Summary of the P1363.2 Ballot Review Group
August 28, 2007

This memo summarizes the purpose and actions of the P1363.2 Ballot Review Group.

Purpose of the Ballot Review Group

The purpose of the P1363.2 Ballot Review Group (BRG) is to address the comments received during Sponsor Ballot of P1362.2 [5], and recommend adaptation to the Microprocessor Standards Committee (MSC), the Sponsor of IEEE P1363 [1]. The BRG takes into account comments received during Sponsor Ballot, in light of the interests of the P1363 Working Group (WG) and the IEEE Standards Association (SA) [4], which range from accuracy and clarity of presentation of technical content to interest in completing the standard in a timely manner, in accordance with IEEE SA practices as documented in [2] and [3].

Members of the BRG

As of July 24, there are five members of the BRG:

Matt Ball	<matt.ball@quantum.com>	
Mike Brenner	<mikeb@mitre.org>	*P1363 Primary Editor*
David Jablon	<jablon1363@yahoo.com>	*P1363.2 document editor*
Phil MacKenzie	<philmac@gmail.com>	
Marc Provencher	<m.provencher@ieee.org>	
William Whyte	<wwhyte@ntru.com>	*P1363 Chair*

Document Status

Draft D27 of IEEE P1363.2 was approved for submission to sponsor ballot by the WG on September 28th, 2006. The P1363.2 sponsor ballot opened on March 24, 2007 and closed on April 21, 2007, with the following results:

RESPONSE RATE: This ballot met the 75% minimum returned ballot requirement.

- 55 eligible people in this ballot group.
- 37 affirmative votes
- 0 negative votes with comments
- 0 negative votes without comments
- 6 abstention votes
- 43 votes received = 78 % returned, 14 % abstention

APPROVAL RATE: The 75% minimum affirmation requirement was met.

- 37 affirmative votes
- 0 negative votes with comments
- 37 votes = 100% affirmative

There were 103 comments received with affirmative ballots, zero comments with negative ballots, another 11 comments from IEEE Editorial Coordination Legal review, and an additional 4 comments by members of the BRG for a total of 118 comments. Among these, 23 were listed as *General*, 1 as *Technical* (Comment # 99), and 94 as *Editorial*. The 11 comments from IEEE Legal review were designated *Must be satisfied*.

Actions of the BRG

The P1363.2 document editor received the comments on July 6, 2007 and reviewed them in preparation for establishing the BRG. Invitations to join the BRG were sent on July 16 to those who submitted Comments during Sponsor Ballot and to the subscribers of Stds-P1363-Discuss mailing list, representing the current active members of

the P1363 Working Group. The open invitation expired at the end of July 19, at which time 5 people accepted membership, and the BRG reserved the right to invite additional members as needed. The BRG planned to review and address comments during July and August, and to present the results of their review to the P1363 Working Group in its August meeting. The BRG's first task was to review and come to agreement on the appropriate membership of the BRG and general plan for proceeding. The next tasks were to review the draft and comments, and to create recommendations for how to address the comments.

The Ballot comments were initially classified as either General, Editorial, or Technical. All such classifications were reviewed by the BRG. One of the comments that was classified as "General" was reclassified by the BRG as Technical (Comment # 103), one that was classified as Technical was reclassified as Editorial (Comment # 99), and the rest of the General comments were reclassified as Editorial (# 1-3, 30, 33, 96-97, 100, 102, 104-114). Among the ballot comments, 11 were duplicates of the 11 Legal comments, although one had a different proposed change. The 11 comments from IEEE Legal (and their 11 duplicates) were designated as "must be satisfied", and must be satisfied before the document can go to RevCom.

As the 92 remaining comments from the Ballot Group were all associated with affirmative votes, and it is not necessary to accommodate formally or reply to comments associated with an affirmative vote, the BRG determined that these comments do not need to be satisfied before the document can go to RevCom, and can be addressed at the discretion of the Sponsor. However, the BRG recommends changes for all but one of these comments.

Recommendations

The BRG documented recommendations for addressing each comment, as shown in Appendix A. The BRG recommends that changes for all but one of the comments be incorporated in the next draft in the belief that they are justified and can be implemented without raising objections from other balloters. One comment (# 103) was rejected by the BRG, as explained in Appendix A.

