Web Crypto API

▶ History

Stability: 2 - Stable

Node.js provides an implementation of the standard Web Crypto API.

Use `globalThis.crypto` or `require('node:crypto').webcrypto` to access this module.

```
const { subtle } = globalThis.crypto;

(async function() {

  const key = await subtle.generateKey({
    name: 'HMAC',
    hash: 'SHA-256',
    length: 256,
  }, true, ['sign', 'verify']);

  const enc = new TextEncoder();
  const message = enc.encode('I love cupcakes');

  const digest = await subtle.sign({
    name: 'HMAC',
  }, key, message);

})(); copy
```

Examples

Generating keys

The `<SubtleCrypto>` class can be used to generate symmetric (secret) keys or asymmetric key pairs (public key and private key).

AES keys

```
const { subtle } = globalThis.crypto;

async function generateAesKey(length = 256) {
  const key = await subtle.generateKey({
    name: 'AES-CBC',
    length,
  }, true, ['encrypt', 'decrypt']);

  return key;
} copy
```

ECDSA key pairs

```
const { subtle } = globalThis.crypto;

async function generateEcKey(namedCurve = 'P-521') {
  const {
    publicKey,
    privateKey,
  } = await subtle.generateKey({
    name: 'ECDSA',
    namedCurve,
  }, true, ['sign', 'verify']);

  return { publicKey, privateKey };
} copy
```

Ed25519/Ed448/X25519/X448 key pairs

> Stability: 1 - Experimental

```
const { subtle } = globalThis.crypto;

async function generateEd25519Key() {
  return subtle.generateKey({
    name: 'Ed25519',
  }, true, ['sign', 'verify']);
}

async function generateX25519Key() {
  return subtle.generateKey({
    name: 'X25519',
  }, true, ['deriveKey']);
} copy
```

HMAC keys

```
const { subtle } = globalThis.crypto;

async function generateHmacKey(hash = 'SHA-256') {
  const key = await subtle.generateKey({
    name: 'HMAC',
    hash,
  }, true, ['sign', 'verify']);

  return key;
} copy
```

RSA key pairs

```
const { subtle } = globalThis.crypto;
const publicExponent = new Uint8Array([1, 0, 1]);

async function generateRsaKey(modulusLength = 2048, hash = 'SHA-256') {
  const {
    publicKey,
    privateKey,
  } = await subtle.generateKey({
    name: 'RSASSA-PKCS1-v1_5',
    modulusLength,
    publicExponent,
    hash,
  }, true, ['sign', 'verify']);

  return { publicKey, privateKey };
} copy
```

Encryption and decryption

```
const crypto = globalThis.crypto;

async function aesEncrypt(plaintext) {
  const ec = new TextEncoder();
  const key = await generateAesKey();
  const iv = crypto.getRandomValues(new Uint8Array(16));

  const ciphertext = await crypto.subtle.encrypt({
    name: 'AES-CBC',
    iv,
  }, key, ec.encode(plaintext));

  return {
    key,
    iv,
    ciphertext,
  };
}

async function aesDecrypt(ciphertext, key, iv) {
  const dec = new TextDecoder();
  const plaintext = await crypto.subtle.decrypt({
    name: 'AES-CBC',
    iv,
  }, key, ciphertext);

  return dec.decode(plaintext);
} copy
```

Exporting and importing keys

```
const { subtle } = globalThis.crypto;

async function generateAndExportHmacKey(format = 'jwk', hash = 'SHA-512') {
  const key = await subtle.generateKey({
    name: 'HMAC',
    hash,
  }, true, ['sign', 'verify']);

  return subtle.exportKey(format, key);
}

async function importHmacKey(keyData, format = 'jwk', hash = 'SHA-512') {
  const key = await subtle.importKey(format, keyData, {
    name: 'HMAC',
    hash,
  }, true, ['sign', 'verify']);

  return key;
} copy
```

Wrapping and unwrapping keys

```
const { subtle } = globalThis.crypto;

async function generateAndWrapHmacKey(format = 'jwk', hash = 'SHA-512') {
  const [
    key,
    wrappingKey,
  ] = await Promise.all([
    subtle.generateKey({
      name: 'HMAC', hash,
    }, true, ['sign', 'verify']),
    subtle.generateKey({
      name: 'AES-KW',
      length: 256,
    }, true, ['wrapKey', 'unwrapKey']),
  ]);

  const wrappedKey = await subtle.wrapKey(format, key, wrappingKey, 'AES-KW');

  return { wrappedKey, wrappingKey };
}

async function unwrapHmacKey(
  wrappedKey,
  wrappingKey,
  format = 'jwk',
  hash = 'SHA-512') {

  const key = await subtle.unwrapKey(
    format,
    wrappedKey,
    wrappingKey,
    'AES-KW',
    { name: 'HMAC', hash },
    true,
    ['sign', 'verify']);

  return key;
} copy
```

