# eole-common - Tâche #13662

Scénario # 13500 (Terminé (Sprint)): Assistance aux utilisateurs (42-44)

## transition à l'utilisation des algorithmes de signatures sha256

10/19/2015 10:58 AM - Benjamin Bohard

| | | | |
|---|---|---|---|
| **Status:** | Fermé | **Start date:** | 10/19/2015 |
| **Priority:** | Normal | **Due date:** | |
| **Assigned To:** | Emmanuel GARETTE | **% Done:** | 100% |
| **Target version:** | Sprint 2015 42-44 - Équipe MENESR | **Estimated time:** | 2.00 hours |
| | | **Spent time:** | 2.33 hours |

**Description**

D'ici la fin de l'année, les certificats utilisant sha1 pour les signatures ne seront plus aussi largement acceptés par les clients.
Il faut prévoir la migration vers sha256.

À vérifier si toutes les bibliothèques utilisées pour les certificats sont compatibles pour les versions des modules utilisant des services web diffusés à l'extérieur.

A minima, il faut changer le modèle servant à générer le certificat "local" (signé par le certificat autosigné).

**Related issues:**

| | |
|---|---|
| Related to eole-common - Evolution #7066: Template ca-eole.conf cert-eole.con... | **Fermé** |

### Associated revisions

**Revision e552bed6 - 10/19/2015 04:26 PM - Emmanuel GARETTE**

remplacer le digest methods par défaut de sha1 à sha256 (ref #13662 @2h)

**Revision 233f4f8e - 10/26/2015 03:00 PM - Emmanuel GARETTE**

remplacer le digest methods par défaut de sha1 à sha256

Ref #13662 @20m [2.4]

Cherry-picked from commit:eole-common:e552bed6

### History

**#1 - 10/19/2015 11:44 AM - Joël Cuissinat**

*- Tracker changed from Demande to Tâche*

*- Estimated time set to 2.00 h*

*- Parent task set to #13500*

*- Remaining (hours) set to 2.0*

*- Distribution set to EOLE 2.5*

```
$ rgrep ' sha1' *
tmpl/certif-eole.conf:default_md        = sha1
tmpl/certif-eole.conf:default_md        = sha1
tmpl/ca-eole.conf:default_md        = sha1
tmpl/ca-eole.conf:default_md        = sha1
```

Tester et annuler la modification si nécessaire.

#### #2 - 10/19/2015 04:43 PM - Emmanuel GARETTE

*- Status changed from Nouveau to En cours*

*- Assigned To set to Emmanuel GARETTE*

*- % Done changed from 0 to 100*

Pour tester, dans firefox, éditer le certificat, Certificate Signature Algorithm doit être à "PKCS #1 **SHA-512** With RSA Encryption" (et ne doit plus être SHA-1).

#### #3 - 10/20/2015 09:47 AM - Scrum Master

*- Status changed from En cours to Résolu*

#### #4 - 10/20/2015 12:04 PM - Emmanuel GARETTE

*- Remaining (hours) changed from 2.0 to 0.25*

#### #5 - 10/30/2015 01:34 PM - Daniel Dehennin

*- Status changed from Résolu to Fermé*

*- Remaining (hours) changed from 0.25 to 0.0*

```
root@amonecole:~# rgrep --color ' sha256' /usr/share/eole/creole/distrib/
/usr/share/eole/creole/distrib/ca-eole.conf:default_md          = sha256
/usr/share/eole/creole/distrib/ca-eole.conf:default_md          = sha256
/usr/share/eole/creole/distrib/certif-eole.conf:default_md              = sha256
/usr/share/eole/creole/distrib/certif-eole.conf:default_md              = sha256
```

Ok dans firefox.