For each of the comments related to IEEE legal review that were designated as must be satisfied, the BRG either accepted the proposed change, or proposed an alternative change to satisfy the comment, as detailed in [6].

As all of the comments accepted by the BRG were Editorial, and as the BRG did not consider any of the recommend changes to be substantive changes, the BRG recommends that a recirculation ballot is not necessary.

References

[1] IEEE P1363 Working Group (WG) - Standard Specifications For Public-Key Cryptography, http://grouper.ieee.org/groups/1363/

[2] IEEE-SA Standards Board Operations Manual, http://standards.ieee.org/guides/opman/sect5.html

[3] IEEE Standards Companion, http://standards.ieee.org/guides/companion

[4] IEEE Standards Association (SA), http://standards.ieee.org/

[5] IEEE P1363.2: *Standard Specifications for Password-Based Public-Key Cryptographic Techniques*, Draft D27, November 2006, (first Sponsor Ballot draft).

[6] IEEE P1363.2: *Standard Specifications for Password-Based Public-Key Cryptographic Techniques*, Draft D28, August 23, 2007, (first Sponsor Ballot draft, as amended and annotated by the BRG).

Appendix A: Summary of Comments & Resolution

==========
Comment # 1: (Page 8, line 14, subclause 4.4)
The formatting for the text often merges two consecutive characters together. An example can be seen in the word "components" in line 14 of page 8

Proposed Change:
Correct the formatting

Resolution: Accept
Change as proposed, if possible. Otherwise add Editor's Note for IEEE editors.

==========
Comment # 2: (Page 3, line 14, subclause 1.4.1)
The formatting for the text often appears to insert a blank space in a word. An example can be seen in the word "that" in line 14 of page 3

Proposed Change:
Correct the formatting

Resolution: Accept
Change as proposed, if possible. Otherwise add Editor's Note for IEEE editors.

==========
Comment # 3: (Page iv(2), subclause Contents)
The page numbers beginning with clause 9 are incorrect

Proposed Change:
Use correct page numbers

Resolution: Accept

==========
Comment # 4: (Page 4, line 23, subclause 3)
Definition numbering is incorrect

Proposed Change:
Number as 3.1

Resolution: Accept

==========
Comment # 5: (Page 4, line 24, subclause 3)
Poor grammar

Proposed Change:
Delete the second word in the line

Resolution: Accept

==========
Comment # 6: (Page 4, line 26, subclause 3)
Definition numbering is incorrect

Proposed Change:

Number as 3.2

Resolution: Accept

==========
Comment # 7: (Page 4, line 29, subclause 3)
Definition numbering is incorrect

Proposed Change:
Number as 3.3

Resolution: Accept

==========
Comment # 8: (Page 4, line 34, subclause 3)
Definition numbering is incorrect

Proposed Change:
Number as 3.4

Resolution: Accept

==========
Comment # 9: (Page 4, line 36, subclause 3)
Definition numbering is incorrect

Proposed Change:
Number as 3.5

Resolution: Accept

==========
Comment # 10: (Page 5, line 1, subclause 3)
Definition numbering is incorrect

Proposed Change:
Number as 3.6

Resolution: Accept

==========
Comment # 11: (Page 5, line 5, subclause 3)
Definition numbering is incorrect

Proposed Change:
Number as 3.7

Resolution: Accept

==========
Comment # 12: (Page 5, line 6, subclause 3)
Definition numbering is incorrect

Proposed Change:
Number as 3.8

Resolution: Accept

==========
Comment # 13: (Page 5, line 10, subclause 3)
Definition numbering is incorrect

Proposed Change:
Number as 3.9

Resolution: Accept

==========
Comment # 14: (Page 5, line 12, subclause 3)
Definition numbering is incorrect

Proposed Change:
Number as 3.10

Resolution: Accept

==========
Comment # 15: (Page 5, line 15, subclause 3)
Definition numbering is incorrect

Proposed Change:
Number as 3.11

Resolution: Accept

==========
Comment # 16: (Page 5, line 17, subclause 3)
Definition numbering is incorrect

Proposed Change:
Number as 3.12

Resolution: Accept

==========
Comment # 17: (Page 5, line 22, subclause 3)
Definition numbering is incorrect

Proposed Change:
Number as 3.13

Resolution: Accept

==========
Comment # 18: (Page 5, line 23, subclause 3)
The sentence at the end of the line begins with the number 2, but there is no number 1

Proposed Change:
Delete the number or add a number 1 to the first sentence

Resolution: Accept
Add "1." before the first sentence.