Sign and verify

```
const { subtle } = globalThis.crypto;

async function sign(key, data) {
  const ec = new TextEncoder();
  const signature =
    await subtle.sign('RSASSA-PKCS1-v1_5', key, ec.encode(data));
  return signature;
}

async function verify(key, signature, data) {
  const ec = new TextEncoder();
  const verified =
    await subtle.verify(
      'RSASSA-PKCS1-v1_5',
      key,
      signature,
      ec.encode(data));
  return verified;
} copy
```

Deriving bits and keys

```
const { subtle } = globalThis.crypto;

async function pbkdf2(pass, salt, iterations = 1000, length = 256) {
  const ec = new TextEncoder();
  const key = await subtle.importKey(
    'raw',
    ec.encode(pass),
    'PBKDF2',
    false,
    ['deriveBits']);
  const bits = await subtle.deriveBits({
    name: 'PBKDF2',
    hash: 'SHA-512',
    salt: ec.encode(salt),
    iterations,
  }, key, length);
  return bits;
}

async function pbkdf2Key(pass, salt, iterations = 1000, length = 256) {
  const ec = new TextEncoder();
  const keyMaterial = await subtle.importKey(
    'raw',
    ec.encode(pass),
    'PBKDF2',
    false,
    ['deriveKey']);
  const key = await subtle.deriveKey({
    name: 'PBKDF2',
    hash: 'SHA-512',
    salt: ec.encode(salt),
    iterations,
  }, keyMaterial, {
    name: 'AES-GCM',
    length,
  }, true, ['encrypt', 'decrypt']);
  return key;
} copy
```

Digest

```
const { subtle } = globalThis.crypto;

async function digest(data, algorithm = 'SHA-512') {
  const ec = new TextEncoder();
  const digest = await subtle.digest(algorithm, ec.encode(data));
  return digest;
} copy
```

Algorithm matrix

The table details the algorithms supported by the Node.js Web Crypto API implementation and the APIs supported for each:

Algorithm	generateKey	exportKey	importKey	encrypt	decrypt	wrapKey	unwrapKey	deriveBits	deriveKey	sign	verify	di ge
'RSASSA-PKCS1-v1_5'	✓	✓	✓							✓	✓	
'RSA-PSS'	✓	✓	✓							✓	✓	
'RSA-OAEP'	✓	✓	✓	✓	✓	✓	✓					
'ECDSA'	✓	✓	✓							✓	✓	
'Ed25519' [1]	✓	✓	✓							✓	✓	
'Ed448' [1]	✓	✓	✓							✓	✓	
'ECDH'	✓	✓	✓					✓	✓			
'X25519' [1]	✓	✓	✓					✓	✓			
'X448' [1]	✓	✓	✓					✓	✓			
'AES-CTR'	✓	✓	✓	✓	✓	✓	✓					
'AES-CBC'	✓	✓	✓	✓	✓	✓	✓					
'AES-GCM'	✓	✓	✓	✓	✓	✓	✓					
'AES-KW'	✓	✓	✓			✓	✓					
'HMAC'	✓	✓	✓							✓	✓	
'HKDF'		✓	✓					✓	✓			
'PBKDF2'		✓	✓					✓	✓			
'SHA-1'												✓
'SHA-256'												✓
'SHA-384'												✓
'SHA-512'												✓

Class: `Crypto`

Added in: v15.0.0

`globalThis.crypto` is an instance of the `Crypto` class. `Crypto` is a singleton that provides access to the remainder of the crypto API.

`crypto.subtle`

Added in: v15.0.0

- Type: <SubtleCrypto>

Provides access to the `SubtleCrypto` API.

`crypto.getRandomValues(typedArray)`

Added in: v15.0.0

- `typedArray` <Buffer> | <TypedArray>
- Returns: <Buffer> | <TypedArray>

Generates cryptographically strong random values. The given `typedArray` is filled with random values, and a reference to `typedArray` is returned.

The given `typedArray` must be an integer-based instance of <TypedArray>, i.e. `Float32Array` and `Float64Array` are not accepted.

