DEFENSE INFORMATION SYSTEMS AGENCY
P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

DISA INSTRUCTION 630-230-32* 27 May 2015

AUTOMATIC DATA PROCESSING

Digital Signatures

1. **Purpose.** This Instruction prescribes policy for digital signatures.

2. **Applicability.** This Instruction applies to all DISA activities.

3. **Scope.**

3.1 This Instruction applies to documents signed by DISA civilian, military, and contractor personnel that are used to conduct official business either internal or external to the Agency.

3.2 This Instruction does not apply to documents identified as "exemptions" or "exceptions" found in Public Law 106-229, Electronic Signatures in Global and National Commerce Act, 30 June 2000, located at http://www.gpo.gov/fdsys/pkg/PLAW-106publ229/pdf/PLAW-106publ229.pdf.)

4. **Authority.** This Instruction is published in accordance with the authority contained in DoD Instruction 8520.02, Public Key Infrastructure (PKI) and Public Key (PK) Enabling, 24 May 2011.

5. **References.**

5.1 DoD Instruction 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), 12 March 2014.

5.2 DISA Principal Director, EIS, Memorandum, Signing and Encryption of Unclassified Email Messages, 28 May 2014, located at https://disa.deps.mil/disa/cop/Privacy_Act/Lists/Announcements/Attachments/15/Signing%20and%20Encryption%20Email%20Memo.pdf

5.3 DISA Instruction 210-15-6, Records Management, 20 November 2012.

6. **Objective.** Adopting digital signatures as an accepted means of conducting business transactions within DISA and reducing DISA's reliance on paper transactions will improve information security and sharing, allow quicker access to documents, and reduce costs and environmental impact. Streamlining processes that required traditional written signatures and replacing them with digital signatures, when practicable, is essential to DISA complying with legislative and DoD mandates for paperless processing. The use of digital signatures will protect

DoD business transactions by supporting data integrity (a document cannot be changed without notification to the originator), nonrepudiation (the sender cannot deny sending or signing the e-mail, form, etc.), and authentication (for identification to networks, applications, and servers).

7. **Policy.**

7.1 Digital signatures will be accomplished using a DoD-approved process that utilizes public key infrastructure (PKI) certificates issued by DoD or a DoD-approved external PKI. (The list of DoD-approved external PKIs is provided on the Information Assurance Support Environment [IASE] Web site at http://iase.disa.mil/pki-pke/Pages/policies.aspx.)

7.2 DoD mission partners may process electronic transactions with DoD or exchange e-mail or other data containing DoD relevant information and will be encouraged to acquire and use certificates issued by approved external PKIs when interfacing with DISA public key enabling (PKE) information systems. (DoD mission partners include Federal, State, local, tribal, and coalition partners; foreign governments and security forces; international organizations; nongovernmental organizations; private sector companies or organizations; and educational institutes.)

7.3 All new digital signature solutions must be certified and accredited and then tested and approved for conformance by the Joint Interoperability Testing Command (JITC) PKE Laboratory before use, in accordance with DoD Instruction 8510.01 (reference 5.1).

7.4 Unclassified and classified e-mail messages will be digitally signed with approved digital signature capability when conducting official government business on property issued by DISA, in accordance with the DISA Principal Director, Enterprise Information Services (EIS), 28 May 2014 memorandum (reference 5.2); as of January 2015, EIS has been renamed to Implementation and Sustainment Center (ISC).

7.5 The organizational adopted application, system, or business process for digital signatures will afford the signer the opportunity to review the information to be signed prior to digitally signing the document and enable a digitally signed document to be converted to a hard copy document, as needed, or as required by law or policy.

7.6 Any hard copy of a document and/or form produced is to be archived according to DISA Instruction (DISAI) 210-15-6 (reference 5.3) and shall reflect that it was digitally signed. When the digital signature information is requested or required for archival, record, and/or legal purposes, the hard copy will, at a minimum, contain the certificate subject name of the individual who digitally signed the document, as well as the date and time the document was digitally signed (see reference 5.3).

7.7 Regardless of media and format, documents that fall into the category of "records," as defined in DISAI 210-15-6 (reference 5.3), and are digitally signed, will be managed in compliance with reference 5.3.

8. **Other Related Documents.** Additional information on digital signatures and topics related to digital signatures is provided in the following documents:

8.1 DoD Deputy CIO Memorandum, DoD-wide Digital Signature Interoperability, 5 May 2006, located at http://www.doncio.navy.mil/ContentView.aspx?ID=699

8.2 Public Law 105-277, Title XVII, Government Paperwork Elimination Act, Sections 1701 through 1710, 21 October 1998, located at http://www.gpo.gov/fdsys/pkg/PLAW-105publ277/pdf/PLAW-105publ277.pdf

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

8.4 National Institute of Standards and Technology (NIST) Special Publication 800-63-2, Electronic Authentication Guideline, August 2013, located at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf

ROSENSTEIN.MARK
.ERIC.1078644431

Digitally signed by
ROSENSTEIN.MARK.ERIC.1078644431
DN: c=US, o=U.S. Government, ou=DoD,
ou=PKI, ou=USA,
cn=ROSENSTEIN.MARK.ERIC.1078644431
Date: 2015.05.27 16:04:40 -04'00'

MARK E. ROSENSTEIN
Colonel, USA
Chief of Staff

____

*This DISA Instruction must be reissued, canceled, or certified current within 5 years of its publication date. If not, it will expire 10 years from its publication date and be removed from the DISA issuances postings.
OPR: ISC - disa.meade.eis.mbx.eis-front-office@mail.mil
DISTRIBUTION: P