

Proposed Disposition of Comments on AHGBEA Study Report Working Draft 2

Date: 2006-05-29 Document: **M1/06-0512**

1	2	(3)	4	5	(6)	(7)
MB¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment²	Comment (justification for change) by the MB	Proposed change by the MB	Proposed Editor's Disposition
TSI-1	7.5		Te major	Change section 7.5.1	<p>7.5.1 Mobile Device Applications Mobile devices are an important element of the e-Authentication environment. Since many of these devices include a stylus and/or other inbuilt biometric sensors, the application of biometric technology to the e-Authentication problem is very relevant. As a result of special properties (see Section 5.6) of secret-based dynamic biometric technology, these technologies are particularly appropriate in a mobile device context.</p> <p>The processes involved in use of this technology in a mobile environment are: Registration, Device Enrollment and Verification, File encryption and Client- Server Communication.</p> <p>Enrollment & Registration</p> <ul style="list-style-type: none"> • Register Device on Authentication Server Using Automatically Generated Device ID • Choose/Allocate Complex Power-Up Password • User Enrolls Secret-Based Biometric Template on Device. • User Sets Power-Up Password (defined by Enterprise if policy dictates) • User Chooses/Sets PIN • Obfuscated Password Stored Securely on Device • Template Encrypted • User/Server enables Power-Up Biometric Protection with PIN. <p>Log-on (Verification)</p> <ul style="list-style-type: none"> • User Submits Biometric Sample to Device • Enters PIN • Template Decrypted • Sample Is Biometrically Matched • Success Releases Power-Up Password to Gain Access to Device • Template is Updated/Re-encrypted 	Accept

1 **MB** = Member of M1

2 **Type of comment:** **ge** = general **te** = technical **ed** **NOTE** Columns 1, 2, 4, 5 are compulsory.

Proposed Disposition of Comments on AHGBEA Study Report Working Draft 2

Date: 2006-05-29	Document: M1/06-0512
------------------	-----------------------------

1	2	(3)	4	5	(6)	(7)
MB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the MB	Proposed change by the MB	Proposed Editor's Disposition
					File Encryption & Device/Server Authentication & Communication <ul style="list-style-type: none"> • Appropriate Device Files Encrypted • Device/User Authenticated to Server. • Enable Encrypted Communication with Server. 	
TSI-2	7.5		Te major	This contribution is essentially an addition to section 5.6, which, among other things outlines a methodology for template encryption and access protection for stand-alone computing devices operating in either a stand-alone or a client-server environment. The detail contained below can be incorporated as a replacement for the current section 7.5 and referenced initially in paragraph 5.6.	Addition of section and subsections in 7.5.2	Noted-Discuss at meeting the proper location of the content. There are some overlaps with existing content in section 5.6 and section 6. This content also provides a detailed example implementation which may be better suited in an annex
TSI-3	5.61		Ed		The reference for the Signature/Sign modality is ANSI/INCITS 395 – 2005	Accepted
TSI-4	5.6.7	Page 35 – last line	Ed		Replace affected by effected	Accepted
TSI-5	6.4		Ge	Don't understand the numerical example for entropy/strength of function.		Noted-TSI is asked to provide description about what is unclear and how the document could better explain the material.
TSI-6	6.5.3	Page 53	Te major	This refers to a 1999 paper by Soutar et al. Reference to this paper by Soutar, et al is contained in the SC 27 Biometric Template Protection initiative which we have decided not to incorporate. The Ad Hoc group should be consistent in its approach to this methodology. Is it in use? Are there any analyses as to the effect on the FAR/FRR performance?	It seems to TSI, that if we incorporate the 1999 paper by Soutar et al we might want to consider endorsing the developing SC 27 initiative on Biometric Template Protection.	Noted-Discuss at meeting
TSI-7	General		Ed	Where the word biometric is used in the document as a noun, it should be replaced by a more specific noun using biometric as an adjective, e.g. biometric sample, biometric		Accept. More specific terminology will be used where appropriate.

1 MB = Member of M1

2 Type of comment: ge = general te = technical ed NOTE Columns 1, 2, 4, 5 are compulsory.

Proposed Disposition of Comments on AHGBEA Study Report Working Draft 2

Date: 2006-05-29	Document: M1/06-0512
------------------	-----------------------------

1	2	(3)	4	5	(6)	(7)
MB¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment²	Comment (justification for change) by the MB	Proposed change by the MB	Proposed Editor's Disposition
				template, biometric technology.		
TSI-8	General	Page 49	Ed	There are numerous places (e.g. Page 49 – last line) in the document which state that biometrics are not secrets or are not assumed to be secret. These statements are attributable to this document, as opposed to the NIST document. For such statements it should be made clear which modalities this does not apply to (in particular, secret-based dynamic biometric technologies) and whether the statement applies to the biometric template, which can be maintained as a secret if it is encrypted, or the biometric sample or both.		Noted-Discuss at meeting. TSI is asked to provide content to instances which this comment applies. Note that 800-63 states in clause 3 "Biometrics do not constitute secrets suitable for use in the conventional remote authentication protocols addressed in this document."
TSI-9	6.2.1, 6.2.2, 6.2.3		Ed	In Paragraphs 6.2.1, 6.2.2 and 6.2.3 there should be a statement to the effect that the majority of the comments refer only to image-based biometric technologies and that dynamic biometric technologies typically provide simple means of revocation.		Noted-Discuss at meeting. TSI is asked to provide content to instances which this comment applies

1 **MB** = Member of M1

2 **Type of comment:** **ge** = general **te** = technical **ed** **NOTE** Columns 1, 2, 4, 5 are compulsory.