Distribution EOLE - Tâche #36802

Scénario # 36416 (Terminé (Sprint)): L'archive générée par gen_rpt devrait être chiffrée

Etude

25/04/2025 09:24 - Emmanuel GARETTE

Statut:	Fermé	**Début:**	01/10/2022
Priorité:	Normal	**Echéance:**	
Assigné à:	Emmanuel GARETTE	**% réalisé:**	100%
Version cible:	Livraison Cadoles - MEN 31/12/2024 (100)	**Temps estimé:**	0.00 heure
		Temps passé:	0.00 heure

Description

Proposition : utiliser la clé publique des dépôts dont seul le PCLL dispose de la clé privée.

Si je regarde les clefs publiques en question :

```
root@amonecole:~# gpg --keyring /etc/apt/trusted.gpg.d/eole-archive-eole-2.9-jammy-jellyfish.gpg --list-keys
/etc/apt/trusted.gpg.d/eole-archive-eole-2.9-jammy-jellyfish.gpg
----------------------------------------------------------------
pub   rsa4096 2022-01-19 [SC]
      06EE28059F3152E87B618743F7D6DCB146E68BDF
uid           [ inconnue] EOLE Repository (EOLE 2.9/Jammy Jellyfish) <repository@listeseole.ac-dijon.fr>
```

Si j'en crois https://lists.gnupg.org/pipermail/gnupg-users/2009-March/035929.html

```
> What do the letters to the right of the words "usage" mean?
> (S,C,A,E) I can only guess |S|ign, |E|ncrypt, ....

(S)ign: sign some data (like a file)
(C)ertify: sign a key (this is called certification)
(A)uthenticate: authenticate yourself to a computer (for example,
logging in)
(E)ncrypt: encrypt data
```

Il manque un ligne qui ressemblerait à :

```
sub   xxxxxx 20XX-XX-XX [E]
```

Donc on peut signer mais pas chiffrer avec ces clefs publique.

D'une façon plus général je ne crois pas que GPG soit l'outil le plus adapté au besoin :

- comment gérer la confiance ?

-- comment organiser l'échange de clef ?

-- est-ce que l'organisme doit faire un clé GPG pour l'organisme + une clef par serveur (bof) qu'il sur-signe ?
-- est-ce que l'organisme doit faire un clé GPG pour l'organisme + une clef par technicien qu'il sur-signe ?

- comment gérer la protection des clefs (je parle en plus de la passphrase) : comment partager les clefs ? Via Zéphir ? Sur tous les serveurs ?

Je ne vois pas du tout l'intérêt de s'embêter avec le partage de clef publique.

Je propose donc :

- EOLE créer un certificat avec l'algorithme RSA (via openssl par exemple) et diffuse la clef publique sur tous les serveurs
- gen_rpt chiffre le fichier sans avoir besoin d'une clef privée
- EOLE peut déchiffer le fichier mais cela ne garanti pas que l'émetteur est bien celui qu'il prétend être.

Historique

#1 - 25/04/2025 09:51 - Emmanuel GARETTE

- Description mis à jour

#2 - 28/04/2025 11:49 - Daniel Dehennin

Effectivement, il manque une clef pour chiffrer à destination des clefs des dépôts :

```
gpg: DBG: finish_lookup: checking key FCA05930 (all)(req_usage=2)
gpg: DBG:     no suitable subkeys found - trying primary
gpg: DBG:     primary key usage does not match: want=2 have=5
gpg: DBG:     no suitable key found -  giving up
```

Nous pouvons utiliser GPG sans avoir de clef de signature sur les serveurs, par exemple :

- On installe la clef des développeurs

```
root@eolebase:~# apt install eole-team-keyring
```

- On chiffre un fichier sans aucune question

```
root@eolebase:~# gpg --trust-model always --batch --yes --no-default-keyring --keyring /usr/share/keyrin
gs/eole-team-keyring.gpg --encrypt --armor -r Joel.Cuissinat@region-academique-bourgogne-franche-comte.fr
/root/getVMContext.sh
```

