TYPO3.Flow - Bug # 40241

Status:	Rejected	**Priority:**	Must have
Author:	Andreas Wolf	**Category:**	Security
Created:	2012-08-26	**Assigned To:**	
Updated:	2012-11-01	**Due date:**	
PHP Version:			
Has patch:	No		
Complexity:			
Affected Flow version:	(any)		
Subject:	Encryption key sometimes readable for anybody		

Description

The encryption key is (on *NIX) generated with the current umask. On most systems, this is something like 0022, making the file readable for anybody. If the key is supposed to be kept secret (which I assume), this might pose a security risk.

This issue could be easily fixed by using chmod() or touch() in Security\Cryptography\HashService.

History

#1 - 2012-08-27 10:32 - Karsten Dambekalns

Off the top of my head I'd respond with "then most systems seem be set up in an insecure way". :/

#2 - 2012-08-27 21:57 - Andreas Wolf

Karsten Dambekalns wrote:

> *Off the top of my head I'd respond with "then most systems seem be set up in an insecure way". :/*

Kind of, yes. But there is data where it doesn't harm that everybody can read them, and others that should be kept secret. I'd say the encryption key is rather of the lattter kind...

#3 - 2012-11-01 19:05 - Robert Lemke

- Status changed from New to Rejected

We generally don't set umasks or owners / groups while creating files because server setups may vary a lot. If I'm not completely mistaken, this can always be solved by a proper server setup and as I experienced in the past, interfering with such as setup (by using chmod) might cause trouble.

I'll close this for now. If there is a bullet-proof solution with proof that it won't have side effects on typical server setups, you can re-open it.