

M1/06-0669

InterNational Committee for Information Technology Standards
INCITS Secretariat, Information Technology Industry Council (ITI)
1250 Eye St. NW, Room 200, Washington, DC 20005
Telephone 202-737-8888; Fax 202-638-4922
email: incits@itic.org

Date: 29 August 2006
Submitted by: Matt Young (Purdue Univ.)
Email: mryoung@purdue.edu

Title: Purdue Comments on WD3 of AHGBEA report

Purdue University Comments on AHGBEA WD3

Overall:

The report has made significant progress just in the past few revisions. The structure of the approach is very well laid out and logical in order. The next step going forward for approval at the October M1 meeting should be to condense down sections that are repetitive or otherwise too lengthy losing the readers focus on the purpose of the report. Ultimately the reader should come away with a clear understanding as to how biometrics could be effectively used in e-authentication and more importantly how the potential scenarios and architectures relate back to OMB M04-04 and NIST SP800-63. This information is first introduced in Section 6 and then later discussed in further detail in Section 8 which is deep in the document. Caution needs to be exercised in what topics and length of discussion are included leading up to the sections these sections as they are most crucial based on the Terms of Reference for the Ad Hoc Group.

Section 5:

5.2: Move discussion on biometric subsystems to directly follow the diagrams before discussion of biometric functions.

5.5a: Condense dynamic biometric subsection a length that is consistent with the overall length of Section 5.

5.5b: Correlate and reduce redundant material with similar text in Sections 7, Sections 8 and Annex E.2. This is certainly interesting material and helpful, but a bit overwhelming as currently laid out.

Section 7:

7.2.1: Condense down text

7.4: Tie entropy and SOF requirements of BEM introduction to the mappings made by this group in section 8.2.5

7.6: Condense down text and tie back to section 5.4 (Comparison of Biometrics and Crypto). The placement of this text and table has been discussed a couple times already, but there may be a smoother correlation than the current one.

Section 8:

This section is very important based upon the fact that implementers will want to analyze the potential threats associated with different architectures.

8.1: Include similar diagrams from the biometric subsystems section in section 5 to emphasize what aspects of the overall system are being discussed in the four major categories of attacks.

8.1.2: Condense down text and/or include sub headings to more accurately emphasize the purpose of the different paragraphs.

8.1.3: Condense down text and/or include sub headings to more accurately emphasize the purpose of the different paragraphs.

8.1.4: Condense down text and/or include sub headings to more accurately emphasize the purpose of the different paragraphs.

8.2.2: Clarify and more clearly explain countermeasures column.

8.2.3: Need to include same level of detail and breakdown that is shown for enrollment for the other 3 types of attacks.

8.3.X: Need to organize the information breakdown into a template for each of the 6 architectures identified.

Page 95: First line of text, list security mechanisms that must be in place.

Section 9:

Expand on Recommendations to SP800-63, thoughts?

Section 10:

Expand on Future work possibilities, thoughts?

Annex A.1:

Are there any more reference that are needed or have been left out thus far?

Annex 4.2:

Put the document #s and titles into a table and update with latest contributions