An error will be thrown if the given `typedArray` is larger than 65,536 bytes.

`crypto.randomUUID()`

Added in: v16.7.0

- Returns: <string>

Generates a random RFC 4122 version 4 UUID. The UUID is generated using a cryptographic pseudorandom number generator.

Class: `CryptoKey`

Added in: v15.0.0

`cryptoKey.algorithm`

Added in: v15.0.0

- Type: <AesKeyGenParams> | <RsaHashedKeyGenParams> | <EcKeyGenParams> | <HmacKeyGenParams>

An object detailing the algorithm for which the key can be used along with additional algorithm-specific parameters.

Read-only.

`cryptoKey.extractable`

Added in: v15.0.0

- Type: <boolean>

When `true`, the <CryptoKey> can be extracted using either `subtleCrypto.exportKey()` or `subtleCrypto.wrapKey()`.

Read-only.

`cryptoKey.type`

Added in: v15.0.0

- Type: <string> One of `'secret'`, `'private'`, or `'public'`.

A string identifying whether the key is a symmetric (`'secret'`) or asymmetric (`'private'` or `'public'`) key.

`cryptoKey.usages`

Added in: v15.0.0

- Type: <string[]>

An array of strings identifying the operations for which the key may be used.

The possible usages are:

- `'encrypt'` - The key may be used to encrypt data.
- `'decrypt'` - The key may be used to decrypt data.
- `'sign'` - The key may be used to generate digital signatures.
- `'verify'` - The key may be used to verify digital signatures.
- `'deriveKey'` - The key may be used to derive a new key.
- `'deriveBits'` - The key may be used to derive bits.
- `'wrapKey'` - The key may be used to wrap another key.
- `'unwrapKey'` - The key may be used to unwrap another key.

Valid key usages depend on the key algorithm (identified by `cryptokey.algorithm.name`).

Key Type	`'encrypt'`	`'decrypt'`	`'sign'`	`'verify'`	`'deriveKey'`	`'deriveBits'`	`'wrapKey'`	`'unwrapKey'`
`'AES-CBC'`	✓	✓					✓	✓
`'AES-CTR'`	✓	✓					✓	✓
`'AES-GCM'`	✓	✓					✓	✓
`'AES-KW'`							✓	✓
`'ECDH'`					✓	✓		
`'X25519'` [1]					✓	✓		
`'X448'` [1]					✓	✓		
`'ECDSA'`			✓	✓				
`'Ed25519'` [1]			✓	✓				
`'Ed448'` [1]			✓	✓				
`'HDKF'`					✓	✓		
`'HMAC'`			✓	✓				
`'PBKDF2'`					✓	✓		
`'RSA-OAEP'`	✓	✓					✓	✓
`'RSA-PSS'`			✓	✓				
`'RSASSA-PKCS1-v1_5'`			✓	✓				

Class: `CryptoKeyPair`

Added in: v15.0.0

The `CryptoKeyPair` is a simple dictionary object with `publicKey` and `privateKey` properties, representing an asymmetric key pair.

`cryptoKeyPair.privateKey`

Added in: v15.0.0

- Type: <CryptoKey> A <CryptoKey> whose `type` will be `'private'` .

`cryptoKeyPair.publicKey`

Added in: v15.0.0

- Type: <CryptoKey> A <CryptoKey> whose `type` will be `'public'` .

Class: `SubtleCrypto`

Added in: v15.0.0

`subtle.decrypt(algorithm, key, data)`

Added in: v15.0.0

- `algorithm` : <RsaOaepParams> | <AesCtrParams> | <AesCbcParams> | <AesGcmParams>
- `key` : <CryptoKey>
- `data` : <ArrayBuffer> | <TypedArray> | <DataView> | <Buffer>
- Returns: <Promise> Fulfills with an <ArrayBuffer>

Using the method and parameters specified in `algorithm` and the keying material provided by `key` , `subtle.decrypt()` attempts to decipher the provided `data` . If successful, the returned promise will be resolved with an <ArrayBuffer> containing the plaintext result.

The algorithms currently supported include:

- `'RSA-OAEP'`
- `'AES-CTR'`
- `'AES-CBC'`
- `'AES-GCM'`

`subtle.deriveBits(algorithm, baseKey, length)`

▶ History

- `algorithm` : <AlgorithmIdentifier> | <EcdhKeyDeriveParams> | <HkdfParams> | <Pbkdf2Params>
- `baseKey` : <CryptoKey>
- `length` : <number> | <null>
- Returns: <Promise> Fulfills with an <ArrayBuffer>

Using the method and parameters specified in `algorithm` and the keying material provided by `baseKey` , `subtle.deriveBits()` attempts to generate `length` bits.

