RFC 4998 : Evidence Record Syntax (ERS)

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 11 octobre 2007

Date de publication du RFC : Août 2007

https://www.bortzmeyer.org/4998.html

Ce RFC spécifie un format pour signer, sur le très long terme, des enregistrements. L'exigence de durée est un gros problème pour la cryptographie car les algorithmes de signature peuvent être cassés avec le temps.

Conçu dans le cadre du groupe de travail IETF ltans <http://www.ietf.org/html.charters/ltans-charter.html>, ce RFC propose une méthode simple. Chaque signature est accompagnée d'une date et les dates sont elles-même signées (et resignées si un algorithme s'avère à l'usage trop simple, donc une application peut avoir à suivre une chaîne de signatures, ce que décrit la section 5). Le RFC 4810 [1] qui donnait le cahier des charges du groupe de travail précisait déjà la nécessité de prouver l'intégrité d'un document après des dizaines d'années, malgré les progrès qu'avait fait la cryptographie pendant ce temps.

Notre RFC spécifie également d'autres techniques pour résister au passage du temps, comme le fait de mettre autant que possible au moins deux signatures, avec des algorithmes différents, pour augmenter les chances qu'un d'eux résiste (section 7).

Le format est spécifié en utilisant le langage ASN.1.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc4810.txt