BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 33-321

1 APRIL 2000

Communications and Information

AUTHENTICATION OF AIR FORCE RECORDS

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

OPR: HQ AFCIC/ITC (Ms. Cheryle Gumaer) Certified by: HQ USAF/SCXX (Lt Col Pricer)
Supersedes AFI 37-121, 18 February 1994. Pages: 5
Distribution: F

This instruction implements Air Force Policy Directive (AFPD) 37-1, *Air Force Information Management* (will convert to AFPD 33-3). It explains what Air Force records are and tells how to authenticate them. Send recommended changes or comments to HQ AFCA/XPXP, 203 W. Losey Street, Room 1060, Scott AFB IL 62225-5222, through appropriate channels, using AF Form 847, **Recommendation for Change of Publication**, with an information copy to HQ Air Force Communications and Information Center (HQ AFCIC/ITC), 1250 Air Force Pentagon, Washington DC, 20330-1250. Refer to **Attachment 1** for a glossary of references and supporting information.

SUMMARY OF REVISIONS

This document is substantially revised and must be completely reviewed. This is the initial publication of AFI 33-321. It defines records, methods to authenticate records, and who may authenticate records.

1. Definition of Terms:

1.1. Records. According to Title 44, United States Code, *Public Printing and Documents*, Section 3301, "records include all books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the US Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of the data in them. Library and museum material made or acquired and preserved solely for reference or exhibition purposes, extra copies of documents preserved only for convenience of reference, and stocks of publications and of processed documents are not included."

Report Documentation Page

Report Date	Report Type	Dates Covered (from... to)
01 Apr 2000	N/A	-

Title and Subtitle Air Force Instruction 33-321 Communications and Information Authentication of Air Force Records	**Contract Number**
	Grant Number
	Program Element Number
Author(s)	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) Secretary of the Air Force Pentagon Washington, DC 20330-1250	**Performing Organization Report Number** AFI33-321
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Sponsor/Monitor's Acronym(s)**
	Sponsor/Monitor's Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes	
Abstract	
Subject Terms	
Report Classification unclassified	**Classification of this page** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** UU
Number of Pages 5	

1.2. Electronic Records. Any combination of text, graphics, data, audio, pictorial, or other information represented in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer.

1.3. Authentication. A process used to ascertain the identity of a person or the integrity of specific information. A record is authenticated when it contains a proper signature or seal indicating the document is genuine and official. A signature or seal may be written, stamped, electronic or digital.

1.4. Electronic and Digital Signatures. It is important to distinguish subtle differences between these terms. Digital signatures are a subset of electronic signatures. Electronic signatures may or may not be tightly linked to a form or document, whereas digital signatures are inextricably linked to the document. Digital signature algorithms are approved by the National Institute of Standards and Technology (NIST), whereas electronic signatures are not.

1.4.1. Electronic Signature. An electronic signature is a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to indicate the person's identity. Electronic signatures include digitized images of paper-based signatures, typed notations such as "//s// John Doe," the address information in an e-mail header, and digital signatures.

1.4.2. Digital Signature. A digital signature is a transformation of a message or document using an asymmetric cryptosystem and a hash function such that a person having the initial message or document and a signer's public key can accurately determine:

1.4.2.1. Whether the transformation was created using the private key that corresponds to the signer's public key, and

1.4.2.2. Whether the initial message or document was altered since the transformation was made.

1.5. Signature Facsimile. A signature facsimile is a stamp that duplicates an original signature and has the same authority as the original signature.

2. Who Can Authenticate Records?

2.1. Authority. An individual's authority to authenticate records is by statute, directive, instruction, delegated authority, duty assignment, or specific position. Thus it is the capacity in which a person acts, not grade, that determines their authority to authenticate records.

2.1.1. Command Capacity. The authority of a commander to authenticate Air Force records, and the extent to which he or she may designate others to authenticate records, follows the principles of command and staff and the principle of delegation of duties contained in AFI 51-604, *Appointments to, and Assumption of, Command*. No record may be signed as "Acting Commander" or "For" or "For and in the absence of" (see AFMAN 33-326, *Preparing Official Communications*, for guidance on the format of the signature element).

2.1.1.1. A commander continues to discharge command functions when absent temporarily from their place of duty (temporary duty, etc.). During absences, designated representatives continue to act for and in the commander's name, as done routinely when the commander is present for duty (see AFI 51-604).

2.1.1.2. When a statute or other directive does not require the commander's personal signature, the deputy or vice commander is authorized to authenticate records without using the

authority line. Any other subordinate, including the staff director of any headquarters below HQ USAF, who authenticates a record on behalf of a commander must use the authority line *For the Commander* (or comparable official title) to indicate that he or she is acting as the commander's authorized agent. The authority line is not used on any communication to a person or agency outside the Department of Defense (see AFMAN 33-326).

2.1.2. Staff and Administrative Capacity. Staff and administrative personnel can authenticate a record without the authority line when it reflects their own opinion, position, or administrative action on matters within their assigned staff or administrative functions (see AFMAN 33-326). They must use the authority line for records representing the coordinated position of the entire staff or headquarters, or for records providing instructions or authorizations.

2.1.3. Professional Capacity. Some staff officers--including doctors, chaplains, and judge advocates--sign documents in the performance of their official duties that require no authority line or further authentication. Examples include: birth, death, and marriage certificates; and records of certain adverse actions.

