.
Identification and Authentication of Signer	▪ Any approach to identification and authentication of the signer is acceptable, subject to a cost-benefit analysis.	▪ The identification and authentication of the signer must be conducted at Level of Assurance 2 or higher, using a method determined by a cost-benefit analysis.	▪ The signer must be identified and authenticated by reference to a digital certificate issued at Level of Assurance 3 or 4 and containing the public cryptographic key that corresponds to the private cryptographic key used to create the digital signature for the record.
Integrity of Signed Record	▪ The federal organization's standard security procedures for ensuring integrity of low risk records are acceptable.	▪ The federal organization's standard security procedures for ensuring integrity of moderate risk records are acceptable.	▪ The record must be digitally signed using a digital signature process operating at Level of Assurance 3 or 4.

5. Evaluating Risk-Based Options: Cost - Benefit Analysis Factors

As noted above, once the Risk Level has been determined, federal organizations must design a signing process that addresses each of the five signature requirements within the parameters outlined in Section E.4 for that specific Risk Level. Regardless of Risk Level however, for intra-governmental transactions where all potential signers possess a PIV card (and the associated card readers, software, and verification processes are already in place), it is recommended that the signing process established for such transactions employ a digital signature created by a properly identified signer through the use of his or her PIV card. This will allow the federal organizations to leverage the highly secure PIV card technology and associated infrastructure already in place, and will satisfy the high risk transaction requirements for all of the signature requirements except for the intent requirement (which must be addressed separately regardless of the technology used).

Designing an appropriate signing process within the options available for the applicable Risk Level requires that federal organizations conduct a cost-benefit analysis to address:

- **Practical considerations** that may require or rule out certain approaches to a signing process (e.g., most citizens don't possess a PIV card, and thus an alternate method of identifying consumers and/or an alternate electronic form of signature must be used in the signing process for most high risk government-to-consumer transactions);
- **Cost considerations** to both the federal organization and the signers that may restrict reasonable options (e.g., issuing smart cards to numerous parties for one-time transactions is not cost-effective; requiring consumers to pay the cost of obtaining digital certificates may be a cost barrier to many transactions).

Practical and cost considerations will most likely focus on the electronic form of signature used, and on the technology and/or processes used to identify and authenticate the signer (attribution). Of course the cost-benefit analysis must be limited to the choices available within the applicable Risk level.

The primary goal of a cost-benefit analysis should be to find a cost-effective signing process within the parameters of the specified risk level. In estimating the cost of any signing process, federal organizations should include costs (both to the federal organization and to the signer) associated with hardware, software, administration, and support of the signing process, both short-term and long-term. Federal organizations should consider the following issues when framing the cost-benefit analysis:

- Offering more than one way to sign electronically may enable more people to conduct electronic transactions. If different partners have different skills and differing security concerns, providing a combination of mechanisms will meet the needs of a greater number of possible partners.

- Electronic transactions can impose costs on the transaction partners. Many electronic signature techniques require specialized computer hardware and technical knowledge. The higher these threshold costs are, the higher the participation costs are for users. Higher costs will tend to narrow the range of potential users, which in turn limits the benefits of electronic communications.
- Federal organizations should assess the costs of developing and maintaining electronic transactions.
- If the cost-benefit analysis of a proposed signing process indicates that the solution is not cost effective, the federal organization should consider whether there are opportunities to reengineer the underlying process being automated. Occasionally, practices and rules under the control of a federal organization are based on factors or circumstances that may no longer apply. In these cases new practices and rules should be proposed if the changes do not undermine the objective or impair security, and if the changes lead to a more efficient process.[79]

Generally, the cost-benefit factors that should be taken into account in determining whether a proposed signing process is appropriate for a given risk level include the following:

(a) Technology Issues

(1) Technology requirements of the electronic form of signature, including hardware and software requirements;

(2) Technology requirements of the transaction, which may be driven by factors such as whether the transaction will involve remote or in-person signing, single or multiple signers, and one or multiple signatures by the same signer;

(3) Technology available to the signing parties, including the hardware and software available to the parties, the range of authentication procedures available to the parties, and the communication capabilities available to the parties;

(4) Availability of alternative electronic forms of signature, alternative methods of identification and authentication, and alternative methods of ensuring integrity of the signed record; and

(6) Susceptibility of each potential electronic form of signature or technology to forgery, compromise, and/or repudiation.

