RFC 7562 : Transport Layer Security (TLS) Authorization Using DTCP Certificate

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 10 juillet 2015

Date de publication du RFC : Juillet 2015

https://www.bortzmeyer.org/7562.html

Le protocole de sécurité TLS permet différents types d'autorisation et ce RFC en ajoute un nouveau, par la présentation d'un certificat DTCP. DTCP est un mécanisme de menottes numériques, et cette extension à TLS permet désormais « TLS pour les ayant-droits ».

DTCP, également connu sous le nom de 5C, est un système fermé. À l'heure actuelle, une version apparemment à jour de la spécification est disponible <http://www.dtcp.com/documents/dtcp/info-20130605-dtcp-v1-rev-1-7-ed2.pdf>. Ce système DTCP est assez répandu dans des télévisions, des tablettes, des consoles de jeu... Les certificats DTCP (qui ne sont **pas** des certificats X.509) sont émis par DTLA <http://www.dtcp.com/> (section 2.1 du RFC).

Le RFC 5878 [1] spécifie l'extension de TLS à d'autres mécanismes d'autorisation. Et le RFC 4680 décrit l'ajout de données supplémentaires (le certificat) dans le message `Handshake` de TLS.

Le type d'autorisation IANA `dtcp_authorization` est désormais enregistré à l'IANA <https://www.iana.org/assignments/tls-parameters/tls-parameters.xml#authorization-data>.

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc5878.txt`