DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No.: 0810011295–81636–02]

Announcing Approval of Federal Information Processing Standard (FIPS) Publication 186–3, Digital Signature Standard (DSS)

AGENCY: National Institute of Standards and Technology (NIST), Department of Commerce.

ACTION: Notice.

SUMMARY: This notice announces the Secretary of Commerce's approval of Federal Information Processing Standard (FIPS) Publication 186–3, Digital Signature Standard (DSS). FIPS 186–3 is a revision of FIPS 186–2. The FIPS specifies three techniques for the generation and verification of digital signatures that can be used for the protection of data: the Digital Signature Algorithm (DSA), the Elliptic Curve Digital Signature Algorithm (ECDSA) and the Rivest-Shamir-Adelman (RSA) algorithm. Although all three of these algorithms were approved in FIPS 186–2, FIPS 186–3 increases the key sizes allowed for DSA, provides additional requirements for the use of RSA and ECDSA, and includes requirements for obtaining the assurances necessary for valid digital signatures. FIPS 186–2 contained specifications for random number generators (RNGs); this revision does not include such specifications, but refers to NIST Special Publication (SP) 800–90 for obtaining random numbers. FIPS 186–3 is available at *http://csrc.nist.gov/publications/PubsFIPS.html;* SP 800–90 is available at *http://csrc.nist.gov/publications/PubsSPs.html.*

FOR FURTHER INFORMATION CONTACT: Elaine Barker, (301) 975–2911, National Institute of Standards and Technology, 100 Bureau Drive, STOP 8930, Gaithersburg, MD 20899–8930, e-mail: *elaine.barker@nist.gov.*

SUPPLEMENTARY INFORMATION: FIPS 186, first published in 1994, specified a digital signature algorithm (DSA) to generate and verify digital signatures. Later revisions (FIPS 186–1 and FIPS 186–2, adopted in 1998 and 1999, respectively) adopted two additional algorithms specified in American National Standards (ANS) X9.31 (Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)), and X9.62 (The Elliptic Curve Digital Signature Algorithm (ECDSA)).

The original DSA algorithm, as specified in FIPS 186, 186–1 and 186–2, allows key sizes of 512 to 1024 bits. With advances in technology, it is prudent to consider larger key sizes. FIPS 186–3 allows the use of 1024, 2048 and 3072-bit keys. Other requirements have also been added concerning the use of ANS X9.31 and ANS X9.62. In addition, the use of the RSA algorithm as specified in Public Key Cryptography Standard (PKCS) #1 (RSA Cryptography Standard) is allowed.

A **Federal Register** Notice (73 FR 66842) was published on November 12, 2008 to request public comments on the draft FIPS 186–3. A total of thirteen parties provided comments (six U.S. government agencies, one university, five private organizations, and one individual). Three parties indicated that the FIPS should be approved without changes. The following is a summary of the remaining comments received and NIST's responses to them:

Comment: Seven commenters suggested a number of editorial changes.

Response: NIST made the appropriate editorial changes, which included correcting typographical errors, format changes, minor word changes and clarifications.

Comment: One commenter suggested relaxing the requirement for hash algorithms to provide equivalent or stronger security than the public key algorithm and key size.

Response: NIST accepted the comment and substituted a requirement that both the hash algorithm and the public key algorithm and key size meet the security requirements for the application. This permits the use of a public key algorithm and key size that is stronger in security than a hash algorithm, so long as both provide sufficient security for the digital signature process. The use of hash algorithms that provide equivalent or stronger security than the public key algorithm and key size is still encouraged as a general practice.

Comment: One commenter suggested imposing additional restrictions on the selection of the public exponent *e* when generating RSA key pairs.

Response: NIST studied the suggestion and decided not to impose further restrictions on the selection of the public exponent *e.* Such restrictions would negatively impact NIST's Cryptographic Module Validation Program (CMVP) by precluding the validation of currently accepted implementations without providing a significant increase in security.

Comment: One commenter suggested relaxing requirements on the generation of the private exponent *d* to improve efficiency when generating RSA key pairs.

Response: NIST studied the suggestion and decided not to make the change, due to a risk of reducing the level of security assurance provided by the suggested method.

Comment: One commenter requested the inclusion of an alternative method for strong prime generation when generating RSA key pairs on constrained computing devices.

Response: NIST decided not to adopt the proposed method for strong prime generation. NIST would need to perform significant further study on any alternative methods before expanding the set of approved methods for strong prime generation in the FIPS. In addition, NIST believes that the methods specified in the standard can be implemented on constrained devices. If implementation experience establishes the need for alternative methods, NIST will conduct the further study necessary and, if appropriate, will include alternative techniques in a later version of the FIPS.

Comment: One commenter requested changes to enhance alignment of ECDSA domain parameter generation and management in the FIPS with American National Standard X9.62.

Response: NIST reviewed the comments and made the appropriate changes to ensure alignment with respect to the generation and management of ECDSA domain parameters. NIST deleted the statement ''ANSI X9.62 has no restriction on the maximum size of [the cofactor]'', since the current version of X9.62 imposes limitations on the size of the cofactor. NIST also revised statements regarding elliptic curve domain parameter generation for purposes other than digital signature generation.

Authority: In accordance with the Information Technology Management Reform Act of 1996 (Pub. L. 104–106) and the Federal Information Security Management Act (FISMA) of 2002 (Pub. L. 107–347), the Secretary of Commerce is authorized to approve Federal Information Processing Standards (FIPS). NIST activities to develop computer security standards to protect Federal sensitive (unclassified) information systems are undertaken pursuant to specific responsibilities assigned to NIST by section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3), as amended by section 303 of the Federal Information Security Management Act of 2002.

