TLS 1.3 MTI

IETF-92, Dallas

Mandatory to Implement Cipher Suites

- Symmetric Ciphers

  MUST AES-GCM 128
  [SHOULD ChaCha20-Poly1305]*

- Hash

  MUST SHA-256

- Key Agreement

  MUST ECDH with P-256
  [SHOULD ECDH with 25519]*

- Signature

  MUST RSA
  MUST ECDSA with P-256

MTI != MTU

[]* CFRG Dependency