[79] OMB M-00-10

(b) Requirements of the Signing Process

(1) Portability of the signature process (i.e., is there a need for signing to occur in many different, and changing, places?)
(2) Suitability of the signature process for multiple signers on same record
(3) Suitability of the signature process for in-person transactions and for remote transactions

(c) Capabilities of the Signing Party

(1) Sophisticated or unsophisticated regarding the transaction
(2) Knowledgeable or not regarding the technology used for signing
(3) Access to needed technology or not

(d) Cost of Implementing / Using the Signing Process

(1) To the federal organization
(2) To the signer

6. Special Rule for Intra-Governmental Transactions

For intra-governmental transactions where all potential signers possess a PIV card (and the associated card readers, software, and verification processes are in place), it is recommended that the signing process established for such transactions employ a digital signature created by the signer through the use of his or her PIV card, or at least accommodate such an option. This will allow the federal organizations to leverage the highly secure PIV card technology and associated infrastructure already in place, and will provide the highest level of reliability for all of the signature requirements, except for the intent requirement (which must be addressed separately as outlined in Sections D.2 and E.4 (b) regardless of the technology used).

F. GLOSSARY

1. **Appendix II to OMB Circular A-130**: Appendix II to OMB Circular A-130, Implementation of the Government Paperwork Elimination Act, November 2000, available at www.whitehouse.gov/omb/circulars_a130_a130appendix_ii. This document provides Executive agencies the guidance required under Sections 1703 and 1705 of the Government Paperwork Elimination Act (GPEA), P. L. 105-277, Title XVII, which was signed into law on October 21, 1998.

2. **Attribution**: The process of establishing or confirming that a specifically identified person is the source of a record or signature.

3. **Authentication**: The process of establishing or confirming that someone is the previously identified person they claim to be.

4. **Biometrics**: Unique physical characteristics of individuals that can be converted into digital form and then interpreted by a computer. Among these are voice patterns (where an individual's spoken words are converted into a special electronic representation), fingerprints, and the blood vessel patterns present on the retina (or rear) of one or both eyes.

5. **Click-wrap**: The process of signing a contract or other document by clicking an "OK" or "I Agree" button on a dialog box or pop-up window.

6. **Consumer**: An individual who obtains, through a transaction, products or services which are used primarily for personal, family, or household purposes, and also means the legal representative of such an individual. E-SIGN 15 U.S.C. Section 7006(1).

7. **Credential**: A digital document that binds a person's identity (and optionally, additional attributes) to a token possessed and controlled by a person. Data that is used to establish the claimed attributes or identity of a person or an entity. Common paper credentials include passports, birth certificates, driver's licenses, and employee identity cards. Common digital credentials include user IDs, and digital certificates. Credentials are a tool for authentication.

8. **Digital Signature**: Encrypted data produced by a mathematical process applied to a record using a hash algorithm and public key cryptography. The encrypted data is such that a person having the initial record and the public key that allegedly corresponds to the private key used to create the encrypted data can accurately determine: (1) whether the encrypted data was created using the private key that corresponds to such public key, and (2) whether the initial message has been altered since the encrypted data was created. The encrypted data constituting the digital signature is sometimes used as an electronic signature, is sometimes used as part of a process to authenticate a person or device, and is sometimes used to verify the integrity of the record.

