Comment Template for: NIST SP 800-63-4 Suite (Initial Public Draft)

Please submit responses to dig-comments@nist.gov by March 24 April 14, 2023

Organization:	*Trusted Computing Group*
Name of Submitter/POC:	*Security Evaluatoin workgroup (Olivier Collart as Chairman)*
Email Address of Submitter/POC:	[REMOVED]

Comment #	**Publication (Base, 63A, 63B, 63C)**	**Section**	**Page #**	**Line #**	**Comment (Include rationale for comment)**	**Suggested Change**
3	63B	5.2.11	38	1490	The authenticator SHALL contain a blocklist (either specified by specific values or by an algorithm) of at least 10 commonly used activation values and SHALL prevent their use as activation secrets	Replace "SHALL" by "SHOULD" for resource constrained hardware-based authenticators when secure element is involved in authentication. Rationale 1: different formats will lead to have 10 commonly used activation values per format. this will not be possible for alphanumeric format. Rationale 2: activation secrets may be generated by systems randomly without blocklist restrictions which would create interoperability issues
4	63B	5.2.11	38	1494	The authenticator or verifier SHALL implement a retry-limiting mechanism that effectively limits the number of consecutive failed activation attempts using the authenticator to ten (10).	Could you clarify that the rate limiting mechanism in line 1498 is the retry-limiting mechanism described in the 1494 requirement?
		5.2.11	39	1498	In all other cases, rate limiting SHALL be implemented in the authenticator.	
6	63B	5.2.11	39	1499	Once the limit of 10 attempts is reached, the authenticator SHALL be disabled and a different authenticator SHALL be required for authentication	Proposed change to allow additional attempts with throttling mechanism without a different authenticator to avoid a permanent lock out. A waiting time mechanism (similar as described in 5.2.2, second bullet) could be configured in order to allow a maximum number of attempts in a given time period. For instance 100 attempts per year after the 10 attempts. Proposal: "Once the limit of "A" attempts is reached, either the authenticator SHALL be disabled and a different role SHALL be required for authentication or a waiting time mechanism is activated in order to limit the number of attemps to X per Y unit of time". The values X and Y would be application specific or defined by the SP800-63.