# 5 FAM 140

# ACCEPTABILITY AND USE OF ELECTRONIC SIGNATURES

*(CT:IM-172;  12-15-2015)*
*(Office of Origin:  IRM/FO/ITI/SI/IIB)*

## 5 FAM 141  PURPOSE

*(CT-IM-112;  07-30-2010)*

The purpose of this FAM chapter is to enable the Department to fulfill its obligations under the Government Paperwork Elimination Act (GPEA), Public Law 105-277 (codified at 44 U.S.C. 3504), and implement OMB guidance.  The GPEA requires all Federal agencies to provide individuals or entities the option to submit information or transact with the agency electronically and encourages Federal Government use of a range of electronic signature alternatives.  This chapter sets forth the Department of State's policy for using and accepting electronic signatures.

## 5 FAM 142  POLICY, SCOPE, AND AUTHORITY

### 5 FAM 142.1  Policy

*(CT-IM-112;  07-30-2010)*

a. Department bureaus and programs should use electronic signatures as appropriate and/or practical based on the policy presented in this subchapter.

b. The decision to use and implement an electronic signature must follow applicable statutes and regulations.  Bureaus that approve adoption of electronic signature solutions must first assess costs and benefits and risks and legal considerations; provide for appropriate records management procedures; and use a technical implementation in accordance with the guidelines in this subchapter and the references listed in 5 FAM 142.3.

c.  Whether bureaus decide to implement or forego electronic signatures for internal processing, section 1707 of the GPEA provides that the electronic signatures or other forms of electronic authentication must not be denied legal effect, validity, or enforceability because such records are in electronic form.

d. Bureau implementation of electronic signatures must take into account:

(1)  Maximizing the benefits and minimizing the risks and other costs;

(2)  Ensuring that forms of electronic signatures are as reliable as appropriate for the purpose in question;

(3)  Protecting the privacy of transaction partners and third parties that have information contained in the transaction, excluding the data that is normally available about the electronic signature itself;

(4) Providing wherever appropriate, for the electronic acknowledgment of electronic filings that are successfully submitted;

(5) Ensuring compliance with recordkeeping responsibilities; and

(6) Maintaining compatibility with standards and technology for electronic signatures generally used in commerce and industry and by State governments when exchanging electronic objects with those organizations.

f. See 5 FAM 611 for authorization to use e-signatures in contracts.

## 5 FAM 142.2 Scope and Applicability

*(CT-IM-112; 07-30-2010)*

a. This subchapter presents the policy for using electronic signatures. It applies to all Department bureaus, entities, and business processes that carry out the Department of State's mission. It also applies where traditional pen and ink (so-called "wet") signatures would be required from employees, members of the public, or representatives of other Federal agencies or other entities, and where electronic signatures are accepted in conformity with the GPEA.

b. This subchapter does not cover additional requirements that may apply to Department of State contractual transactions in the commercial, business, or consumer spheres that are governed by the Electronic Signatures in Global and National Commerce Act ("E-Sign"), Public Law 106-229, 114 Statute 464 (2000) (codified at 15 U.S.C. 7001 et seq.).

c. Bureaus implementing digital signatures must follow the applicable policies and procedures outlined in this subchapter, including the special provisions for using and accepting digital signatures as outlined in 5 FAM 145.2-2.

## 5 FAM 142.3 Authorities and References

*(CT:IM-172; 12-15-2015)*

In addition to those sources listed in 5 FAM 712, 5 FAM 140 derives from the following authorities and guidance documents:

(1) Government Paperwork Elimination Act (GPEA), Public Law 105-277, Title XVII 1701-1710 (1998), codified at 44 U.S.C. 3504 note:

(a) OMB M-00-10: OMB Procedures and Guidance on Implementing the Government Paperwork Elimination Act (April 25, 2000);

(b) Department of Justice: Legal Considerations in Designing and Implementing Electronic Processes: A Guide for Federal Agencies (November 2000) [hereinafter "DOJ Guidelines"];

(c) National Archives and Records Administration: Records Management Guidance for Agencies Implementing Electronic Signature Technologies (October 18, 2000); and

(d) OMB M-04-04: E-Authentication Guidance for Federal Agencies (December 16, 2003);

(2) E-Government Act of 2002, Public Law 107-347;

(3) Federal Information Security and Management Act of 2002, (44 U.S.C. 3541 et seq.) (enacted as Title III of the E-Government Act of 2002);

(4) Federal Records Act, 44 U.S.C. Chapter 33;