E.O. 12866: This notice has been determined not to be significant for the purposes of E.O. 12866.

Dated: June 1, 2009.

Patrick Gallagher,

Deputy Director.

[FR Doc. E9–13513 Filed 6–8–09; 8:45 am]

BILLING CODE 3510–13–P

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[090520915–9921–01]

Initial List of Smart Grid Interoperability Standards; Request for Comments

AGENCY: National Institute of Standards and Technology (NIST), Department of Commerce.

ACTION: Notice; request for comments.

SUMMARY: The National Institute of Standards and Technology (NIST) seeks comments on a preliminary set of smart grid interoperability standards and specifications identified for inclusion in the Smart Grid Interoperability Standards Framework, Release 1.0.

DATES: Comments must be received on or before July 9, 2009.

ADDRESSES: Written comments may be sent to: George Arnold, 100 Bureau Drive, Stop 8100, National Institute of Standards and Technology, Gaithersburg, MD 20899–8100. Electronic comments may be sent to: *smartgridcomments@nist.gov.*

The list of proposed standards and specifications is available at: *http://www.nist.gov/smartgrid/standards.html.* Additional information may be found at: *http://www.nist.gov/smartgrid.*

FOR FURTHER INFORMATION CONTACT: George Arnold, 100 Bureau Drive, Stop 8100, National Institute of Standards and Technology, Gaithersburg, MD 20899–8100, telephone (301) 975–5627.

SUPPLEMENTARY INFORMATION: Section 1305 of the Energy Independence and Security Act (EISA) of 2007 (Pub. L. 110–140) requires the Director of the National Institute of Standards and Technology (NIST) ''to coordinate the development of a framework that includes protocols and model standards for information management to achieve interoperability of smart grid devices and systems.'' NIST has identified an initial set of standards and specifications listed in the box below for inclusion in Release 1.0 of the Smart Grid Interoperability Standards Framework. Release 1.0 is a work in progress. It is not complete, nor is it exclusionary. Existing standards that do not appear in this first installment to Release 1.0 have not been eliminated from consideration. Standards that currently appear on the list ultimately may not be included.

This initial set of standards represents the first step in Phase I of the NIST three-phase plan for smart grid interoperability. The full plan is available at: *http://www.nist.gov/public_affairs/smartgrid_041309.html.*

To assist in carrying out its plan, NIST awarded a contract to Electric Power Research Institute (EPRI) to organize and facilitate two workshops, held on April 28–29, 2009 and May 19–20, 2009. Under its contract, EPRI is also required to use its technical expertise to compile, distill, and organize stakeholder contributions into a draft interim roadmap for smart grid interoperability standards. The proposed set of standards is based on input received from participants in the public Smart Grid Interoperability Standards Interim Roadmap Workshop I, held on April 28–29 in Reston, Virginia. Notes and outcomes of the workshop can be found at *http://collaborate.nist.gov/twiki-sggrid/bin/view/_SmartGridInterimRoadmap/InterimRoadmapWorkshop1*.

The more than 400 people who participated in the April 28–29 workshop represented a large cross-section of smart grid stakeholders. NIST recognizes, however, that not all interested stakeholders participated in the workshop. Arranged in alphabetical order, the list of proposed standards and specifications will be expanded as the process continues and as the standards framework is developed further to support the functionality envisioned for the Smart Grid and as technology evolves.

Although not included in this initial list, communication standards pertaining to basic connectivity and data networking are also important for Smart Grid interoperability. They will be part of the interoperability framework. Initial standards in these categories will be evaluated following the Smart Grid Interim Standards Roadmap Workshop II, held on May 19–20. Altogether, several hundred standards that are identified or developed over the span of several years may be required to achieve secure, end-to-end interoperability across a fully implemented Smart Grid.

NIST recognizes that the standards and specifications listed below will require further development and that many additional standards and specifications are needed to achieve interoperability of Smart Grid devices and systems. Updated versions of the Smart Grid Interoperability Framework will be published periodically to include additional standards as they are recognized by NIST and to remove standards from the list, as appropriate, as the coordination process moves forward.

Standard	Application
AMI–SEC System Security Requirements	Advanced metering infrastructure (AMI) and Smart Grid end-to-end security.
ANSI C12.19/MC1219	Revenue metering information model.
BACnet ANSI ASHRAE 135–2008/ISO 16484–5	Building automation.
DNP3	Substation and feeder device automation.
IEC 60870–6/TASE.2	Inter-control center communications.
IEC 61850	Substation automation and protection.
IEC 61968/61970	Application level energy management system interfaces.
IEC 62351 Parts 1–8	Information security for power system control operations.
IEEE C37.118	Phasor measurement unit (PMU) communications.
IEEE 1547	Physical and electrical interconnections between utility and distributed generation (DG).
IEEE 1686–2007	Security for intelligent electronic devices (IEDs).
NERC CIP 002–009	Cyber security standards for the bulk power system.
NIST Special Publication (SP) 800–53, NIST SP 800–82.	Cyber security standards and guidelines for federal information systems, including those for the bulk power system.
Open Automated Demand Response (Open ADR)	Price responsive and direct load control.
OpenHAN	Home Area Network device communication, measurement, and control.
ZigBee/HomePlug Smart Energy Profile	Home Area Network (HAN) Device Communications and Information Model.