OTPme - Feature #30

add option to configure hash type for CTP and SLP generation

24 January 2015 15:56 - The 2nd

Status:	Erledigt	**Start date:**	02 February 2015
Priority:	Normal	**Due date:**	
Assignee:	The 2nd	**% Done:**	0%
Category:		**Estimated time:**	0:00 hour
Target version:	OTPme 0.2		

Description

this should improve protection against dictionary attacks if someone was able to keylogg/sniff both, the OTP and the CTP

- we should split e.g. a 128 char hash into four 32 char strings and choose a random one for CTP/SLP creation
  - this should be configurable per client because some clients may not support any hash type (e.g. sha512)

Subtasks:

Feature # 37: implement support for different hash types for CTP generation in roundcub...	**Neu**

History

#1 - 02 February 2015 17:58 - The 2nd

implemented for CTPs now. SLP is less important but may follow later...

#2 - 02 February 2015 17:58 - The 2nd

- Status changed from Neu to Gelöst

#3 - 02 February 2015 17:59 - The 2nd

- Status changed from Gelöst to Erledigt