

**M1/05-0782 - Comments on INCITS1706-D – Application for Commercial Physical Access Control.**

Date:	Document: <b>M1/05-0701</b>
-------	-----------------------------

1	2	(3)	4	5	(6)	(7)
Mem <sup>1</sup>	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment <sup>2</sup>	Comment (justification for change) by the Member	Proposed change by the Member	Proposed Editors Disposition
Biocom	Entire Doc	Headers	Ed	Headers are inconsistent	Change all headers to Project INCITS 1706-D	
Biocom	6.1	List	Te-maj	Do not understand what value this section adds. All it seems to do is to list possible security threats (although this is not clear) but not how to address or identify them.	Either delete 6.1 as a whole or clarify with additional explanatory text why these potential security threats have been identified in the context of this standard.	
Biocom	6.2.1	2 <sup>nd</sup> sentence	Te-Maj	It states “Such structures shall conform to a publicly available CBEFF-compliant patron format. The CBEFF-compliant patron header shall specify a conforming standard biometric header(SBH) and a CBEFF-compliant BDB. The use of a signature block is optional. The use of encryption or other security techniques is optional”  What if the chosen “publicly available CBEFF-compliant patron format” requires the use of the signature block and encryption?	Clarify using additional text or Change to “Such structures shall conform to any publicly available CBEFF patron format that specifies that the use of a signature block is optional and that the use of encryption or other security techniques is optional.	
Biocom	6.2.2	Entire clause	Te-Min	“Reader” and “terminal” are not defined.	Define “Reader” and “terminal”	
Biocom	6.2.2 and Annex B		Te-Maj	One of the biggest disadvantages of using the “bump in the wire” technology where the biometric reader is inserted between the access control card reader and the access control panel (or controller) is that if the verification fails or an identification is not made, the access control system never even knows that an attempt was made to enter through a specific door. This is not advisable since it is crucial that the access control application contains logs and records of all attempted transactions.	Consider adding an additional Wiegand 26 bit formatting to allow a biometric system to send the same Wiegand string to the access control system but in a different format (e.g inverse parity) so that the access control application can log that an access attempt has been made.	

<sup>1</sup> **Mem** = Member organization

<sup>2</sup> **Type of comment:** **ge** = general    **te** = technical    **ed** = editorial – For technical comments, please indicate whether your comment is a MAJOR or MINOR technical comment.

**NOTE** Columns 1, 2, 4, 5 and 6 are compulsory.