==========
Comment # 19: (Page 5, line 26, subclause 3)
Definition numbering is incorrect

Proposed Change:
Number as 3.14

Resolution: Accept

==========
Comment # 20: (Page 5, line 28, subclause 3)
Definition numbering is incorrect

Proposed Change:
Number as 3.15

Resolution: Accept

==========
Comment # 21: (Page 5, line 30, subclause 3)
Definition numbering is incorrect

Proposed Change:
Number as 3.16

Resolution: Accept

==========
Comment # 22: (Page 5, line 32, subclause 3)
Definition numbering is incorrect

Proposed Change:
Number as 3.17

Resolution: Accept

==========
Comment # 23: (Page 5, line 34, subclause 3)
Definition numbering is incorrect

Proposed Change:
Number as 3.18

Resolution: Accept

==========
Comment # 24: (Page 5, line 38, subclause 3)
Definition numbering is incorrect

Proposed Change:
Number as 3.19

Resolution: Accept

==========

Comment # 25: (Page 5, line 39, subclause 3)
Definition numbering is incorrect

Proposed Change:
Number as 3.20

Resolution: Accept

==========

Comment # 26: (Page 6, line 4, subclause 3)
Definition numbering is incorrect

Proposed Change:
Number as 3.21

Resolution: Accept

==========

Comment # 27: (Page 6, line 6, subclause 3)
Definition numbering is incorrect

Proposed Change:
Number as 3.22

Resolution: Accept

==========

Comment # 28: (Page 6, line 9, subclause 3)
Definition numbering is incorrect

Proposed Change:
Number as 3.23

Resolution: Accept

==========

Comment # 29: (Page 6, line 11, subclause 3)
Definition numbering is incorrect

Proposed Change:
Number as 3.24

Resolution: Accept

"==========

Comment # 30: (Page 14, line 1, subclause 4.7.1)
This list needs to contain all trhe acronyms used in this document and the expansion of the acronym, not just the acronyms unique to this document (e.g. IEEE, NIST, FIPS). Also the normal convention of expressing the expansion of an acronym when first used shuld be employed in this document as well

Proposed Change:
Add list of acronym and follow standard acronym convention

Resolution: Accept
Move 4.7.1 to 3.2, in accordance with IEEE style guide treatment of acronyms and abbreviations, and in 4.7 par. 1, delete the words "", followed by a summary of acronyms"".

Amend ""Acronyms and abbreviations"" subclause (now 3.2) to cite bibliography references for AMP, PAK, PPK, SPEKE, SRP.

Note that some acronyms in cited references are used merely as parts of names or identifiers, where the expansion of the acronym is irrelevant to this standard. For example, ""RFC"" is a designation specific to IETF standards that is expanded within the appropriate IETF references. Similarly, AMP, PAK, PPK, SPEKE, SRP were acronyms that are re-used merely as identifiers within the names of techniques defined in this standard, where the expansion of the original acronym is not particularly relevant to this standard.

Use of ""IEEE"" seems to be in accordance with IEEE practices.

==========

Comment # 31: (Page 45, line 38, subclause 9.1.1)
This paragrapgh should be formatted the same as the paragraph which precedes it.

Proposed Change:
Reformat paragraph

Resolution: Accept

==========

Comment # 32: (Page 19, line 40, subclause 8.1.3)
some headings are at end of page

Proposed Change:
move heading to next page

Resolution: Accept
Change as proposed. (Error in IEEE Document Template. Should change paragraph formatting of "IEEEStds Level 2 Header" style to "keep with next".)

==========

Comment # 33: ()
Safety: From MEC legal review, use of the terms "safe," "safety," and "safely" are deemed appropriate in contexts in which tangible harm to people and/or animals is a concern. Also, the term "safe" may be appropriate in the context of a "safe" choice or option. However, in contexts in which intangible harms are addressed, another term should be used. For example, in the context of the electronic transactions at issue in this document, terms such as "secure" or "reliable" are more appropriate. Specific changes along these lines are described below.

