

[Email This Letter](#)

23 September 2005

Bob Davis
Summit Computer System, Inc.
22685 Summit Road
Los Gatos, CA 95033-9310
bob@scsi.com

Re: P1363 - Standard Specifications for Public Key Cryptography

Dear Bob:

I am pleased to inform you that on 22 September 2005 the IEEE-SA Standards Board approved the above referenced project until 31 December 2009. A copy of the file can be found on our website at <http://standards.ieee.org/board/nes/projects/1363.pdf>.

Now that your project has been approved, please forward a roster of participants involved in the development of this project. This request is in accordance with the IEEE-SA Operations Manual, Clause 5.1.2i under Duties of the Sponsor which states:

"Submit annually to the IEEE Standards Department an electronic roster of individuals participating on standards projects"

For your convenience, an Excel spreadsheet for your use has been posted on our website at <http://standards.ieee.org/guides/par/roster.xls>. Please forward this list to me via e-mail at j.haasz@ieee.org no later than 21 December 2005.

Please visit our website, IEEE Standards Development Online (<http://standards.ieee.org/resources/development/index.html>), for tools, forms and training to assist you in the standards development process. Also, we strongly recommend that a copy of your draft be sent to this office for review prior to the final vote by the working group to allow for a quick review by editorial staff before sponsor balloting begins.

If you should have any further questions, please contact me at 732-562-6367 or by email at j.haasz@ieee.org.

Sincerely,

Jodi Haasz
Program Manager
International Stds Programs and Governance
Standards Activities
Phone +1 732 562 6367
FAX +1 732 875 0695
Email: j.haasz@ieee.org

CC: wwhyte@ntru.com

PAR FORM

PAR Status: Revision PAR

PAR Approval Date: 2005-09-22

PAR Signature Page on File: Yes

1. Assigned Project Number: P1363

2. Sponsor Date of Request: 2005-07-11

3. Type of Document:

4. Title of Document:

Draft: Standard Specifications for Public Key Cryptography

5. Life Cycle: Full-Use

6. Type of Project:

6a. Is this an update to an existing PAR? No

6b. The Project is a: Revision of Std 1363-2000

7. Working Group Information:

Name of Working Group: Working Group for Public-Key Cryptographic

Approximate Number of Expected Working Group Members:12

8. Contact information for Working Group Chair:

Name of Working Group Chair: William Whyte

Telephone: 781-418-2534 **FAX:** 781-418-2532

Email: wwwhyte@ntru.com

9. Contact information for Co-Chair/Official Reporter, Project Editor or Document Custodian if different from the Working Group Chair:

Name of Co-Chair/Official Reporter, Project Editor or Document Custodian:

Telephone: FAX:

Email:

10. Contact information for Sponsoring Society or Standards Coordinating Committee:

Name of Sponsoring Society and Committee: IEEE Computer Society Microprocessors and Microcomputers

Name of Sponsoring Committee Chair: Bob Davis

Telephone: 408-353-2706 **FAX:** 408-353-8116

Email: bob@scsi.com

Name of Liaison Rep. (if different from the Sponsor Chair):

Telephone: FAX:

Email:

Name of Co-Sponsoring Society and Committee:**Name of Co-Sponsoring Committee Chair:****Telephone: FAX:****Email:****Name of Liaison Rep. (if different from the Sponsor Chair):****Telephone: FAX:****Email:****11. The Type of ballot is:** Individual Sponsor Ballot**Expected Date of Submission for Initial Sponsor Ballot:** August 2006**12. Projected Completion Date for Submittal to RevCom:** January 2007**Target Extension Request Information for a Modified PAR whose completion date is being extended past the original four-year life of the PAR:****13. Scope of Proposed Project:**

This document will provide the specifications of common public-key cryptographic techniques, including mathematical primitives for secret value (key) derivation, public-key encryption, digital signatures, and identification, and cryptographic schemes based on those primitives. It also includes specifications of related cryptographic parameters, public keys and private keys. Class of computer and communications systems is not restricted.

Is the completion of this document contingent upon the completion of another document?

No

14. Purpose of Proposed Project:

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. However, there has been no single, comprehensive reference defining a wide range of common public-key techniques covering key agreement, public-key encryption, digital signatures, and identification from several families, such as discrete logarithms, integer factorization, and elliptic curves. It is not the purpose of this project to mandate any particular set of public-key techniques, or particular attributes of public-key techniques such as key sizes. Rather, the purpose is to provide a reference for specifications of a variety of techniques from which applications may select. This document merges the basic techniques specified in IEEE Std 1363-2000 with the additional techniques specified in IEEE Std 1363a-2004.

15. Reason for the Proposed Project:

This Revision project will develop a document that merges the basic techniques specified in IEEE Std 1363-2000 with the additional techniques specified in IEEE Std 1363a-2004 and some technical changes based on advances in cryptographic research since the publication of these existing documents. There may be some technical changes based on advances in cryptographic research since the publication of 1363-2000 and 1363a-2004, but these are not expected to be extensive. The Class of computer and communications systems is not restricted. The stakeholders are the current users of these well established cryptographic techniques.

16. Intellectual Property:

- a. Has the IEEE-SA policy on intellectual property been presented to those responsible for preparing/submitting this PAR? Yes 2005-07-11
- b. Is the sponsor aware of copyright permissions needed for this project? No
- c. Is the sponsor aware of trademarks that apply to this project? No
- d. Is the sponsor aware of possible registration activity related to this project? No

17. Are there other documents or projects with a similar scope? No

Similar Scope Project Information:

18. Is there potential for this document (in part or in whole) to be adopted by another national , regional or international organization? Do not know at this time

If yes, the following questions must be answered:

Organization Name?

Technical

Committee

International

Contact

Information?

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

If yes, please explain:

20. Sponsor Information

a. Is the scope of this project within the approved/scope/definition of the Sponsor's Charter? Yes

If no, please explain:

b. The Sponsor's procedures have been accepted by the IEEE-SA Standards Board Audit Committee? Yes

21. Additional Explanatory Notes: (Item Number and Explanation)