(5) National Archives and Records Administration (NARA) regulations on electronic records at 36 C.F.R. 1234;

(6) National Institute of Standards and Technology Special Publications:

(a) NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook (October 1995);

(b) NIST SP 800-18, Guide for Developing Security Plans for Information Technology Systems (December 1998);

(c) NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations (August 2009); and

(d) NIST SP 800-63, Electronic Authentication Guideline (April 2006);

(7) OMB Circular A-130, "Management of Federal Information Resources," Appendix III;

(8) *Federal Information Technology Acquisition Reform (FITARA) is Title VIII Subtitle D Sections 831-837 of Public Law 113-291 - Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015;*

(9) *OMB Memorandum (M-15-14); Management and Oversight of Federal Information Technology;*

(10) Federal Information Processing Standards Publications, National Institute of Standards and Technology:

(a) FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004;

(b) FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006;

(c) FIPS PUB 201 (change 1), Personal Identity Verification (PIV) of Federal Employees and Contractors, March 2006;

(d) FIPS 186-2, Digital Signature Standard, January 2007; and

(e) FIPS 196, Entity Authentication Using Public Key Cryptography, February 1997;

(11) Signatures in Global and National Commerce Act (commonly referred to as E-Sign); and

(*12*) Department of State Guidebook for the Implementation of Electronic Signatures

## 5 FAM 142.4 Definitions

*(CT-IM-112; 07-30-2010)*

Assurance: With regard to any particular form of electronic signature, assurance refers to:

(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. See 5 FAM 146.

Authentication: The process of establishing confidence in user identities, derived from NIST SP 800-63, Electronic Authentication Guideline.

Click-wrap: A procedure where the user must click on an object before further action can take place. For example, a website might require a user to acknowledge certain terms and conditions before allowing the user to log in or access certain parts of the website. For purposes of this chapter, "click-wrap" procedures that lack any mechanism for authenticating the identity of the signer are not considered electronic signatures.

Digital Signature: A digital signature is an application of technology for signing an electronic message that ordinarily provides the highest degree of assurance for identifying the signer. Digital signatures are a subset of electronic signatures, but unlike other electronic signatures, digital signatures are cryptographically derived, i.e., backed by a process such as a public key infrastructure (PKI).

Digitized Signature: A graphical image of a handwritten signature, not to be confused with a digital signature.

e-Authentication: Electronic authentication (e-authentication) is the process of establishing confidence in user identities presented electronically to an information system.

Electronic Object: An electronic object is a file that may contain documents, images, data, e-mail, etc. As used in this policy, electronic objects may be signed to authenticate the originator and provide a means to determine if the content has been changed subsequent to signing. Electronic objects may also be encrypted to protect the content from unauthorized access.

Electronic Signature: An electronic signature is defined in section 1710 of the GPEA as a method of signing an electronic message that:

(1) Identifies and authenticates a particular person as the source of the electronic message; and

(2) Indicates such person's approval of the information contained in the electronic message.

Identification: Identification is the means by which a user provides a claimed identity to the system, derived from NIST SP 800-12.

Non-Repudiation: The recipient of signed data can use a digital signature as evidence in demonstrating to a third party that the signature was, in fact, generated by the claimed signatory. This is known as non-repudiation, since the signatory cannot easily repudiate the signature at a later time.

Public Key Infrastructure: Provides a verifiable association between a public key (the public component of an asymmetric key pair) and the identity (and/or other attributes) of the holder of the corresponding private key (the private component of that pair).

"Wet" Signature: A "wet" signature is a traditional pen-and-ink signature. For the purposes of this policy, faxed signatures and non-electronic signatures included in pdf files will be considered "wet" signatures.

# 5 FAM 143 ROLES AND RESPONSIBILITIES

*(CT:IM-172; 12-15-2015)*

a. Bureaus and offices will routinely monitor and assess their use of "wet" and electronic signatures; conduct analyses of costs, benefits, and risks of accepting electronic signatures; decide the required assurance levels in accordance with 5 FAM 144; and adopt new procedures and technologies for using electronic signatures as appropriate and consistent with laws and regulations. Bureau executive officers must assign a responsible person (e.g., project manager) to oversee business process analysis; consider legal risks; decide on the required assurance level; and ensure adherence to e-signature policy.

b. IRM Governance and Policy Division (IRM/BMP/GRP/GP): Maintains 5 FAM 140 Electronic Signatures.

c. Information Integrity Branch (IRM/*FO*/ITI/SI/IIB): Administers the Department's PKIs and provides guidance to bureaus and offices for implementing solutions for electronic signature requirements.

d. Directives Management (A/GIS/DIR): Manages electronic forms.

e. Information Programs and Services (A/GIS/IPS): Performs records management functions; manages Privacy Impact Assessments (PIAs).

f. Office of the Legal Adviser/Office of Management (L/M): Advises bureaus on adopting electronic signatures to ensure that records using electronic signatures are created and maintained in accordance with all applicable laws and regulations. You may also need to consult with other offices within L bureau that provide advice.

