OTPme - Feature #68

Add optional support for signing authentication replies

24 December 2015 12:19 - The 2nd

Status:	In Bearbeitung	**Start date:**	24 December 2015
Priority:	Normal	**Due date:**	
Assignee:	The 2nd	**% Done:**	50%
Category:		**Estimated time:**	0:00 hour
Target version:	OTPme 0.3		

Description

- The client should send a challenge to the OTPme server that will be signed with its public key
  - This reduces the code where authentication related bugs may lead to false positives
- Using JWT for this feature will allow us to re-use it for web authentication in later versions (https://en.wikipedia.org/wiki/JSON_Web_Token)

History

#1 - 30 December 2015 02:41 - The 2nd

- % Done changed from 40 to 50

- Current implementation sends a challenge with the authentication request which is added to a JWT signed with the public key of the "site certificate" and send back in the authentication reply. This is used e.g. when logging in via OTPme PAM module.

#2 - 07 August 2018 14:06 - The 2nd

- Status changed from Neu to In Bearbeitung