The Node.js implementation requires that when `length` is a number it must be multiple of `8` .

When `length` is `null` the maximum number of bits for a given algorithm is generated. This is allowed for the `'ECDH'` , `'X25519'` , and `'X448'` algorithms.

If successful, the returned promise will be resolved with an <ArrayBuffer> containing the generated data.

The algorithms currently supported include:

- `'ECDH'`
- `'X25519'` [1]
- `'X448'` [1]
- `'HKDF'`

- `'PBKDF2'`

`subtle.deriveKey(algorithm, baseKey, derivedKeyAlgorithm, extractable, keyUsages)`

▶ History

- `algorithm` : <AlgorithmIdentifier> | <EcdhKeyDeriveParams> | <HkdfParams> | <Pbkdf2Params>
- `baseKey` : <CryptoKey>
- `derivedKeyAlgorithm` : <HmacKeyGenParams> | <AesKeyGenParams>
- `extractable` : <boolean>
- `keyUsages` : <string[]> See Key usages.
- Returns: <Promise> Fulfills with a <CryptoKey>

Using the method and parameters specified in `algorithm` , and the keying material provided by `baseKey` , `subtle.deriveKey()` attempts to generate a new <CryptoKey> based on the method and parameters in `derivedKeyAlgorithm` .

Calling `subtle.deriveKey()` is equivalent to calling `subtle.deriveBits()` to generate raw keying material, then passing the result into the `subtle.importKey()` method using the `deriveKeyAlgorithm` , `extractable` , and `keyUsages` parameters as input.

The algorithms currently supported include:

- `'ECDH'`
- `'X25519'` [1]
- `'X448'` [1]
- `'HKDF'`
- `'PBKDF2'`

`subtle.digest(algorithm, data)`

Added in: v15.0.0

- `algorithm` : <string> | <Object>
- `data` : <ArrayBuffer> | <TypedArray> | <DataView> | <Buffer>
- Returns: <Promise> Fulfills with an <ArrayBuffer>

Using the method identified by `algorithm` , `subtle.digest()` attempts to generate a digest of `data` . If successful, the returned promise is resolved with an <ArrayBuffer> containing the computed digest.

If `algorithm` is provided as a <string> , it must be one of:

- `'SHA-1'`
- `'SHA-256'`
- `'SHA-384'`
- `'SHA-512'`

If `algorithm` is provided as an <Object>, it must have a `name` property whose value is one of the above.

`subtle.encrypt(algorithm, key, data)`

Added in: v15.0.0

- `algorithm` : <RsaOaepParams> | <AesCtrParams> | <AesCbcParams> | <AesGcmParams>
- `key` : <CryptoKey>
- `data` : <ArrayBuffer> | <TypedArray> | <DataView> | <Buffer>
- Returns: <Promise> Fulfills with an <ArrayBuffer>

Using the method and parameters specified by `algorithm` and the keying material provided by `key`, `subtle.encrypt()` attempts to encipher `data`. If successful, the returned promise is resolved with an <ArrayBuffer> containing the encrypted result.

The algorithms currently supported include:

- `'RSA-OAEP'`
- `'AES-CTR'`
- `'AES-CBC'`
- `'AES-GCM'`

`subtle.exportKey(format, key)`

▶ History

- `format` : <string> Must be one of `'raw'`, `'pkcs8'`, `'spki'`, or `'jwk'`.
- `key` : <CryptoKey>
- Returns: <Promise> Fulfills with an <ArrayBuffer> | <Object>.

Exports the given key into the specified format, if supported.

If the <CryptoKey> is not extractable, the returned promise will reject.

When `format` is either `'pkcs8'` or `'spki'` and the export is successful, the returned promise will be resolved with an <ArrayBuffer> containing the exported key data.

When `format` is `'jwk'` and the export is successful, the returned promise will be resolved with a JavaScript object conforming to the JSON Web Key specification.