9. **Digitized Signature**: A digital image of a handwritten signature. The image can be as simple as a scanned image of an ink-based signature handwritten on paper. In some cases the image is created by the signer using a special computer input device, such as a digital pen and pad, to write out his or her name in a manner that is captured and stored digitally. A digital image of a handwritten signature is sometimes used as an electronic signature.

10. **Document**: See "Record" and "Electronic Record."

11. **Electronic**: The term ''electronic'' means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities. E-SIGN, 15 U.S.C. § 7006(2), and UETA Section 2(5).

12. **Electronic Record**: A contract or other record created, generated, sent, communicated, received, or stored by electronic means. E-SIGN 15 U.S.C. § 7006(4). A record created, generated, sent, communicated, received, or stored by electronic means. UETA Section 2(7).

13. **Electronic Signature**: The term "electronic signature" is defined in each of the E-Transaction laws as follows:

    E-SIGN: 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. E-SIGN, 15 U.S.C. § 7006(5).

    GPEA: a method of signing an electronic message that-- (A) identifies and authenticates a particular person as the source of the electronic message; and (B) indicates such person's approval of the information contained in the electronic message. GPEA (Section 1710).

    UETA: an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record. UETA Section 2(8).

14. **E-SIGN**: Electronic Records and Signatures in Global and National Commerce Act" ("E-SIGN") (Pub.L. 106-229, § 1, June 30, 2000, 114 Stat. 464, codified at 15 U.S.C. §§ 7001-7006).

    Under E-SIGN, 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. E-SIGN, 15 U.S.C. § 7006(5).

15. **E-Transaction Laws**: E-SIGN, UETA, and GPEA.

16. **Electronic form of signature**: The particular sound, symbol or process used to represent the signer's signature. In a paper environment, a common form of signature is one's handwritten name. In an electronic environment, commonly used

forms of signature include typed names, digitized images of one's handwritten name, PINs, clicking an "I Agree" button on a website, and a digital signature.

17. **FIPS Pub. 199**: National Institute of Standards and Technology, FIPS Pub. 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.

18. **GPEA**: The Government Paper Elimination Act of 1998 ("GPEA"), Pub. L. No. 105-277, ''1701-1710 (1998) (codified as 44 U.S.C.A. § 3504 n. (West Supp. 1999)).

    Under GPEA, the term "electronic signature" means a method of signing an electronic message that-- (A) identifies and authenticates a particular person as the source of the electronic message; and (B) indicates such person's approval of the information contained in the electronic message. GPEA (Section 1710).

19. **Hash function:** A mathematical function that takes a variable length input string (such as the contents of an electronic record) and converts it to a smaller fixed-length output string (called a message digest, etc.), that is for all relevant purposes unique to the data used as input to the message digest function. The message digest is, in essence, a digital fingerprint of the data to which it relates.

20. **Identification**: The process of verifying and associating attributes with a particular person designated by an identifier.

21. **Identity**: A unique name of an individual person (an identifier), and any associated attributes; the set of the properties of a person that allows the person to be distinguished from other persons.

22. **Integrity**: A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.

23. **Intent**: Purpose: an anticipated outcome.

24. **Intent to Sign**: The intent of a person that a sound, symbol, or process that he or she applies to a record have a legally binding effect – e.g., applying ones name to a document or electronic record to affirm a particular reason for signing (e.g., to agree to the terms of a contract) as opposed to applying ones name to a document or electronic record for an administrative or transactional purpose (e.g., identifying oneself or specifying the name of the person to whom the goods should be shipped). "Intent to sign" should be distinguished from the "reason for signing" (see below).

25. **Level of Assurance**: One of four identity authentication assurance levels that describe the degree of certainty that a user has presented an identifier (i.e., a credential) that refers to his or her identity. The levels of assurance range from 1 (lowest) to 4 (highest) and are used to define a combination of (1) the degree of confidence in the vetting process used to establish the identity of the individual to

whom the credential was issued, and (2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued. The four levels of assurance are defined in Office of Management and Budget Memorandum M-04-04, **E-Authentication Guidance for Federal Agencies**, December 16, 2003, available at http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf.

