IANA Registry Updates for TLS and DTLS

draft-ietf-tls-rfc8447bis

Sean Turner, Joe Salowey

TLS@IETF114 - 20220725

Refresher

Adopted March 2022

-00 included resolution of SAAG consensus decision to add “D” to Recommended column values

-01 first attempt at applying “D” to the registries

NOTE:

- To make it easier on IANA, we are indicating which requests have already been deployed.
- New registrations since RFC 8447, are making this update mildly painful because we need to note which ones have already been assigned.

References: Update to draft-ietf-tls-rfc8446bis and draft-ietf-tls-rfc8447bis

ExtensionType Values: N → D

truncated_hmac
connection_id (deprecated)

Cipher Suites Registry: Hoping -deprecate-obsolete-kex will address this registry?

****NEW****:

- It was short-sighted on our part to not include the Recommended column in the HashAlgorithm, SignatureAlgorithm, and ClientCertificateTypes.
- The thinking, at the time, was that these were orphaned by TLS 1.3.
- But, these registries do apply to TLS 1.2 and TLS 1.2 is not going anywhere anytime soon. The next two slides are the Recommended values we are suggesting.

HashAlgorithm

none	Y
md5	**D**
sha1	**D**
sha224	**D**
sha256	Y
sha384	Y
sha512	Y
Intrinsic	Y

SignatureAlgorithm

anonymous	**N**
rsa	Y
dsa	**N**
ecdsa	Y
ed25519	Y
ed448	Y
gostr34102012_256	**N**
gostr34102012_512	**N**

NOTE: The ones in **bold** are to contrast the Y ones.

ClientCertificateTypes

rsa_sign	Y
dss_sign	N
rsa_fixed_dh	**N**
dss_fixed_dh	**N**
rsa_ephemeral_dh_RESERVED	D
dss_ephemeral_dh_RESERVED	D

fortezza_dms_RESERVED	D
ecdsa_sign	Y
rsa_fixed_ecdh	**N**
ecdsa_fixed_ecdh	**N**
gost_sign256	N
gost_sign512	N

NOTE: The ones in **white** we could also see as D.

Open Issues

EC Curve Types, EC Curve Point Types, and ClientCertificateTypes also apply to TLS 1.2.

Handle in this I-D or -deprecate-obsolete-kex?

Registered Values:

EC Point Formats

uncompressed
ansiX962_compressed_prime
ansiX962_compressed_char2

EC Curve Types

explicit_prime
explicit_char2
named_curve

Next Steps

Revise

Plead for reviews

Ask for WGLC