Lasso - Development #10155

Ability to set the "DigestMethod" of a saml response

02 mars 2016 00:56 - Brett Gardner

Statut:	Fermé	**Début:**	02 mars 2016
Priorité:	Normal	**Echéance:**	
Assigné à:	Benjamin Dauvergne	**% réalisé:**	100%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:	2.6.0		
Patch proposed:	Non	**Planning:**	

Description

When building a signed SAML response, there is no way to set the "DigestMethod" of the signature to SHA256, It defaults to SHA1

Attached is a test case, note this is the same test case as issue 10154 hence the name "lasso-bug.tar.bz2"

<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
<SignedInfo>
<CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
<SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
<Reference URI="#_A7F3AF0951AD63AB216597DE5743EC91">
<Transforms>
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
<Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
</Transforms>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>...</DigestValue>
</Reference>
</SignedInfo>
<SignatureValue>...</SignatureValue>
<KeyInfo>
<X509Data>
<X509Certificate>...</X509Certificate>
</X509Data>
</KeyInfo>
</Signature>

Révisions associées

Révision 95252372 - 06 mars 2016 01:43 - Benjamin Dauvergne

Choose the Reference transform based on the chosen Signature transform (fixes #10155)

i.e. if the signature use SHA2 then use SHA2 of the same strength for digesting
references.

Historique

#1 - 02 mars 2016 01:30 - Benjamin Dauvergne

- Statut changé de Nouveau à Rejeté

LassoServer structure has a signature_method field for this.

#2 - 02 mars 2016 01:34 - Brett Gardner

I don't want to set the SignatureMethod to SHA256, I'm already doing this, I want to set the DigestMethod

#3 - 02 mars 2016 01:47 - Benjamin Dauvergne

- Statut changé de Rejeté à Nouveau

It's not handled currently, please provide a patch.

#4 - 06 mars 2016 01:45 - Benjamin Dauvergne

- Statut changé de Nouveau à Résolu (à déployer)

- % réalisé changé de 0 à 100

Appliqué par commit 9525237236eef4097300d9b6e93d2178a7a72267.

#5 - 06 mars 2016 11:51 - Benjamin Dauvergne

- Assigné à mis à Benjamin Dauvergne

#6 - 06 mars 2016 11:51 - Benjamin Dauvergne

- Version cible mis à 318

#7 - 28 juin 2018 10:37 - Benjamin Dauvergne

- Version cible changé de 318 à 2.6.0

#8 - 28 juin 2018 10:42 - Benjamin Dauvergne

- Statut changé de Résolu (à déployer) à Fermé

Fichiers

lasso-bug.tar.bz2	11,3 ko	01 mars 2016	Brett Gardner