

VVT 2014 : Actu Truecrypt

Le contexte :

- Logiciel de chiffrement
- Première version en 2004, version 7.1a en Février 2012
- Recommandé, jusqu'en Mai 2014 par l'ANSSI
- Certifié par L'ANSSI (version 6.0 en 2008 et 7.1a en Octobre 2013)
- Déployé par certaines unités CNRS dans le cadre d'une politique de chiffrement des portables
- Seul logiciel :
 - disponible sur les systèmes d'exploitations les plus communs
 - simple d'utilisation
 - Gratuit
 - offre la possibilité de chiffrer des volumes, des conteneurs, de masquer la présence de conteneurs

Truecrypt : la situation

- Version 7.1a complète (cf certification ANSSI), Février 2012
- Version 7.2, diffusée par les membres du projet en Mai 2014, est fortement dégradée : elle permet seulement de lire des conteneurs truecrypt, il est désormais impossible d'en créer de nouveau.
- La documentation, le site truecrypt.org et le site truecrypt.sourceforge.net renvoient à l'utilisation de BitLocker, de FileVault pour OsX, ou aux outils linux disponibles.
- A priori, les développeurs auraient décidé d'arrêter. Leurs raisons restent mystérieuses.

Conséquences

- Agitation légitime des utilisateurs
- Etat du projet :
 - Peu de chances de “forker”, problème de license
 - Pas encore de prétendants pour le remplacer dans tous ses aspects. L’ANSSI indique plusieurs solutions, en fonction de l’objectif
- En attendant, la version 7.1a reste toujours “certifiée”