

## OTPme - Feature #30

### add option to configure hash type for CTP and SLP generation

24 January 2015 15:56 - The 2nd

<b>Status:</b>	Erledigt	<b>Start date:</b>	02 February 2015
<b>Priority:</b>	Normal	<b>Due date:</b>	
<b>Assignee:</b>	The 2nd	<b>% Done:</b>	0%
<b>Category:</b>		<b>Estimated time:</b>	0:00 hour
<b>Target version:</b>	OTPme 0.2		
<b>Description</b>			
this should improve protection against dictionary attacks if someone was able to keylogg/sniff both, the OTP and the CTP			
<ul style="list-style-type: none"><li>• we should split e.g. a 128 char hash into four 32 char strings and choose a random one for CTP/SLP creation<ul style="list-style-type: none"><li>◦ this should be configurable per client because some clients may not support any hash type (e.g. sha512)</li></ul></li></ul>			
<b>Subtasks:</b>			
Feature # 37: implement support for different hash types for CTP generation in roundcub...			<b>Neu</b>

### 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