26. **Method**: A particular way of doing something, a means, process, or manner of procedure, especially a regular and systematic way of accomplishing something, and an orderly arrangement of steps to accomplish an end.

27. **NIST Special Publication 800-63:** National Institute of Standards and Technology, Special Publication 800-63, Electronic Authentication Guidance; available at csrc.nist.gov/publications/PubsSPs.html.

28. **National Archives and Records Administration**, 44 U.S.C. Chapter 33

29. **OMB M-00-10**: Office of Management and Budget Memorandum M-00-10, Implementation of the Government Paperwork Elimination Act (April 25, 2000), available at www.whitehouse.gov/omb/memoranda_m00-10.

30. **OMB M-00-15**: Office of Management and Budget Memorandum M-00-15, OMB Procedures and Guidance on Implementing the Government Paperwork Elimination (September 25, 2000), available at www.whitehouse.gov/omb/memoranda_m00-15.

31. **OMB M-04-04**: Office of Management and Budget Memorandum M-04-04, E-Authentication Guidance for Federal Agencies (December 16, 2003); available at http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf.

32. **Password**: A secret word or string of characters that is used for authentication, to prove identity, or gain access to a resource.

33. **Person**: An individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture, governmental organization, public corporation, or any other legal or commercial entity. E-SIGN, 15 U.S.C. § 7006(8); UETA Section 2(12).

34. **Personal Identification Number (PIN) or password**: A user accessing a government organization's electronic application is requested to enter a "shared secret" (called "shared" because it is known both to the user and to the system), such as a password or PIN. When the user of a system enters her user ID, she also enters a password or PIN. The system checks that password or PIN against data in a database to ensure its correctness and thereby "authenticates" the user.

35. **PIV Card**: Personal Identity Verification Card issued to US federal government employees and contractors under Homeland Security Presidential Directive/Hspd-12. A PIV Card can be used by the person to whom it was issued to electronically sign a record using a digital signature that is attributable to such person.

36. **Process**: A procedure: a particular course of action intended to achieve a result.

37. **Reason for signing**: The purpose or statement of a person with regard to a document or electronic record that is affirmed by signing the document or record. Common reasons for signing a document or electronic record include:

    - Approving, assenting to, or agreeing to the information in the document or record signed (e.g., agreeing to the terms of a contract or inter-agency memorandum);
    - Certifying or affirming the accuracy of the information stated in the document or record signed (e.g., certifying that the statements in one's tax return are true and correct);
    - Acknowledging access to or receipt of information set forth in the document or record signed (e.g., acknowledging receipt of a disclosure document);
    - Witnessing the signature or other act of another (e.g., notarization); or
    - Certifying the source of the information in the document or record signed (e.g., certifying data in a clinical trial record, certifying an inventory count, etc.)

    The "reason for signing" should be distinguished from the "intent to sign" (see above).

38. **Record**: Information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form. E-SIGN, 15 U.S.C. § 7006(9); UETA Section 2(13).

39. **Repudiation**: Refuse to acknowledge, ratify, or recognize as valid.

40. **Security Procedure**: A procedure employed for the purpose of verifying that an electronic signature, record, or performance is that of a specific person or for detecting changes or errors in the information in an electronic record. The term includes a procedure that requires the use of algorithms or other codes, identifying words or numbers, encryption, or callback or other acknowledgment procedures. UETA Section 2(14).

41. **Signature**: A method of signifying *intent* in a manner that has legal significance; the means by which a person indicates a specified intent with respect to a document, record, or transaction; legally-binding evidence of the intention (will) of a person with regard to a document, record, or transaction.

42. **Signing process**: The overall set of means, processes and procedures whereby: (i) a person applies an electronic form of signature to an electronic record, (ii) does so with the intent to sign the record, (iii) the electronic form of signature is attached to or logically associated with the record being signed, (iv) the signer is identified and authenticated, and (v) the integrity of the signed record is verified.