Proposed Change:
See list of changes below.

Resolution: Accept
Change per Comments # 34-47.

==========

Comment # 34: (Page ii, line 5, subclause Abstract)
See Safety comment [#33] above. No replacement word is needed because "securing" is already used in the sentence.

Proposed Change:
p. ii: Delete "safely".

Resolution: Accept

==========
Comment # 35: (Page 1, line 8, subclause 1.1)
See Safety comment [#33] above. No replacement word is needed because "securing" is already used in the sentence.

Proposed Change:
p. 1: Delete "safely".

Resolution: Accept

==========
Comment # 36: (Page 1, line 19, subclause 1.2)
See Safety comment [#33] above.

Proposed Change:
p. 1: Change "safely" to "securely".

Resolution: Accept

==========
Comment # 37: (Page 6, line 23, subclause 4.1)
See Safety comment [#33] above.

Proposed Change:
p. 6: Change "safely" to "securely".

Resolution: Accept

==========
Comment # 38: (Page 11, line 8, subclause 4.4.5)
See Safety comment [#33] above. The word "safely" is redundant in this context.

Proposed Change:
p. 11: Delete "safely".

Resolution: Accept

==========
Comment # 39: (Page 56, line 16, subclause 9.4.3.2)
See Safety comment [#33] above.

Proposed Change:
p. 56: Change "safely" to "reliably".

Resolution: Accept

==========
Comment # 40: (Page 106, line 45, subclause D.2.1.4)
See Safety comment [#33] above.

Proposed Change:
p. [106]: Change "safely used" to "used reliably".

Resolution: Accept

==========

Comment # 41: (Page 107, line 47, subclause D.2.1.5)
See Safety comment [#33] above.

Proposed Change:
p. 107: Change "To be safe, one can always" to "One can securely".

Resolution: Accept

==========
Comment # 42: (Page 108, line 32, subclause D.2.1.6)
See Safety comment [#33] above.

Proposed Change:
p. 108: Change "safely revealed" to "revealed without compromising security".

Resolution: Accept

==========
Comment # 43: (Page 108, line 35, subclause D.2.1.6)
See Safety comment [#33] above.

Proposed Change:
p. 108: Delete "safely" and append "without compromising security" after "valid public key".

Resolution: Accept

==========
Comment # 44: (Page 108, line 37, subclause D.2.1.6)
See Safety comment [#33] above.

Proposed Change:
p. 108: Delete "safely" and append "without compromising security" after "this step".

Resolution: Accept

==========
Comment # 45: (Page 109, line 26, subclause D.2.1.9)
See Safety comment [#33] above.

Proposed Change:
p. 109: Change "safe" to "secure" [in D.2.1.9].

Resolution: Accept

==========
Comment # 46: (Page 109, line 29, subclause D.2.1.9.1)
See Safety comment [#33] above.

Proposed Change:
p. 109: Change "Safe" to "Secure".

Resolution: Accept

==========
Comment # 47: (Page 120, line 10, subclause D.2.2.3.2)
See Safety comment [#33] above. The word "safely" is redundant in this context.

Proposed Change:
p. 120: Delete "safely".

Resolution: Accept

==========
Comment # 48: (Page 11, line 51, subclause 4.5)
For clarity:

Proposed Change:
p. 11: Change "addressed in more detail" to "addressed for informational purposes".

Resolution: Accept

==========
Comment # 49: (Page 107, line 27, subclause D.2.1.5)
Avoid an unnecessary characterization of a testing method.

Proposed Change:
p. 107: Delete "sure".

Resolution: Accept

==========
Comment # 50: ()
Adversary: In light of MEC legal review and subsequent WG discussion, recommend changing the word "enemy" to either "adversary" or "attacker" throughout the document, using "adversary" for the general case, and "attacker" for cases that refer to a specific attack. Accordingly, replace "attacker" with "adversary", where appropriate. Specific changes along these lines are described below.

Proposed Change:
See list of changes below.

Resolution: Accept
Change per Comments # 51-81.

==========
Comment # 51: (Page 4, line 24, subclause 3)
See Adversary comment [#50] above.