Nous finissions bien avec un fichier chiffré **getVMContext.sh.asc** :

```
-----BEGIN PGP MESSAGE-----

hQGMA1te3Giqs72wAQwAm7Wd6z2xBhMAQKMMub3PP5JtlpkhrYgcsjT+jSle3eU6
o2CrRX8NjJrqemADTG1yKIerE0ycQJgookHKgirtaHxuwlTPI+6xmqO23qdQHYRp
tGhqO0jI7ritv4JNcEjLM3H4jZm2kZjKR+aaHTD+fTb1IUEimPpcmZBx9P6EjKI+
/fDV4xuusYYgHvDc/z2BdSK9VE9UOUHoV3ATEMkxSW6GubWhMUMzkFHurAHh6k+1
MLVFPYpGOg7gbsR8zVKAGl0881WqHkt9gSYmLqqIaKOSY1K3Jf1oWsiDj+75mUfB
+FvWIjLPtpI3UT/CrvPBPcfAI3JulfCjdSFWnGC6SubY5vxyauk7HjoVrTngq0rq
NZME/t5NJvy5pzB/TMYx3bj7t1EGhSk5R/uxQFvX8fyOUbrUZImcE0Vt34sfJy0m
JBhZWnjwZGfE6EKl6HMnYrlWctVS8MAnpTMGUWC22a4ZoOHt7vAruYPWBvoFoKKB
etoOIDUkpeYybcJ0c3cr0ukBA19mbAAlggR/G5zBb1Ri0hl56W98Z2PwdM3HZ+mK
2P7t9YWRVQjlK+s9SM66zQm4Q+fhWJs8DbOskmz+XbJ8etLJp6C0kXebmXYTSkTy
kbAjwggt3EJCmdWKYx+fgctjfiZ8gjOYVG5xFKQp2/BVHJJ3y5l3V29V2LU2ILFg
+nOX/1S+DKOk7WBH5Y7zxjJ0iUEulAznT2QhMei2ulj58IKSarD8wsT3MLviADBd
96C5pjzmJ8B1rTQDYDJlCW35FKgLg3F0UQdc6HFK1/AK4W7nE5ZJufORc/hmu5l5
sljP89tgxKLu3dDP7Qy3zGQyuYOfeMuaq+D4+zkyHCXyPSFD4/d9Jn+N5BV7bm70
Vk3UbLriCDGar5Iaycc+RACKGnhja1SDv1Fn2LiGyHf7b2uoeaqeDr1J9uzt36y8
jt1cNSsjoM4wjB0OPDIJfjyfxZLtjAIeMfj04axojHgxOjzC1lfAMrKnjWmfvw9v
WOn8PgzG6O/XUKLIpP3ojAtEQWoXhbKUr14lBWuIjuIpxHLyZKZmaPgxied67TNM
FxSIkrfahaMK7J+Bd2IvkPnhvaCAl+0QkDkfZfZFKaPdd7O9eFtswDn5BdwoKQ0U
65bTiS6JMfnKEX94hZlGNk/OBTqeXhtmevxh1VkGA1vJICxx7ceTLIx8UX87o7ar
psExCZn6pZC012cAYIuv9SYKdRLFCOdYoVAZRtRptugbWkUErWV3fLA8O4XmRlYx
```

```
msCusAv+af4oLwquRuGrLQvsaJ3IXSIwt56iDSebgShKBkivUerqLtfEQNjbwUVn
p6Nh3+N0m3v355HiUSI4C+IpJO/UKsOMRuBCCigLqA2FxDBG7a3Are5PhDZAu0EM
3p+I2222ylb29CWtds8xM+Zi17q6b5fsho8hKTEumG0np8QzTZJptYhpPPln/6np
96bSInIHegE8+nEL4e14/qvwGclT24B5DplZa2+YSWjysyb/F4hAIuS7GqyIptsZ
JD4PLYJBPBm+bGOKtN7errkt4B3RQ91j2XDO6HGYUyQndcylsIpCAsRTS3Er2mHW
mFUQljl1a5LfJqTJplNZOi8/j4WIiJCgn5fFuT1hQu0G2mzFD2wh8hvtzfFzWnoH
RWPxVgkFuQl+0/f/62TdMBEksopl6ZweICUr4naW6RaSTFo2CQDo6k5HIR9KBFoE
rfXjYktppgTNF+HRiyYN6Nhv1ENDgMdggNS43OG1yeN5o7DEqbIlIu1orHWgnFjS
0EYJ0qaDXtZGYUU4LrktPWRgpwl3z3PWvpJKFrN00kaJGV1HY2/lPiSAuJeT6sEO
VdRzGdQKPWB28XMe682ReSBjP10=
=1ArK
-----END PGP MESSAGE-----
```

Dans ce cas, nous pouvons fournir une clef de chiffrement GPG dédiée.

#3 - 29/04/2025 13:57 - Emmanuel GARETTE

- Statut changé de Nouveau à À valider

- Assigné à mis à Emmanuel GARETTE

- % réalisé changé de 0 à 100

Commit fait en 2.7.2 mais commité que sur 2.9 et 2.10 (la clef publique ne permet pas de chiffrer en 2.7 et 2.8 pour le moment).

#4 - 29/04/2025 14:37 - Benjamin Bohard

- Statut changé de À valider à Résolu

#5 - 22/05/2025 15:44 - Joël Cuissinat

- Statut changé de Résolu à Fermé

- Restant à faire (heures) mis à 0.0

OK