

Core - Feature # 28230

Status:	Accepted	Priority:	Should have
Author:	Stefan Neufeind	Category:	
Created:	2011-07-15	Assigned To:	Stefan Neufeind
Updated:	2014-12-18	Due date:	
PHP Version:			
Complexity:			
Sprint Focus:			
Subject:	Add support for PBKDF2 to hashing		
Description			
<p>An implementation is already pending for FLOW3 (see #26786, https://review.typo3.org/#change,2332) which is planned to replace MD5 (current default). It would be great to have this available for passwords (FE/BE) and stdWrap.hash (see #28095).</p> <p>I'm not yet sure how it would fit within current sysex "saltedpasswords" though.</p>			
Related issues:			
related to TYPO3 Flow Base Distribution - Feature # 26786: Use a safe passwor...		Resolved	2011-05-12
related to Core - Feature # 28095: Add hashing algorithms to stdWrap		Closed	2011-07-11

History

#1 - 2014-12-18 13:11 - Mathias Schreiber

- Status changed from New to Needs Feedback
- Assigned To set to Stefan Neufeind

Is this still valid?

#2 - 2014-12-18 13:22 - Stefan Neufeind

- Status changed from Needs Feedback to Accepted

still not available in TYPO3 CMS (saltedpasswords, TypoScript). The hash-stdWrap relies on the php-hash-functions and even on a recent PHP a call to hash_algos() doesn't seem to support PBKDF2.

#3 - 2014-12-18 13:57 - Marcus Krause

I started with this feature in March 2013 - see <https://twitter.com/t3sec/status/313413250693881858>

Let's see if I can find this code somewhere here. :))

#4 - 2014-12-18 14:02 - Stefan Neufeind

We should have an implementation in Flow as well already (see description).