43. **Signing requirements**: The requirements that must be satisfied to create a valid and enforceable electronic signature, as follows:

    - A person (i.e., the signer) must use an acceptable ***electronic form of signature***;

- The electronic form of signature must be executed or adopted by a person with the ***intent to sign*** the electronic record, (e.g., to indicate a person's approval of the information contained in the electronic record);
- The electronic form of ***signature must be attached to or associated with the electronic record*** being signed;
- There must be a means to ***identify and authenticate*** a particular person as ***the signer***; and
- There must be a means to preserve the ***integrity of the signed record***.

44. **Smart Card**: A smart card is a plastic card the size of a credit card containing an embedded integrated circuit or "chip" that can generate, store, and/or process data. It can be used to facilitate various authentication technologies also embedded on the same card. A user inserts the smart card into a card reader device attached to a computer or network input device. Information from the card's chip is provided to the computer only when the user also enters a PIN, password, or biometric identifier recognized by the card. Thus, the user authenticates to the card, making available electronic credentials which can then be used by the computer or network to strongly authenticate the user for transactions. This method offers far greater security than the typical use of a PIN or password, because the shared secret is between the user and the card, not with a remote server or network device. Moreover, to impersonate the user requires possession of the card as well as knowledge of the shared secret that activates the electronic credentials on the card. Thus, proper security requires that the card and the PIN or password used to activate it be kept separate. This is not a concern if a biometric is used for the latter purpose.

45. **UETA**: Uniform Electronic Transactions Act ("UETA") approved by the National Conference of Commissioners on Uniform State Laws (NCCUSL) on July 23, 1999, and adopted by 47 states as of November 2010.

    Under UETA, the term "electronic signature" means an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record. UETA Section 2(8).

46. **Voice Signature**: An audio recording created by an individual who intends to sign a particular transaction (or document) and used as the electronic form of signature.

G. STATUTES

1. **Electronic Records and Signatures in Global and National Commerce Act**" ("E-SIGN") (Pub.L. 106-229, § 1, June 30, 2000, 114 Stat. 464, codified at 15 U.S.C. §§ 7001 -- 7006); available at www.ogc.doc.gov/ogc/contracts/cld/ecomm/esgnca.pdf.

2. **The Government Paper Elimination Act of 1998** ("GPEA"), Pub. L. No. 105-277, ''1701-1710 (1998) (codified as 44 U.S.C.A. § 3504 n. (West Supp. 1999)); available at www.cio.noaa.gov/Policy_Programs/pea.pdf.

3. **Uniform Electronic Transactions Act** ("UETA"), approved by the National Conference of Commissioners on Uniform State Laws (NCCUSL) on July 23, 1999, adopted by 47 states as of November 2010; available at www.law.upenn.edu/bll/archives/ulc/fnact99/1990s/ueta99.htm.

H. REFERENCES

1. Appendix II to OMB Circular A-130; Implementation of the Government Paperwork Elimination Act, November 2000, available at www.whitehouse.gov/omb/circulars_a130_a130appendix_ii.

2. OMB M-00-10, Implementation of the Government Paperwork Elimination Act, April 25, 2000, available at www.whitehouse.gov/omb/memoranda_m00-10

3. Office of Management and Budget Memorandum M-00-15, Guidance on Implementation of the Electronic Signatures in Global and National Commerce Act (E-SIGN), September 25, 2000; available at www.whitehouse.gov/omb/memoranda_m00-15.

4. U.S. Department of Justice, Legal Considerations in Designing and Implementing Electronic Processes: A Guide for Federal Agencies, November 2000; available at www.cio.noaa.gov/Policy_Programs/eprocess.pdf.

5. National Institute of Standards and Technology, Special Publication 800-63, Electronic Authentication Guidance; available at csrc.nist.gov/publications/PubsSPs.html.