# 5 FAM 144 ANALYZING COSTS, BENEFITS, RISKS AND PRIVACY

*(CT:IM-112; 07-30-2010)*

a. To evaluate the suitability of electronic signature alternatives for a particular application, bureaus must perform both a benefit cost analysis (BCA) (as described in 5 FAM 660), and a risk assessment (as described in 5 FAM 1065 and NIST SP 800-53). The goals of the assessment are to determine whether an electronic signature solution is appropriate to supplement or replace an existing paper-based process, and if so, to identify the particular technologies, practices, and management controls best suited to minimize the risk and cost to acceptable levels while maximizing the benefits to the parties involved. A privacy impact assessment (PIA), as described in the E-Government Act of 2002, section 208 must also be conducted and will address considerations unique to the implementation of electronic signature technologies.

b. To minimize analysis impact on bureaus, the Department of State has established a PKI that provides a digital signature with a high level of identity assurance and durability for the signature. PKI is approved for use on the Department's network. If a bureau chooses to utilize the Department's PKI, it may do so with no further technical assessment, but the bureau is still governed by DOS policies regarding PKI digital signatures. The Department's PKI may not be feasible to implement in every situation, i.e., general public transactions. See 5 FAM 145.2-1 for further information.

## 5 FAM 144.1 Cost Benefit Assessments

*(CT:IM-112; 07-30-2010)*

Submit a benefit cost analysis (See 5 FAM 660) with a detailed analysis appropriate to the size of the investment. It must be consistent with the methodology described in OMB Circular A-94, as well as rely on systematic measures of mission performance and a systematic methodology for comparing alternative means of meeting a specific objective. The BCA will identify alternatives for accomplishing the objective against mission performance criteria. This should be performed, together with the risk assessment, which will identify alternatives for accomplishing the objective against risk management criteria.

## 5 FAM 144.2 Risk Assessments

*(CT:IM-112; 07-30-2010)*

Program managers must document a risk assessment, as part of the system security plan (see 5 FAM 842 and NIST SP 800-18).

Specific guidance for performing a risk assessment for electronic signature functions is provided in the Department of State Guidebook for the Implementation of Electronic Signatures at.

## 5 FAM 144.3 Assurance Levels

*(CT:IM-112; 07-30-2010)*

a. Analysis included in the risk assessment will determine what assurance level is required for a given electronic signature transaction. Identification of the assurance level will take into account the legal consideration, like confidence in the signature process or legal admissibility (See 5 FAM 146). Identification of the assurance level will also guide the selection of electronic signature technology (e.g., non-cryptographic or cryptographic technology). Combinations of technologies may also prove practical.

b. There are four identity authentication assurance levels for e-government transactions, described in the E-Authentication Guidance for Federal Agencies (OMB M-04-04). Each assurance level describes the degree of certainty that the user has presented an identifier that refers to his or her identity. The four assurance levels are:

(1) Level 1: Little or no confidence exists in the asserted identity;

(2) Level 2: Some confidence exists in the asserted identity's validity;

(3) Level 3: High confidence exists in the asserted identity's validity; and

(4) Level 4: Very high confidence exists in the asserted identity's validity.

c. Determination of the assurance level will identify what technology or technologies are required for a given electronic signature transaction. "The Department of State Guidebook for the Implementation of Electronic Signatures" at provides guidance on identifying the appropriate assurance level, the available technologies, and the selection.

## 5 FAM 144.4 Privacy Impact Assessments

*(CT:IM-112;  07-30-2010)*

When developing authentication processes, bureaus must satisfy the requirements for managing security in the collection and storage of information associated with validating user identities. The E-Government Act of 2002, section 208, requires agencies to conduct privacy impact assessments for electronic information systems and collections. This includes performing an assessment when authentication technology is added to an electronic information system accessed by members of the public. For additional information on privacy impact assessments, consult OMB guidance M-03-22.

