draft-ietf-tls-md5-sha1-deprecate

A.Ghedini, Kathleen Kathleen Moriarty, Loganaden Velvindron

Only 1 change

draft-ietf-tls-md5-sha1-deprecate-00.xml

-157,7 +157,8 @@

```
<t>
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">
```

```
157      <t>
158      Clients SHOULD NOT include MD5 and SHA-1 in  signature_algorithms extension.
         If
159      a client does not send a  signature_algorithms extension, then the server
160  +   MUST abort the handshake and send a handshake_failure alert, except when
161  +   digital signatures are not used (for example, when using PSK ciphers).
162      </t>
163      </section>
164      <section anchor="cert_requests" title="Certificate Request">
```

Can we go forward with WGLC ?

Please let us know.