OTPme - Feature #64

Implement U2F token

29 November 2015 16:43 - The 2nd

Status:	In Bearbeitung	**Start date:**	17 December 2015
Priority:	Normal	**Due date:**	
Assignee:	The 2nd	**% Done:**	90%
Category:		**Estimated time:**	0:00 hour
Target version:	OTPme 0.3		

Description

- Add generic U2F token
- Implement deployment with OTPme client tools

U2F Specs: https://fidoalliance.org/specifications/download/
Example server: https://github.com/Yubico/python-u2flib-server
Example client: https://github.com/Yubico/python-u2flib-host

Subtasks:

Feature # 66: Allow usage of U2F token as second factor token with "password" tokens	**In Bearbeitung**

History

#1 - 29 November 2015 18:16 - The 2nd

Some notes on U2F:

It looks like the "master key" of a U2F token is generated while manufacturing the key and cannot be regenerated by the user. Like described in the links below the reason for this are the attestation certificates. They are used to ensure that the key is not backed-up/cloned and thus the authentication service can use them to apply rules like "only allow U2F tokens from manufacturer X". This is a nice feature for everyone who wants to allow users to roll out their own tokens but want to prevent users from using insecure (e.g. software) tokens. But it also means that you have to trust the manufacturer. Currently there seems to be no way around this. But as yubico stated in the forum post below they could at least sell "un-programmed" tokens that users could load their own keys and attestation certificates to. Another and IMHO better solution would be to allow the U2F feature of the yubikey to use a second slot just like its done for the OTP/static password feature. This would allow us to use the yubikey with a trusted self created secret for your own systems without killing the manufacturer key/certs which may be needed if you want to use the yubikey with a third party that requires valid attestation certificates.

https://developers.yubico.com/U2F/Protocol_details/Key_generation.html
http://forum.yubico.com/viewtopic.php?f=33&t=1666

#2 - 03 December 2015 00:11 - The 2nd

- % Done changed from 0 to 30

#3 - 07 December 2015 00:36 - The 2nd

- % Done changed from 30 to 70

Implemented first working version that can be used to do OTPme realm authentication.

- Checking U2F counter needs to be implemented
- Current version misses offline login possibilities

#4 - 08 December 2015 23:08 - The 2nd

- Status changed from Neu to In Bearbeitung

- % Done changed from 70 to 80

- Implemented counter check using the token counter mechanism for synchronization between nodes/hosts