

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 update page?
6a.PM↔DB	: does user have enrolled credentials?
7a.PM	: If yes, create dummy credentials (DumCred)
8a.PM→User	: insert DumCred in old credentials field and send update page
9a.User	: enter new credentials (NewCred)
10a.Browser	: encNewCredwithPal=Enc(NewCred)PALpub
11a.Browser→PM	: encNewCredwithPal
12a.PM	: Execute Credential Decryption Protocol and get NewCred
13a.PM↔DB	: Retrieve user's encCredwithPAL, nonce and sealedPALpriv
14a.PM	: Execute Credential Decryption Protocol and get Old Credentials (OldCred)
14b.PM	: Insert OldCred and NewCred
15a.PM→Server	: Submit Update Page
16a.Server→PM	: User credentials are updated
17a.PM→DB	: Update user's record with the new encNewCredwithPal, sealedPALpriv and nonce
18a.PM→User	: User credentials are updated