RFC 9851 : TLS 1.2 is in Feature Freeze

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 16 juillet 2026

Date de publication du RFC : Juillet 2026

https://www.bortzmeyer.org/9851.html

Vous pouvez toujours utiliser la version 1.2 de TLS mais ne demandez pas des ajouts, des extensions, etc. Elle est désormais gelée, aucune nouvelle fonction ne sera ajoutée, tout le travail se fait désormais sur la meilleure version, la 1.3, normalisée dans le RFC 9846[1].

TLS 1.3 (RFC 9846) a en effet plusieurs avantages : il chiffre une plus grande proportion de la négociation au début de la session et, surtout, il a fait l'objet d'une analyse de sécurité formelle, donc il est considéré comme plus sûr. Dans ces conditions, continuer à travailler sur la version 1.2 (RFC 5246) n'a plus guère de sens. TLS 1.2 n'est pas abandonné (ne paniquez pas si vous l'utilisez encore), mais il n'évoluera plus.

Il y aura quand même quelques nouveautés permises : les identificateurs ALPN <https://www.iana.org/assignments/tls-extensiontype-values/tls-extensiontype-values.xml#alpn-protocol-i
les "*exporter labels*" <https://www.iana.org/assignments/tls-parameters/tls-parameters.xml#exporter-labels>, et, bien sûr, des éventuels changements nécessaires en urgence si une faille de sécurité était découverte dans la version 1.2.

Sinon, vous avez certainement entendu parler de cryptographie post-quantique, qui remplacera les bons vieux RSA et ECDSA si un calculateur quantique futur le nécessite. Les algorithmes sont déjà normalisés <https://www.bortzmeyer.org/nist-pq.html> mais il reste à les intégrer dans TLS. Celui-ci va permettre d'utiliser ces nouveaux algorithmes mais cela ne concernera **que la version 1.3** (section 2 du RFC), la 1.2 étant gelée. La 1.2 ne survivra donc pas aux CRQC ("*Cryptographically Relevant Quantum Computers*"). (Le RFC rappelle que la première discussion sérieuse à l'IETF sur ce sujet était en 2016 <https://www.ietf.org/proceedings/95/slides/slides-95-cfrg-4.pdf>. La normalisation prend du temps.)

Notez que cette décision de gel ne concerne pas DTLS (RFC 6347), seulement TLS.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc9846.txt