

M1/06-0349

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: 1 April 2006

Submitted by: Matt Young (Purdue Univ.)

Email: [mryoung@purdue.edu](mailto:mryoung@purdue.edu)

---

## AHGBEA Issues List and Action Items

### Section 1 - Introduction

Item #	Subsection	Raised by	Issue or Item	Action:
1.1	General	Unidentified	What is the overview of? Is it the document or the problem?	Comments needed
1.2	General	Unidentified	What are the assumptions for reading the document?	Comments needed

### Section 2 – Statement of the Problem

Item #	Subsection	Raised by	Issue or Item	Action:
2.1	General	Mrs. Tilton	What it is that we are trying to do?	Comments needed

### Section 3 – Study Methodology

### Section 4 - References

## Section 5 – Biometric Authentication Concepts and Architectures

Item #	Subsection	Raised by	Item or Issue	Action:
5.1	General	Unidentified	Insert Diagram on Biometric Enrollment/Verification	Contributions needed
5.2	General	Unidentified	What is the right term of verification?	Comments needed
5.3	General	Unidentified	What is the right term of identification?	Comments needed
5.4	General	Unidentified	Should the need for a claimed identity by means of a PIN be allowed?	Comments needed
5.5	General	Unidentified	Review the Liaison Statement out of Kyoto resolution 4.2 as it relates to the rate of acceptable 1 in N for biometrics.	Contributions needed
5.6	General	Unidentified	Is 1:N ever applicable in remote environment, and if so then where?	Contributions needed
5.7	General	Unidentified	What is the role of privacy? Biometrics inherently also provide information that lead to identity.	Contributions needed
5.8	5.1	Unidentified	Insert diagram on biometric profile including the terminology	Contributions needed
5.9	5.2.1	Unidentified	What is the definition of compromise?	Comments needed
5.10	5.2.1	Unidentified	Which levels do compromise actually affect and where does it need to be addressed based upon motivation of the attacker?	Contributions needed
5.11	5.2.1	Unidentified	Contradict ourselves in the document based upon the discussion and insertion of the physical and behavioral section of the report.	Comments needed
5.12	5.2.1	Unidentified	When talking about compromise you must address credential compromise and system compromise.	Contributions needed
5.13	5.2.1	Unidentified	How does compromise relate to the different levels of security?	Contributions needed
5.14	5.2.1	Mr. Burr	It makes more sense to talk about the characteristics of biometrics and less time talking about password systems.	Comments needed
5.15	5.2.1	Mr. Burr	How can biometrics be effectively combined with other authentication mechanisms?	Contributions needed
5.16	5.2.5	Mr. Burr	Need a sentence to address why password mechanisms are directly called out and compared to biometric secrecy.	Contributions needed
5.17	5.3	Dr. Cambier	Section doesn't adequately discuss image and static biometric	Contributions needed
5.18	5.3	Mr. Podio	Introduce role of multi-biometrics	Contributions needed
5.19	5.3	Mrs. Valencia	Insert diagrams about the architectures	Contributions needed

5.20	5.5	Unidentified	Insert schematic of remote e-authentication of biometric system as it relates to the biometric process.	Contributions needed
5.21	5.5	Mr. Burr	Compromise of biometric database and local database needs consistency which the discussion of compromise above.	Comments needed
5.22	5.5	Dr. Cambier	It is not addressed that central database systems prevent duplicate enrollment.	Contributions needed

## Section 6 – Critiques

Item #	Subsection	Raised by	Item or Issue	Action:
6.1	General	Unidentified	This section needs to use the Issue or Challenge template.	Comments needed
6.2	General	Unidentified	What is the correct order of the Critiques?	Comments needed
6.3	6.1	Unidentified	What is the need to address integrity v. secrecy?	Comments needed
6.4	6.1	Mr. Hapeman	What is the true challenge with compromise and revocation? Is it the fact that biometrics can be compromised...or is it finding a way to revoke them?	Contributions needed
6.5	6.1	Mr. Modi	Where does revocation initiated by the user come in?	Contributions needed
6.6	6.1	Mr. Burr	What is the need to report a lost smart card if the biometric is public information?	Contributions needed
6.7	6.2	Unidentified	Add lead into sensor spoof section as what is covered there.	Contributions needed
6.8	6.2	Unidentified	Move the detail of the level of attacks and details about it should be noted, but maybe not in the document itself maybe as an annex.	
6.9	6.2	Unidentified	The offsetting fact of a second factor needs to be discussed at the end of section 6.2	Comments needed
6.10	6.3	Mr. Triglia	The SOF takes into consideration more than just the FAR	Contributions needed
6.11	General	Mrs. Tilton	Need a coherent discussion of the issue and display the findings, this section is not going to be resolved by the time the report is completed	Contributions needed
6.12	6.3	Unidentified	What are the required entropy of the different levels?	Contributions needed
6.13	6.3	Mr. Burr	Need to have expensive 3 <sup>rd</sup> party tests to determine what the actual FAR tests are	Comments needed

## Section 7 – Threats, Vulnerabilities and Models

Item #	Subsection	Raised by	Issue or Item	Action:
7.1	General	Mrs. Tilton	Need coherent explanation of threats and countermeasures	Contributions needed

## Section 8 – Recommendations

Item #	Subsection	Raised by	Issue or Item	Action:
8.1	General	Mrs. Tilton	What recommendations will be made? To whom?	Contributions needed

## Section 9 – Future Work