Comment Template for: NIST SP 800-157r1 (Initial Public Draft)

Please submit responses to piv_comments@nist.gov by March 24, 2023

Organization:	*Intercede*
Name of Submitter/POC:	
Email Address of Submitter/POC:	

Comment #	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	3.1.4 Activation Dat	12	623-627	3.1.4 Activation Data Lines 623-627 "If the activation secret has been forgotten or the permitted number of consecutive wrong attempts has been reached, the home agency SHALL be required to input the PIN unblocking key (PUK). If the PUK is not implemented by the authenticator or cannot be provided, either the authenticator certificates SHALL be revoked or the associated private keys SHALL be destroyed or zeroized." Problems: The first sentence here in many cases is a requirement that can be impossible to meet (either due to PUK not being implemented, PUK entry not being possible, or there being cases where it is unknown if the cardholder has forgotten the activation secret). But because it is a SHALL, it is necessary to meet this (potentially impossible) requirement to be compliant with the spec. The points about how to handle a blocked or forgotten activation secret are problematic because there are some unknowns: the authenticator cannot know if the secret has been forgotten (it can only validate a given attempt), the authenticator cannot know if a PUK can/cannot be provided (it can only know if it has been given a correct PUK). At the point of attempted authentication where the activation secret is unknown there is no authentication – so in practice triggering certificate revocation on the server may not be possible when the activation secret is blocked or forgotten.	Resolution: I propose replacing 623-628 with the following: “The authenticator MAY support a PIN unblocking key (PUK) that can be used to unblock/reset the activation secret for the cases where the activation secret has been forgotten or the permitted number of consecutive wrong attempts has been reached. If the PUK is not implemented by the authenticator, when the activation secret becomes blocked due to number of consecutive wrong attempts, either the authenticator certificates SHALL be revoked or the associated private keys SHALL be destroyed or zeroized.”