draft-ietf-tls-md5-sha1-deprecate

A.Ghedini, Kathleen Kathleen Moriarty, Loganaden Velvindron
Clients SHOULD NOT include MD5 and SHA-1 in signature_algorithms extension.

a client does not send a signature_algorithms extension, then the server
MUST abort the handshake and send a handshake_failure alert.

!</t>
</section>

<section anchor="cert_requests" title="Certificate Request">

Clients SHOULD NOT include MD5 and SHA-1 in signature_algorithms extension.

If

a client does not send a signature_algorithms extension, then the server
MUST abort the handshake and send a handshake_failure alert, except when
digital signatures are not used (for example, when using PSK ciphers).

!</t>
</section>

<section anchor="cert_requests" title="Certificate Request">
Can we go forward with WGLC?

Please let us know.