# 5 FAM 145 ELECTRONIC SIGNATURE TECHNOLOGIES

*(CT:IM-172;  12-15-2015)*

Bureaus considering electronic signature implementations should consult IRM/FO/ITI/SI/IIB. Send e-mail inquiries to PKIRegistrationCenter@state.gov.

## 5 FAM 145.1 Non-Cryptographic Technologies

*(CT:IM-112;  07-30-2010)*

a. Examples of non-cryptographic technologies that can be deployed in electronic signature applications include PINs, passwords, and digitized signatures, i.e., a graphic representation of a signature.

b. By themselves, non-cryptographic technologies do not directly bind identity to the contents of a document as do digital signatures, which actually use the document information to make the signature.

## 5 FAM 145.2 Cryptographic Technologies

## 5 FAM 145.2-1 Digital Signatures and PKI

*(CT:IM-112;  07-30-2010)*

a. A digital signature is a technology for signing an electronic message that ordinarily provides the highest degree of assurance for identifying the signer. Unlike other electronic signatures, digital signatures are cryptographically derived, i.e., backed by a process such as public key infrastructure (PKI).

b. The Department of State has established a PKI that enables digital signing in a manner that provides a high level of identity assurance and durability for the signature. This PKI is cross-certified with the Federal Bridge Certification Authority (FBCA) (see) and is therefore acceptable for use in transactions with other FBCA governmental and commercial member entities. It also represents the backbone for the Department's participation in e-Authentication at high assurance.

c. PKI is approved for use on the Department's network with no further technical assessment on the part of the bureau. When using PKI, bureaus are governed by DOS policies regarding PKI digital signatures (i.e., DOS PKI X.509 Certificate Policy and the Federal Bridge Certification Authority Certificate Policy.

d. Generally speaking, the Department's cryptographic digital signature (PKI) solution will provide the highest degree of assurance, but within the scope of this policy, the

Department's PKI is normally only feasible to implement in certain internal Department or U.S. Government transactions, i.e., transactions that may not include the general public.

## 5 FAM 145.2-2 Use and Acceptance of Digital Signatures

*(CT:IM-112; 07-30-2010)*

a. Through the use of the PKI and its underlying policies, the Department provides for the application of a very strong digital signature that is tightly bound to the individual signer. This signature can be used in any application that is designed to integrate PKI into the application. This signature must be accepted within the Department of State in the same manner as an inked (so-called "wet") signature when used on any documentation not specifically proscribed by e-Signature or existing Department-level policy.

b. To ensure the viability of the Department's PKI-based digital signature, the digital signature may not be applied to documentation in a manner that could circumvent the intent of the signature:

(1) This would include the use of digital signatures on documents, which could have information to which the signer attested, then was changed without deleting or invalidating the signature; and

(2) Exceptions would include information to which the signer was not attesting by the signature, i.e., information that could normally be changed without having to resign such documentation. This would include inconsequential information that is provided only as information and is not being attested to by the signer.

c. The Department must accept digital signatures from other entities as follows:

(1) Signatures from entities that have cross-certified with the FBCA and/or the Federal Common Policy Framework (FCPF); and

(2) Other such digital signatures as validated unilaterally by the Department as being supported by another entity's certificate authority in a sufficiently rigorous manner to ensure the viability of such signatures;

d. The Department is not obligated to accept digital signatures from entities, including FBCA and/or FCPF member entities that have not been validated by the Department as being sufficiently high enough for the intended application or may otherwise pose a potential threat to the Department's systems and operations.

## 5 FAM 145.3 Using Anonymous Credentials

*(CT:IM-112; 07-30-2010)*

a. Unlike identity authentication, anonymous credentials may be appropriate to evaluate an attribute when authentication need not be associated with a known personal identity. To protect privacy, it is important to balance the need to know who is communicating with the Department, from outside the Department, against the user's right to privacy. This includes using information only in the manner in which individuals have been assured it will be used. It may be desirable to preserve anonymity in some cases, and it may be sufficient to authenticate that:

(1) The user is a member of a group; and/or

(2) The user is the same person who supplied or created information in the first place; and/or

(3) A user is entitled to use a particular pseudonym.

b. These anonymous credentials have limited application and are to be implemented on a case-by-case basis. Some people may have anonymous and identity credentials. As general matter, anonymous credentials are appropriate for assurance Levels 1 and 2 only.