Proposed Change:
p. 4: Change "attacker" to "adversary".

Resolution: Accept

==========
Comment # 52: (Page 7, line 12, subclause 4.2)
See Adversary comment [#50] above.

Proposed Change:
p. 7: Change "enemy" to "adversary".

Resolution: Accept

==========

Comment # 53: (Page 7, line 15, subclause 4.2)
See Adversary comment [#50] above.

Proposed Change:
p. 7: Change "enemy" to "adversary".

Resolution: Accept

==========
Comment # 54: (Page 10, line 8, subclause 4.4.3)
See Adversary comment [#50] above.

Proposed Change:
p. 10: Change "attacker" to "adversary".

Resolution: Accept

==========
Comment # 55: (Page 10, line 10, subclause 4.4.3)
See Adversary comment [#50] above.

Proposed Change:
p. 10: Change "attacker" to "adversary".

Resolution: Accept

==========
Comment # 56: (Page 10, line 11, subclause 4.4.3)
See Adversary comment [#50] above.

Proposed Change:
p. 10: Change "attacker" to "adversary".

Resolution: Accept

==========
Comment # 57: (Page 10, line 12, subclause 4.4.3)
See Adversary comment [#50] above.

Proposed Change:
p. 10: Change "attacker" to "adversary".

Resolution: Accept

==========
Comment # 58: (Page 73, line 4, subclause 9.8.3.2)
See Adversary comment [#50] above.

Proposed Change:
p. 73: Change "attacker" to "adversary".

Resolution: Accept

==========
Comment # 59: (Page 73, line 5, subclause 9.8.3.2)
See Adversary comment [#50] above.

Proposed Change:
p. 73: Change "attacker" to "adversary".

Resolution: Accept

==========
Comment # 60: (Page 100, line 40, subclause C.1.1.8)
See Adversary comment [#50] above.

Proposed Change:
p. 94: Change "enemy" to "adversary".

Resolution: Accept

==========
Comment # 61: (Page 96, line 16, subclause B.1.1.2)
See Adversary comment [#50] above.

Proposed Change:
p. 96: Change "attacker" to "adversary".

Resolution: Accept

==========
Comment # 62: (Page 100, line 18, subclause C.1.1.7)
See Adversary comment [#50] above.

Proposed Change:
p. 100: Change "attacker" to "adversary".

Resolution: Accept

==========
Comment # 63: (Page 101, line 14, subclause C.2.1)
See Adversary comment [#50] above.

Proposed Change:
p. 101: Change "attacker" to "adversary".

Resolution: Accept

==========
Comment # 64: (Page 107, line 33, subclause D.2.1.5)
See Adversary comment [#50] above.

Proposed Change:
p. 107: Change "attacker" to "adversary".

Resolution: Accept

==========
Comment # 65: (Page 107, line 34, subclause D.2.1.5)
See Adversary comment [#50] above.

Proposed Change:

p. 107: Change "attacker" to "adversary".

Resolution: Accept
Change as proposed, and make same change in two more places in fifth paragraph of D.2.1.5.

==========
Comment # 66: (Page 108, line 8, subclause D.2.1.6)
See Adversary comment [#50] above.

Proposed Change:
p. 108: Change "attacker" to "adversary".

Resolution: Accept

==========
Comment # 67: (Page 110, line 4, subclause D.2.1.9.1)
See Adversary comment [#50] above.

Proposed Change:
p. 110: Change "enemy" to "adversary".

Resolution: Accept

==========
Comment # 68: (Page 110, line 17, subclause D.2.1.10)
See Adversary comment [#50] above.

Proposed Change:
p. 110: Change "attacker" to "adversary".

Resolution: Accept

==========
Comment # 69: (Page 110, line 21, subclause D.2.1.10)
See Adversary comment [#50] above.

Proposed Change:
p. 110: Change "attacker" to "adversary".

Resolution: Accept

==========
Comment # 70: (Page 111, line 1, subclause D.2.1.12)
See Adversary comment [#50] above.

Proposed Change:
p. 111: Change "attacker" to "adversary".

Resolution: Accept

==========
Comment # 71: (Page 111, line 24, subclause D.2.1.13)
See Adversary comment [#50] above.

Proposed Change:
p. 111: Change "attacker" to "adversary".

