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→User	: If not, send login page with empty fields
8a.User	: enter credentials
9a.Browser	: encCredwithPal= Enc(credentials)PALpub
10a.Browser→PM	: encCredwithPal
11a.PM↔PAL	: Execute Credential Decryption Protocol
12a.PM	: Insert original credentials
13a.PM→Server	: Submit credentials
14a.Server→PM	: User is authenticated
15a.PM→DB	: store encCredwithPal, sealedPALpriv and nonce
16a.PM→User	: User is authenticated