# 5 FAM 146 LEGAL CONSIDERATIONS

## 5 FAM 146.1 Legal Review

*(CT:IM-112; 07-30-2010)*

As part of their business-process analysis, bureaus must consult with the Office of the Legal Adviser/Office of Management (L/M), as well as the substantive L supporting office (e.g., Office of the Legal Adviser, Consular Affairs (L/CA); Employment Law (L/EMP)), when introducing electronic signatures, in order to validate the legal sufficiency of the solution and to establish whether there are any specific legal implications of using electronic signatures for a particular program or purpose. Bureaus also should review the Department of Justice Guidelines (Legal Considerations in Designing and Implementing Electronic Processes: A Guide for Federal Agencies), in particular, Section III and Appendix A.

## 5 FAM 146.2 General Parameters

*(CT:IM-112; 07-30-2010)*

a. To establish admissibility in court, electronic processes must be designed so that at least the following information can be proved with regard to sensitive or significant communications and transactions by, with, or within the Department. Hence, bureaus must ensure that business processes and systems relying on electronic signatures are capable of gathering, retaining, and making available the following information:

(1) Date and time that the communication or transaction was sent or initiated; and

(2) Identity and location of each particular person who transmitted such items. This includes:

(a) An identifier traceable to a particular individual (e.g., digital or digitized signatures or other identifiers, depending on which is appropriate); and

(b) A means of identifying the source of the transmission (e.g., mail server identification, e-mail account name, time-stamped Internet Protocol ("IP") address);

b. Identity of an individual can be established to varying degrees of certainty by the individual's transmission or use of any of the following:

(1) Something the individual knows (e.g., a password or secret number, personal information);

(2) Something the individual possesses (e.g., a token or magnetic card);

(3) Something the individual is (i.e., a biometric attribute); or

(4) Combinations of the above, which can substantially increase the security of an authentication system.

c. Bureaus should assess which of the above methods are suitable for each type of transaction or function. The Department's PKI Program provides the most secure capabilities with digital signatures that are:

(1) Unique to the signer;

(2) Under the signer's sole control;

(3) Capable of being verified by a third party; and

(4) Linked to data in such a manner that changes to the data invalidate the signature. The degree to which these attributes are necessary depends on the risks of the particular transaction:

(a) Non-Repudiation, showing that the communication or transmission actually was sent and/or received, by whom, and the date and time;

(b) Intent certification data, showing what the sender or originator of the communication or transmission intended by it, and the date and time he or she signed it. For example, certain electronic processes should be able to prove that a person who submits a report certifies to the agency that the report is true, accurate, and correct at the time submitted. If the submitter of a document is shown a banner on the computer screen on which the submitter must click "yes," the electronic process must be able to prove that the banner (including its precise text) was in fact displayed and that the submitter clicked "yes";

(c) When applicable, proof should be sought that the submitting individual was authorized to report for the company or other entity (e.g., by position or title); and

(d) Where applicable, proof should be sought that the individual has certified to the truth and accuracy of the information submitted and has submitted the information under penalty of perjury. This might include proof that a banner was displayed to the submitter, informing him that by clicking "yes," he acknowledges those matters;

(5) The complete contents of the communication or transaction, including any attachments or exhibits. This can include the terms unique to a given transaction and "boilerplate" terms that, on paper, might have been printed on the back of a form or in a set of instructions. Complete contents include both data and information submitted by the individual or company and the agency forms, questions, or certifications to which the information responded:

(a) If the communication contains answers or responses to questions on a form, include a means of proving the precise questions, instructions, or contents of the version of the form actually used;

(b) For communication with attachments, there must be a means for preserving the attachments and permanently "binding" them to the electronic communications;

(c) A means of proving that the information in the transmission was not altered. This includes proving that no one (e.g., neither the submitter nor the agency) altered the information after the submitter sent it, perhaps by proving that the electronic system allows no one the ability to alter such documents. Or the electronic process might be designed to provide an "audit

trail" showing all alterations, the date and time they were made, identifying who made them, and so on;

(d) As appropriate, a means of showing all relevant communications and documents on a given subject or point; and

(e) A means of distinguishing final documents from drafts.

## 5 FAM 146.3 Contract Transactions or Benefit Programs

*(CT:IM-112; 07-30-2010)*

Additional requirements may apply to contract transactions or provision of federal benefits. Please consult L/M and Section III-C-2-a and III-C-2-c of the DOJ Guidelines.

# 5 FAM 147 ELECTRONIC RECORDS MANAGEMENT

*(CT:IM-112; 07-30-2010)*

Electronic record management is the responsibility of the Office of Information Programs and Services (A/GIS/IPS). Bureaus using electronic signatures must comply with the applicable requirements defined in 5 FAM 440.

# 5 FAM 148 THROUGH 149 UNASSIGNED