Resolution: Accept

==========
Comment # 72: (Page 117, line 37, subclause D.2.2.1.4)
See Adversary comment [#50] above.

Proposed Change:
p. 111: Change "enemy" to "adversary".

Resolution: Accept

==========
Comment # 73: (Page 113, line 14, subclause D.2.1.15.3)
See Adversary comment [#50] above.

Proposed Change:
p. 113: Change "attacker" to "adversary".

Resolution: Accept

==========
Comment # 74: (Page 115, line 31, subclause D.2.1.21)
See Adversary comment [#50] above.

Proposed Change:
p. 115: Change "attacker" to "adversary".

Resolution: Accept

==========
Comment # 75: (Page 118, line 4, subclause D.2.2.1.5)
See Adversary comment [#50] above.

Proposed Change:
p. 118: Change "enemy" to "adversary".

Resolution: Accept

==========
Comment # 76: (Page 118, line 29, subclause D.2.2.2.2)
See Adversary comment [#50] above.

Proposed Change:
p. 118: Change "attacker" to "adversary".

Resolution: Accept

==========
Comment # 77: (Page 120, line 9, subclause D.2.2.3.2)
See Adversary comment [#50] above.

Proposed Change:
p. 120: Change "attacker" to "adversary".

Resolution: Accept

==========
Comment # 78: (Page 121, line 10, subclause D.2.2.3.4.2)
See Adversary comment [#50] above.

Proposed Change:
p. 121: Change "enemy" to "adversary".

Resolution: Accept

==========
Comment # 79: (Page 121, line 11, subclause D.2.2.3.4.2)
See Adversary comment [#50] above.

Proposed Change:
p. 121: Change "enemy" to "adversary".

Resolution: Accept

==========
Comment # 80: (Page 121, line 13, subclause D.2.2.3.4.2)
See Adversary comment [#50] above.

Proposed Change:
p. 121: Change "enemy" to "adversary".

Resolution: Accept

==========
Comment # 81: (Page 122, line 38, subclause D.2.2.4.4)
See Adversary comment [#50] above.

Proposed Change:
p. 122: Change "enemy" to "attacker".

Resolution: Accept

==========
Comment # 82: (Page 4, line 23, subclause 3)
Missing subclause numbers.

Proposed Change:
p. 4: Add subclause numbers for first 5 Definitions, and correct subsequent subclause numbers.

Resolution: Accept

==========
Comment # 83: (Page 102, line 20, subclause C.2.5.1)
Incorrect grammar.

Proposed Change:
p. 102: Change "AMP most efficient." to "AMP is most efficient."

Resolution: Accept

==========

Comment # 84: (Page 111, line 6, subclause D.2.1.12)
Incorrect punctuation.

Proposed Change:
p. 111: Delete the comma in "easier than, an".

Resolution: Accept

==========
Comment # 85: (Page 111, line 20, subclause D.2.1.13)
Apparent typographical error in "of the is large" [in D.2.1.13].

Proposed Change:
p. 111: Change "of the is large" to "is large".

Resolution: Accept

==========
Comment # 86: (Page 115, line 49, subclause D.2.1.21)
Incorrect use of apostrpohe in "Server's".

Proposed Change:
p. 115: Change "Server's" to "Servers".

Resolution: Accept

==========
Comment # 87: (Page 47, line 32, subclause 9.2)
Inconsistent formatting.

Proposed Change:
p. 47: Insert a blank line after line 31.

Resolution: Accept

==========
Comment # 88: (Page i, line 27, subclause Title page)
On page i, Editor's Note 2 is incorrect now that drawings have been merged into the file.

Proposed Change:
p. i: Delete Editor's Note 2 on page i.

Resolution: Accept

==========
Comment # 89: (Page iv(2), subclause Contents)
Duplicate page number "iv", possibly a template problem.

Proposed Change:
p. iv: Change numbers of second page "iv" and page "v" to "v" and "vi".

Resolution: Accept

==========
Comment # 90: (Page iv(2), subclause Contents)
Most page numbers in the table of contents are incorrect.

Proposed Change:
p. iv: Update the page numbers for all TOC entries.

