TYPO3.Flow - Bug # 4870

Status:	Resolved	**Priority:**	Should have
Author:	David Bruehlmeier	**Category:**	Security
Created:	2009-10-02	**Assigned To:**	Karsten Dambekalns
Updated:	2010-10-20	**Due date:**	
PHP Version:			
Has patch:			
Complexity:			
Affected Flow version:			
Subject:	Tests with RSAWalletServicePHP fail on Windows		

Description

```
Error in encryptingAndDecryptingBasicallyWorks Detail
E:\Sources\FLOW3\Packages\Framework\FLOW3\Classes\Security\Cryptography\RSAWalletServicePHP.php:232
Warning: openssl_pkey_get_details() expects parameter 1 to be resource, boolean given in
E:\Sources\FLOW3\Packages\Framework\FLOW3\Classes\Security\Cryptography\RSAWalletServicePHP.php line 232
Error in checkRSAEncryptedPasswordReturnsTrueForACorrectPassword Detail
E:\Sources\FLOW3\Packages\Framework\FLOW3\Classes\Security\Cryptography\RSAWalletServicePHP.php:232
Warning: openssl_pkey_get_details() expects parameter 1 to be resource, boolean given in
E:\Sources\FLOW3\Packages\Framework\FLOW3\Classes\Security\Cryptography\RSAWalletServicePHP.php line 232
Error in checkRSAEncryptedPasswordReturnsFalseForAnIncorrectPassword Detail
E:\Sources\FLOW3\Packages\Framework\FLOW3\Classes\Security\Cryptography\RSAWalletServicePHP.php:232
Warning: openssl_pkey_get_details() expects parameter 1 to be resource, boolean given in
E:\Sources\FLOW3\Packages\Framework\FLOW3\Classes\Security\Cryptography\RSAWalletServicePHP.php line 232
Error in decryptingWithAKeypairUUIDMarkedForPasswordUsageThrowsAnException Detail
E:\Sources\FLOW3\Packages\Framework\FLOW3\Classes\Security\Cryptography\RSAWalletServicePHP.php:232
Warning: openssl_pkey_get_details() expects parameter 1 to be resource, boolean given in
E:\Sources\FLOW3\Packages\Framework\FLOW3\Classes\Security\Cryptography\RSAWalletServicePHP.php line 232
```

My Setup

- Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
- Windows NT SP3

Associated revisions

Revision 96f1aa81 - 2009-10-06 16:23 - Karsten Dambekalns

[~BUGFIX] FLOW3 (Security): Added an exception if SSL private key generation fails, relates to #4870.

History

#1 - 2009-10-06 16:07 - Karsten Dambekalns

- Category set to Security

- Status changed from New to Accepted

- Assigned To set to Karsten Dambekalns

It seems openssl_pkey_new() in generateNewKeyPair() returns FALSE instead of the expected resource. There are two things to do:

- (we) check the return value so we get a sensible error message
- (you, David) check your setup, see below

It seems on Windows you need to configure things correctly so OpenSSL works as expected, see http://de3.php.net/manual/en/openssl.installation.php

- did you make sure it is set up as needed?

#2 - 2009-10-07 20:00 - David Bruehlmeier

Hi

OpenSSL is installed and working according to phpinfo():

```
openssl
OpenSSL support     enabled
OpenSSL Library Version     OpenSSL 0.9.8k 25 Mar 2009
OpenSSL Header Version     OpenSSL 0.9.8k 25 Mar 2009
```

However, when I execute this:

```
$key = openssl_pkey_new();
while ($msg = openssl_error_string())
    echo $msg . "<br />\n";
```

I get

```
error:02001003:system library:fopen:No such process
error:2006D080:BIO routines:BIO_new_file:no such file
error:0E064002:configuration file routines:CONF_load:system lib
error:02001003:system library:fopen:No such process
error:2006D080:BIO routines:BIO_new_file:no such file
error:0E064002:configuration file routines:CONF_load:system lib
```

I guess its due to a misconfiguration in openssl.cnf, but what exactly might it be...? Has anybody else got the same problem?

#3 - 2009-10-08 11:40 - Karsten Dambekalns

David Bruehlmeier wrote:

> *OpenSSL is installed and working according to phpinfo():*

Installed yes, working - not necessarily.

> *I guess its due to a misconfiguration in openssl.cnf, but what exactly might it be...?*

Given the error message, I think the DLLs (ssleay.dll and libeay.dll) are missing - did you check? Or the configuration file is not found.

#4 - 2009-10-09 22:04 - David Bruehlmeier

You were right, it was installed, but not working... I solved it by installing "Win32 OpenSSL v0.9.8k Light" from http://www.slproweb.com/products/Win32OpenSSL.html (without changing the default installation directory which seems to be C:\OpenSSL). The tests now run "green" even on 1.0.0-alpha5.

#5 - 2009-10-09 22:32 - Karsten Dambekalns

- Status changed from Accepted to Resolved

- Target version set to 1.0 alpha 6

- % Done changed from 0 to 100

Ok, glad you got it working now.