Deprecating MD5 and SHA-1 signature hashes in TLS 1.2

draft-lvelvindron-tls-md5-sha1-deprecate

Proposed changes

- Make signature_algorithms extension mandatory.

- Forbid MD5 and SHA-1-based algorithms in signature_algorithms, CertificateRequest, ServerKeyExchange and CertificateVerify.

Why now ?

Deprecating TLS 1.0 and TLS 1.1

(See archives on TLS WG)

Statistics (from Cloudflare)

Data collected from samples of TLS 1.2 connections to Cloudflare’s edge network shows that percentage of connections with no signature_algorithms extension, and of connections with only MD5 and/or SHA-1-based algorithms is negligible.

Impact

Share your statistics with us.

Questions

Please do not hesitate.

-Alessandro Ghedini (Cloudflare)

-Kathleen Moriarty (Dell)

-Loganaden Velvindron (cyberstorm.mu)