Lasso - Bug #10019

Setting a signature algorithm to a SHA greater than 1 fails

18 février 2016 05:43 - Brett Gardner

Statut:	Fermé	**Début:**	18 février 2016
Priorité:	Normal	**Echéance:**	
Assigné à:		**% réalisé:**	100%
Catégorie:	SAMLv2	**Temps estimé:**	0:00 heure
Version cible:	2.5.1		
Patch proposed:	Oui	**Planning:**	

Description

If you set the signature method to a SHA256, SHA384 or SHA512 the signature created is invalid. Eg (php)

$sp_server = new LassoServer($xml,$key,NULL,$crt);
LassoServer_signatureMethod_set($sp_server->_cptr,LASSO_SIGNATURE_METHOD_RSA_SHA256);

Also note, that there is a bug in the lasso.php file that is shipped / generated whereby you have to set the signature method as above, if you attempt to do the following it fails as the "LassoServer::set_signaturemethod" is expecting a Lasso object instead of a constant. Note this may be incorrect usage by myself.

$sp_server->signatureMethod = LASSO_SIGNATURE_METHOD_RSA_SHA256;

Attached is a patch that corrects this behaviour. However I do not have a reproduce case

This may be related to bug #9479

Demandes liées:

Duplique Lasso - Bug #9479: Version 2.5.0 with ADFS and SHA256	**Fermé**	**04 janvier 2016**

Révisions associées

Révision 74e8705b - 18 février 2016 22:52 - Benjamin Dauvergne

tools.c: use correct NID and digest length when building RSA signature using SHA-2 digest (fixes #10019)

Thanks to Brett Gardner for the bug report and patch.

Licence: MIT

Historique

#1 - 18 février 2016 10:46 - Benjamin Dauvergne

Looks good, thank your. I'll see to integrate your patch today or tomorrow, could you send a mail to our mailing list stating that your contributin to lasso will be under the MIT license please ? It's our contributor agreement. Or you can send it directly to support@entrouvert.com. Thank you.

#2 - 18 février 2016 23:00 - Benjamin Dauvergne

- Statut changé de Nouveau à Résolu (à déployer)

- % réalisé changé de 0 à 100

Appliqué par commit 74e8705b57b6fd5972f28c646d84087c8011bb54.

#3 - 19 février 2016 10:41 - Benjamin Dauvergne

- Version cible mis à 2.5.1

#4 - 19 février 2016 10:41 - Benjamin Dauvergne

- Duplique Bug #9479: Version 2.5.0 with ADFS and SHA256 ajouté

#5 - 19 février 2016 10:42 - Benjamin Dauvergne

- Statut changé de Résolu (à déployer) à Solution déployée

#6 - 19 février 2016 11:11 - Benjamin Dauvergne

- Statut changé de Solution déployée à Fermé

Fichiers

lasso-2.5.0-fix-sha256.patch	3,12 ko	18 février 2016	Brett Gardner