1a.User→PM	: SSL web site connection request
2a.PM	: Check whether user is authenticated
3a.PM↔User	: set up SSL connection with the User
4a.PM↔Server	: validate Target Certificate and set up SSL connection with the Target Server
5a.PM	: is login page?
6a.PM↔DB	: does user have enrolled credentials?
7a.PM	: If yes, create dummy credentials (DumCred)
8a.PM→User	: insert DumCred and send login page
9a.User→PM	: submit login page
10a.PM↔DB	: Retrieve user's encCredwithPAL, nonce and sealedPALpriv
11a.PM	: Execute Credential Decryption Protocol
11b.PM	: Insert original credentials
12a.PM→Server	: submit credentials
13a.Server→PM	: User is authenticated
14a.PM→User	: User is authenticated