RFC 1984 : IAB and IESG Statement on Cryptographic Technology and the Internet

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 22 septembre 2005

Date de publication du RFC : Août 1996

https://www.bortzmeyer.org/1984.html

Un RFC très politique, que ce 1984 qui s'attaque aux restrictions d'usage à la cryptographie. Au moment où il est sorti, la cryptographie était de fait interdite en France <https://www.bortzmeyer.org/crypto.html> (et la situation, si elle s'est améliorée, est encore loin d'être parfaite). Et les États-Unis restreignaient très sévèrement l'exportation de logiciels cryptographiques (là encore, ces restrictions n'ont pas complètement disparu).

Le RFC prend nettement position : l'IAB et l'IESG, ensemble, affirment que la cryptographie forte (pas les systèmes ultra-bridés qui étaient proposés à l'époque avec les navigateurs Web) est indispensable à la sécurité de l'Internet, qu'il n'existe aucune autre méthode réaliste d'assurer une sécurité raisonnable sur un réseau ayant l'architecture de l'Internet et que cette sécurité ne doit pas être sacrifiée aux intérêts des polices et des services secrets.

Le RFC se penche aussi sur des cas plus techniques, comme sur les clés cryptographiques ne servant qu'à la signature, qui ne devraient jamais faire l'objet d'un dépôt de séquestre, puisqu'il n'existe aucune raison légitime de les "saisir".

Ce RFC dont le numéro ne doit rien au hasard, a marqué une étape dans la construction politique de l'Internet.