myProject™ - P1363.1 PAR Detail

Submitter Email: wwhyte@ntru.com
Type of Project: New IEEE Standard
PAR Request Date: 27-Oct-2000
PAR Approval Date: 07-Dec-2000
PAR Expiration Date: 31-Dec-2008
PAR Signature Page on File: Yes
Status: PAR for a New IEEE Standard
Project: 1363.1
Root Project:

1.1 Project Number: P1363.1
1.2 Type of Document: Standard
1.3 Life Cycle: Full Use
1.4 Is this project in ballot now? Yes
Invitation History

2.1 Title: Standard Specification for Public-Key Cryptographic Techniques Based on Hard Problems over Lattices

3.1 Working Group: Working Group for Public-Key Cryptographic (C/MSC/1363_WG)
Contact Information for Working Group Chair
William Whyte
Email: wwhyte@ntru.com
Phone: 508 878 4585
Contact Information for Working Group Vice-Chair
None

3.2 Sponsoring Society and Committee: IEEE Computer Society/Microprocessors and Microcomputers (C/MSC)
Contact Information for Sponsor Chair
James R Davis
Email: bob@scsi.com
Phone: 408-353-2706/408-857-1273 Cell
Contact Information for Standards Representative
None

4.1 Type of Ballot: Individual
4.2 Expected Date of Submission for Initial Sponsor Ballot: 01/2008
4.3 Projected Completion Date for Submittal to RevCom: 07/2008

5.1 Approximate number of people expected to work on this project: 15
5.2 Scope: Specifications of common public-key cryptographic techniques based on hard problems over lattices supplemental to those considered in IEEE 1363 and IEEE P1363a, including mathematical primitives for secret value (key) derivation, public-key encryption, identification and digital signatures, and cryptographic schemes based on those primitives. Specifications of related cryptographic parameters, public keys and private keys. Class of computer and communications systems is not restricted.
5.3 Is the completion of this standard dependent upon the completion of another standard: No

5.4 Purpose: The transition from paper to electronic media brings with it the need for electronic privacy and authenticity. Public-key cryptography offers fundamental technology addressing this need. Many alternative public-key techniques have been proposed, each with its own benefits. The IEEE 1363 Standard and P1363a project have produced a comprehensive reference defining a range of common public-key techniques covering key agreement, public-key encryption and digital signatures from several families, namely the discrete logarithm, integer factorization, and elliptic curve families. IEEE P1363.1 will specify cryptographic techniques based on hard problems over lattices. These techniques may offer tradeoffs in operating characteristics when compared with the methods already specified in IEEE 1363-2000 and draft P1363a. It is also intended that P1363.1 provide a second-generation framework for the description of cryptographic techniques, as compared to the initial framework provided in 1363-2000 and draft P1363a. It is not the purpose of this project to mandate any particular set of public-key techniques or security requirements (including key sizes) for this or any family. Rather, the purpose is to provide: (1) a reference for specification of a variety of techniques from which applications may select, (2) the relevant number-theoretic background, and (3) extensive discussion of security and implementation considerations so that a solution provider can choose appropriate security requirements for itself.

5.5 Need for the Project:

5.6 Stakeholders for the Standard:

Intellectual Property

6.1.a. Has the IEEE-SA policy on intellectual property been presented to those responsible for preparing/submitting this PAR prior to the PAR submittal to the IEEE-SA Standards Board? Yes

6.1.b. Is the Sponsor aware of any copyright permissions needed for this project? No

6.1.c. Is the Sponsor aware of possible registration activity related to this project? No

7.1 Are there other standards or projects with a similar scope? No

7.2 Future Adoptions

Is there potential for this standard (in part or in whole) to be adopted by another national, regional, or international organization? Unknown

7.3 Will this project result in any health, safety, security, or environmental guidance that affects or applies to human health or safety? No

7.4 Additional Explanatory Notes: (Item Number and Explanation)