

Un système de cryptage RSA pour les cartes à puce.

Fujitsu a développé un système de cryptage capable d'assurer la sécurité des informations contenues dans une carte à puce nécessitant un temps de décryptage de quelques 20 millions d'années, même pour un supercalculateur....

Fujitsu

envisage de commercialiser cette technologie d'ici un an afin de sécuriser les signatures électroniques pour les institutions financières, notamment pour les cartes de crédit.

La technologie de Fujitsu utilise le système RSA, le cryptage le plus largement utilisé, avec un nombre de 2048 chiffres pour code, soit une taille double des codes utilisés par les autres technologies de cryptage RSA.

Normalement une telle taille pose un problème au niveau du temps de traitement de la carte à puce, cependant Fujitsu a développé un nouveau circuit qui permet de traiter les cartes à puce à grande vitesse et faible puissance, ce qui rend à présent la commercialisation d'un tel système possible.

Ambassade de France à Tokyo

Source & infos complémentaires :

Agence pour la Diffusion de l'Information Technologique

Par

Publié sur Cafeduweb - Archives le mardi 20 juillet 2004

Consultable en ligne : <http://archives.cafeduweb.com/lire/4650-systeme-cryptage-rsa-pour-les-cartes-a-puce.html>