3. How To Authenticate an Air Force Record. Use one of the following methods to authenticate records issued in the conduct of Air Force business:

3.1. Authentication by Written Signature. Sign the appropriate paper-based signature block using black or dark blue ink. Do not sign for another person; official directives or statutes require the personal signature of designated persons on many types of Air Force records. The signature of any other person using "For" or "For and in the absence of" does not meet administrative and legal requirements.

3.2. Authentication by Signature Facsimile. Do not use signature facsimile to authenticate a record unless the records requiring signature are so numerous that the act of written authentication becomes a monotonous and time-consuming task.

3.2.1. You can use a signature facsimile on clerical records, such as form letters or letters of transmittal.

3.2.2. You must physically safeguard signature facsimile equipment that is used to authorize the spending of government funds, the exercise of public power, or the binding of the Air Force or the Government to a course of action.

3.3. Authentication by Reproducing the Record That Has the Official Signa ture. Unless stated otherwise in the applicable statute or official directive, copies of a record bearing a reproduced signature have the same authority as the original.

3.4. Authentication by Use of Seals in Lieu of Signature. You can use a headquarters *OFFICIAL* seal instead of a signature if it will enhance efficiency or standardization. If you use a seal, affix it immediately above the signature block. For some records, such as awards and certificates of achievement, you can use both a signature and the seal.

3.4.1. Use standard seals 1 3/8 inches in diameter or less, with a lead or zinc alloy (or comparable material) die, mounted on a metal base.

3.4.2. Use impress or imprint seals made of metal, plastic, rubber, or another suitable material.

3.4.3. In organizations authorized to use seals, the custodian of the seals establishes controls to protect them and ensure that they are used properly. The functional office of primary responsibility assumes responsibility for protection of the seal.

3.5. Authentication by Electronic Signature. An electronic record is authenticated by a signature or seal which verifies both the identity of the signer and the authenticity of the data contained in the record. Electronic signatures may be attached to an electronic record to show ownership or responsibility; however, a digital signature is required on electronic documents requiring authentication.

3.5.1. Authentication by digital signature will eventually be based on the use of Public Key Encryption and Authentication. This technology uses a user-specific public/private key pair. The private key is maintained by the user and the public key is maintained centrally by a certificate authority. The public key and the private key combine to verify both the user's identity and provide confidentiality of the authenticity of the data contained in the record. A digital signature is:

3.5.1.1. unique to the signer and under the signer's sole control, using multiple controls (e.g., card, token, or password and personal identifier) to gain access to the signature,

3.5.1.2. capable of being verified,

3.5.1.3. linked to the data in such a manner that if the data is altered during transmission or storage the signature is invalidated, and

3.5.1.4. based on existing or future NIST Federal Information Processing Standards (FIPS) Pub 186-1, *Digital Signature Standard (DSS).*

3.6. Security . Protect classified and sensitive unclassified information in accordance with AFPD 33-2, *Information Protection*; the 33-200 series publications; AFI 31-401, *Information Security Program Management*; DoD 5400.7-R/Air Force Supplement, *DoD Freedom of Information Act Program*; and AFI 33-332, *Air Force Privacy Act Program.*

4. Publications That Outline Special Authentication Methods:

4.1. AFI 33-360, Volume 1, *Publications Management Program*, outlines the procedures for authenticating standard publications.

4.2. AFMAN 33-326, *Preparing Official Communications*, prescribes the requirements for drafting, coordinating, and authenticating messages for electrical transmission.

4.3. AFI 33-119, *Electronic Mail (E-Mail) Management and Use*, describes user and recipient responsibilities and authentication procedures for E-mail.

4.4. AFI 51-301, *Civil Litigation*, prescribes how to authenticate legal records.

WILLIAM J. DONAHUE, Lt General, USAF
Director, Communications and Information

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Title 44, United States Code, *Public Printing and Documents,* Section 3301

NIST FIPS Pub 180-1, *Secure Hash Standards,* 17 Apr 95

NIST FIPS Pub 186-1, *Digital Signature Standard (DSS),* 15 Dec 98

DoD 5400.7-R/Air Force Supplement, *DoD Freedom of Information Act Program*

AFPD 33-2, *Information Protection*

AFPD 37-1, *Air Force Information Management* (will convert to AFPD 33-3)

AFI 31-401, *Information Security Program Management*

AFI 33-119, *Electronic Mail (E-Mail) Management and Use*

AFMAN 33-326, *Preparing Official Communications*

AFI 33-332, *Air Force Privacy Act Program*

AFI 33-360, Volume 1, *Publications Management Program*

AFI 51-301, *Civil Litigation*

AFI 51-604, *Appointments to, and Assumption of, Command.*

Abbreviations and Acronyms

AFCIC—Air Force Communications and Information Center

AFI—Air Force Instruction

AFPD—Air Force Policy Directive

FIPS—Federal Information Processing Standards

NIST—National Institute of Standards and Technology

Terms

Asymmetric Cryptosystem—A cryptographic system based on public/private key pair encryption and decryption. The basis of asymmetric encryption is the requirement for a pair of two keys, when one key encrypts, the other must be used to decrypt. The foundation of the public/private key pair is one key cannot be derived from the other.

Hash Function—An algorithm mapping or translation of one sequence of bits into another, generally smaller set resulting in a condensed representation of a message or file. (Reference: NIST FIPS Pub 180-1, *Secure Hash Standards,* 17 Apr 95).