Resolution: Accept

==========
Comment # 91: (Page 4, line 23, subclause 3)
Definitions on this page are without numbering, not sorted correctly with definitions on next pages.

Proposed Change:

Resolution: Accept

==========
Comment # 92: (Page 6, line 41, subclause 4.2)
"See Error! Reference source not found." in footnote :)

Proposed Change:

Resolution: Accept
Change per # 101.

==========
Comment # 93: (Page 15, line 31, subclause 5.2.1)
Line 31 should be deleted - repeated contents of line 30.

Proposed Change:
[Delete the extra copy of ", where n is a hexadecimal digit".]

Resolution: Accept

==========
Comment # 94: (Page 45, line 38, subclause 9.1.1)
Missing bullet

Proposed Change:

Resolution: Accept

==========
Comment # 95: (Page 111, line 6, subclause D.2.1.12)
unnecessary comma: "easier than, an exhaustive"

Proposed Change:
"easier than an exhaustive"

Resolution: Accept

==========
Comment # 96: (Page 128, line 16, subclause F)
Final draft should not contain revision history

Proposed Change:
Remove 'Editor's Note--Editorial changes between D26 and D27 include the following:' and all subsequent lines

Resolution: Accept
Change as proposed, and remove Editor's Note 3 on page i.

==========

Comment # 97: (Page 48, line 1, subclause 9)
The word 'must' appears in several figures, in phrases such as "Client must verify KCF before revealing K". In most of the instances, the correct word is probably 'shall'.

Proposed Change:
Review usage of word 'must' in all figures and replace with 'shall' if this reflects a requirement.

Resolution: Accept
In Figures 1 (p. 48), 4 (p. 57), 6 (p. 64), 8 (p. 69), 9 (p. 70), and 10 (p. 74), change "must verify" to "verifies". In Figure 12 (p. 82), change "Client must generally verify" to "Client application generally needs to verify".

==========

Comment # 98: (Page 4, line 23, subclause 3)
The draft incorrectly numbers the first 5 definitions.

Proposed Change:
Make sure definitions are numbered correctly before publishing

Resolution: Accept

==========

Comment # 99: (Page 5, line 1, subclause 3)
Definition for 'Dictionary Attack': Definition 1 is not generally correct as stated. That is, a general dictionary attack is not constrained only by the attacker's resources--it may also be constrained by limits imposed by the server. Definition 1 is only true for an 'off-line' dictionary attack. On-line dictionary attacks are additionally constrained by time delays introduced by the server or limits to the number of password guesses.

Proposed Change:
Change definition to read 'off-line dictionary attack', or add a qualifier in the definitions stating that this definition only applies to off-line dictionary attacks.

Resolution: Accept
Delete the text “, constrained only by the attacker’s resources”.

==========

Comment # 100: (Page 5, line 5, subclause 3)
The use of 'hash function' is somewhat ambiguous. Does this mean a cryptographic hash function or non-cryptographic hash function?

Proposed Change:
Qualify usage of 'hash function' with 'cryptographic'

Resolution: Accept
Change as proposed, in subclauses 3.7 hashed password, 3.9 iterated hash, and 3.10 low-grade secret.

==========

Comment # 101: (Page 6, line 41, subclause 4.2)
Broken link in footnote

Proposed Change:
Replace "Error! Reference source not found" with the appropriate link

Resolution: Accept

==========
Comment # 102: (Page 3, line 24, subclause 1.4.2)
"where a step include" => "where a step includes"

Proposed Change:
"where a step include" => "where a step includes"

Resolution: Accept

"==========
Comment # 103: (Page 48, line 1, subclause 9)
In section 9 there are a number of figures illustrating the (key agreement) schemes. The form in which these schemes are presented seems to present an algorithm in which the processing has had a line drawn between client side processing and server side processing. However the scheme does not reflect that fact that when one send a request from the client to the server, the response from the server returns to the requestor logic, and not to a part of the logic somewhat removed.
For example on page 48, the PEPKGP-PAK in the client sends a password entangled public key to the server, after which a response (a public key ws) is sent from the PKGP-DH to the check of ws being in the parent group.

Proposed Change:
I would like to propose that all of the figures in which the client communiactes with the server, the figures should reflect the aspects of this communication. For example, have the server return a response to the caller that then proceeds with the processing.

