Nouveau guide pour l'usage de la cryptographie dans les agences fédérales

Publié le jeudi 5 janvier 2006
Voir en ligne : https://www.france-science.org/Nouveau-guide-pour-l-usage-de-la.html

Le NIST a mis à jour son document "Special Publication 800-21-1" qui consiste en un ensemble de préconisations en matière de cryptographie. Ce guide a pris une importance renouvelée dans le cadre du FISMA (Federal Information Security Management Act) de 2002, qui établit des exigences de certification et d'accréditation de la sécurité des systèmes d'information des agences fédérales. Les algorithmes reposant sur AES ou TDEA, ou sur les courbes elliptiques sont préconisés.
Un peu plus tôt, le NIST a émis en décembre un guide de choix de générateurs de nombres aléatoires, autre composante significative en matière de sécurité. Le NIST préconise des générateurs déterministes de bits aléatoires.

Source :

- http://www.gcn.com/vol1_no1/daily-updates/37840-1.html
- http://csrc.nist.gov/publications/drafts/sp800-90_draft_dec2005.pdf

Pour en savoir plus, contacts :

http://csrc.nist.gov/publications/nistpubs/800-21-1/sp800-21-1_Dec2005.pdf
Code brève
ADIT : 31458

Rédacteur :

Sébastien Morbieu, tic.vi@ambafrance-us.org