26.5.2020

# CRYPTO

determining if crypto support is unavailable

class: Certificate
- exportChallenge
- exportPublicKey
- verifySpkac

legacy API
new Certificate()
- exportChallenge
- exportPublicKey
- verifySpkac

class: Cipher
- final
- setAAD
- getAuthTag
- setAutoPadding
- update

class: Decipher
- final
- setAAD
- setAuthTag
- setAutoPadding
- update

class: DiffieHellman
- computeSecret
- generateKeys
- getGenerator
- getPrime
- getPrivateKey
- getPublicKey
- setPrivateKey
- setPublicKey
- verifyError

class: DiffieHellmanGroup

class: ECDH
ECDH.convertKey
ecdh.computeSecret
- generateKeys
- getPrivateKey
- getPublicKey
- setPrivateKey
- setPublicKey

class: Hash
hash.copy
- digest
- update

class: Hmac
hmac.digest
- update

class: KeyObject
- asymmetricKeyType
- export
- symmetricKeySize
- type

class: Sign
- Sign
- update

class: Verify
- update
- verify

Crypto. Constants
- createCipheriv
- createDecipheriv
- createDiffieHellman
- createDiffieHellman
- createDiffieHellmanGroup
- createECDH
- createHash
- createHmac
- createPrivateKey
- createPublicKey
- createSecretKey
- createSign
- createVerify
- diffieHellman
- generateKeyPair
- generateKeyPairSync

- getCiphers
- getCurves
- getDiffieHellman
- getFips
- getHashes
- pbkdf2
- pbkdf2Sync
- privateDecrypt
- privateEncrypt
- randomBytes
- randomFillSync
- randomFill
- scrypt
- scryptSync
- setEngine
- setFips
- Sign
- timingSafeEqual
- Verify

notes
legacy streams API (pre node.js V.0.10)
recent ECDH changes
support for weak or compromised algorithms.
CCM mode.

Crypto constants
OpenSSL options
openSSL engine constants
other openSSL constants
nodejs crypto constants