Resolution: Accept
Comment appears to be based on a false assumption of a required ordering for all Client/Server communications. For example, in BPKAS-PAK, wS and wC may be sent in any order, per D27 subclause 1.4.2.

==========
Comment # 104: (Page ii, line 5, subclause Abstract)
Legal review conducted on this documents, requires that the word safely be removed from the third sentence of the abstract.

Proposed Change:
"& designed to utilize passwords and other low-grade secrets as a basis for securing electronic transactions&."

Resolution: Accept

==========
Comment # 105: (Page 1, line 8, subclause 1.1)
Legal review conducted on this documents, requires that the word safely be removed from the third sentence of the scope.

Proposed Change:
& designed to utilize passwords and other low-grade secrets as a basis for securing electronic transactions&.

Resolution: Accept

==========
Comment # 106: (Page 1, line 19, subclause 1.2)

Legal review conducted on this document requires that the first sentence of the second paragraph of the purpose be revised.

Proposed Change:
"P1363.2 specifies public-key cryptographic techniques specifically designed to securely perform password-based..."

Resolution: Accept

==========
Comment # 107: (Page 11, line 50, subclause 4.5)
Legal review conducted on this documents, requires that the last sentence on page 11 in 4.5 Schemes be revised for clarity.

Proposed Change:
"Issue of proper key management that may be essential for security and yet are outside the scope of this standard are addressed for informational purposes in Annex D."

Resolution: Accept

==========
Comment # 108: (Page 56, line 16, subclause 9.4.3.2)
Legal review conducted on this document, requires that Note 3 be revised.

Proposed Change:
"&Such proofs can reliably use common techniques&."

Resolution: Accept

==========
Comment # 109: (Page 107, line 47, subclause D.2.1.5)
Legal review conducted on this document requires that the second sentence in Note 1 be revised.

Proposed Change:
One can safely chose b=r

Resolution: Accept
Change per # 41.

==========
Comment # 110: (Page 108, line 32, subclause D.2.1.6)
Legal review conducted on this document requires that the sentence be revised.

Proposed Change:
"&with a value for the low bit that may be revealed without compromising security&"

Resolution: Accept

==========
Comment # 111: (Page 108, line 35, subclause D.2.1.6)
Legal review conducted on this document requires that the sentence be revised.

Proposed Change:
"One may omit the step of verifying Wc as a valid public key without compromising security. For other choices of domain parameters, further analysis may be required by the implementer in order to omit or replace this step without compromising security."

Resolution: Accept

==========
Comment # 112: (Page 109, line 26, subclause D.2.1.9)
Legal review conducted on this document requires that the sentence be revised.

Proposed Change:
"This difference raises a special concern for the secure use of unilateral schemes&"

Resolution: Accept

==========
Comment # 113: (Page 109, line 29, subclause D.2.1.9.1)
Legal review conducted on this document requires that the title of the subclause be changed.

Proposed Change:
Secure use of unilateral commitment schemes

Resolution: Accept

==========
Comment # 114: (Page 120, line 10, subclause D.2.2.3.2)
Legal review conducted on this document requires that the language of Note be revised.

Proposed Change:
"&membership in the parent group can be omitted without compromising a secure (functionally equivalent) scheme depends,&"

Resolution: Accept

==========
Comment # 115: (Page iv(2), subclause Contents)
Figures should be listed in Table of Contents.

Proposed Change:
Add an Editor's Note to that effect.

Resolution: Accept

==========
Comment # 116: (Page i, line 25, subclause Title page)
Editor's Notes should be resolved and removed if possible. Any remaining Editor's Notes should be resolved by the IEEE editorial staff.

Proposed Change:
On page i, remove Editor's Notes 1-3. As needed, add an Editor's Note to page i that documents any unresolved editorial issues to be communicated to the IEEE editors.

Resolution: Accept

==========
Comment # 117: (Page v, subclause Participants)
In Participants, update the lists.

Proposed Change:

Update the lists.

Resolution: Accept

==========

Comment # 118: (Page 127, subclause F)
In Bibliography, correct [B14] for FIPS Draft 186-3.

Proposed Change:
Insert "Draft" before "Federal", and change "Publication 186-2" to "Publication 186-3".

Resolution: Accept

==========