Lasso - Bug #98

Support for encrypted private keys is incomplete

15 juin 2010 19:08 - Benjamin Dauvergne

Statut:	Fermé	**Début:**	15 juin 2010
Priorité:	Immediat	**Echéance:**	
Assigné à:	Benjamin Dauvergne	**% réalisé:**	100%
Catégorie:	SAMLv2	**Temps estimé:**	15:00 heures
Version cible:	2.3.0		
Patch proposed:		**Planning:**	

Description

For the moment we can load the definition of a private key and its password in a LassoServer object. All the plumbing which goes from the LassoServer object to signed LassoNode is missing for the password argument.

What's needed:
- a way to attach the password to signed node, without breaking ABI compatibility (so adding a public field is forbidden) ;
- to use this new parameter in calls to lasso_sign_node ;
- to serialize this new field with the old ones.

The objects to extend are LassoSamlp2StatusResponse, LassoSamlp2RequestAbstract and LassoSaml2Assertion.

ID-FFv1.2 is not a priority.

Historique

#1 - 19 juin 2010 11:50 - Benjamin Dauvergne

- % réalisé changé de 0 à 50

#2 - 05 juillet 2010 13:41 - Clément Oudot

I tested today, and I confirm this not working for now. Passwords are loaded, but we then have this kind of error:

```
Enter PEM pass phrase:
func=xmlSecOpenSSLAppKeyLoadBIO:file=app.c:line=243:obj=unknown:subj=PEM_read_bio_PrivateKey and PEM_read_bio_
PUBKEY:error=4:crypto library function failed:
func=xmlSecOpenSSLAppKeyLoadMemory:file=app.c:line=193:obj=unknown:subj=xmlSecOpenSSLAppKeyLoadBIO:error=1:xml
sec library function failed:
Enter PEM pass phrase:
func=xmlSecOpenSSLAppKeyLoadBIO:file=app.c:line=243:obj=unknown:subj=PEM_read_bio_PrivateKey and PEM_read_bio_
PUBKEY:error=4:crypto library function failed:
func=xmlSecOpenSSLAppKeyLoadMemory:file=app.c:line=193:obj=unknown:subj=xmlSecOpenSSLAppKeyLoadBIO:error=1:xml
sec library function failed:
Enter PEM pass phrase:
```

And:

```
[Mon Jul 05 13:34:57 2010] [debug] CGI.pm(91): Lemonldap::NG::Portal::SharedConf: Lasso error [ debug ]: 2010-
07-05 13:34:57 (tools.c/:985) Failed to load private key.
[Mon Jul 05 13:34:57 2010] [debug] CGI.pm(91): Lemonldap::NG::Portal::SharedConf: Lasso error [ warning ]: 201
0-07-05 13:34:57\tSigning of saml2:Assertion failed: Failed to load private key.
[Mon Jul 05 13:34:57 2010] [debug] CGI.pm(91): Lemonldap::NG::Portal::SharedConf: Lasso error [ debug ]: 2010-
07-05 13:34:57 (tools.c/:985) Failed to load private key.
[Mon Jul 05 13:34:57 2010] [debug] CGI.pm(91): Lemonldap::NG::Portal::SharedConf: Lasso error [ warning ]: 201
0-07-05 13:34:57\tSigning of samlp2:StatusResponse failed: Failed to load private key.
[Mon Jul 05 13:34:57 2010] [debug] CGI.pm(91): Lemonldap::NG::Portal::SharedConf: Lasso error [ debug ]: 2010-
07-05 13:34:57 (tools.c/:985) Failed to load private key.
[Mon Jul 05 13:34:57 2010] [debug] CGI.pm(91): Lemonldap::NG::Portal::SharedConf: Lasso error [ warning ]: 201
0-07-05 13:34:57\tSigning of samlp2:StatusResponse failed: Failed to load private key.
```

#3 - 19 juillet 2010 16:30 - Benjamin Dauvergne

- % réalisé changé de 50 à 100

#4 - 19 juillet 2010 16:32 - Benjamin Dauvergne

- Statut changé de Nouveau à Fermé