Key Type	'spki'	'pkcs8'	'jwk'	'raw'
'AES-CBC'			✓	✓
'AES-CTR'			✓	✓
'AES-GCM'			✓	✓
'AES-KW'			✓	✓
'ECDH'	✓	✓	✓	✓
'ECDSA'	✓	✓	✓	✓
'Ed25519' [1]	✓	✓	✓	✓
'Ed448' [1]	✓	✓	✓	✓
'HDKF'				
'HMAC'			✓	✓
'PBKDF2'				
'RSA-OAEP'	✓	✓	✓	
'RSA-PSS'	✓	✓	✓	
'RSASSA-PKCS1-v1_5'	✓	✓	✓	

```
subtle.generateKey(algorithm, extractable, keyUsages)
```

Added in: v15.0.0

- `algorithm` : <AlgorithmIdentifier> | <RsaHashedKeyGenParams> | <EcKeyGenParams> | <HmacKeyGenParams> | <AesKeyGenParams>
- `extractable` : <boolean>
- `keyUsages` : <string[]> See Key usages.
- Returns: <Promise> Fulfills with a <CryptoKey> | <CryptoKeyPair>

Using the method and parameters provided in `algorithm` , `subtle.generateKey()` attempts to generate new keying material. Depending the method used, the method may generate either a single <CryptoKey> or a <CryptoKeyPair> .

The <CryptoKeyPair> (public and private key) generating algorithms supported include:

- `'RSASSA-PKCS1-v1_5'`
- `'RSA-PSS'`
- `'RSA-OAEP'`
- `'ECDSA'`

- `'Ed25519'` [1]
- `'Ed448'` [1]
- `'ECDH'`
- `'X25519'` [1]
- `'X448'` [1]

The <CryptoKey> (secret key) generating algorithms supported include:

- `'HMAC'`
- `'AES-CTR'`
- `'AES-CBC'`
- `'AES-GCM'`
- `'AES-KW'`

`subtle.importKey(format, keyData, algorithm, extractable, keyUsages)`

▶ History

- `format` : <string> Must be one of `'raw'` , `'pkcs8'` , `'spki'` , or `'jwk'` .
- `keyData` : <ArrayBuffer> | <TypedArray> | <DataView> | <Buffer> | <Object>
- `algorithm` : <AlgorithmIdentifier> | <RsaHashedImportParams> | <EcKeyImportParams> | <HmacImportParams>
- `extractable` : <boolean>
- `keyUsages` : <string[]> See Key usages.
- Returns: <Promise> Fulfills with a <CryptoKey>

The `subtle.importKey()` method attempts to interpret the provided `keyData` as the given `format` to create a <CryptoKey> instance using the provided `algorithm` , `extractable` , and `keyUsages` arguments. If the import is successful, the returned promise will be resolved with the created <CryptoKey> .

If importing a `'PBKDF2'` key, `extractable` must be `false` .

The algorithms currently supported include:

Key Type	`'spki'`	`'pkcs8'`	`'jwk'`	`'raw'`
`'AES-CBC'`			✓	✓
`'AES-CTR'`			✓	✓
`'AES-GCM'`			✓	✓
`'AES-KW'`			✓	✓
`'ECDH'`	✓	✓	✓	✓
`'X25519'` [1]	✓	✓	✓	✓
`'X448'` [1]	✓	✓	✓	✓
`'ECDSA'`	✓	✓	✓	✓
`'Ed25519'` [1]	✓	✓	✓	✓
`'Ed448'` [1]	✓	✓	✓	✓
`'HDKF'`				✓
`'HMAC'`			✓	✓
`'PBKDF2'`				✓
`'RSA-OAEP'`	✓	✓	✓	
`'RSA-PSS'`	✓	✓	✓	
`'RSASSA-PKCS1-v1_5'`	✓	✓	✓	

```
subtle.sign(algorithm, key, data)
```

▶ History

- `algorithm` : <AlgorithmIdentifier> | <RsaPssParams> | <EcdsaParams> | <Ed448Params>
- `key` : <CryptoKey>
- `data` : <ArrayBuffer> | <TypedArray> | <DataView> | <Buffer>
- Returns: <Promise> Fulfills with an <ArrayBuffer>

Using the method and parameters given by `algorithm` and the keying material provided by `key` , `subtle.sign()` attempts to generate a cryptographic signature of `data` . If successful, the returned promise is resolved with an <ArrayBuffer> containing the generated signature.

The algorithms currently supported include:

- `'RSASSA-PKCS1-v1_5'`
- `'RSA-PSS'`

- `'ECDSA'`
- `'Ed25519'` [1]
- `'Ed448'` [1]
- `'HMAC'`

`subtle.unwrapKey(format, wrappedKey, unwrappingKey, unwrapAlgo, unwrappedKeyAlgo, extractable, keyUsages)`

Added in: v15.0.0

- `format` : <string> Must be one of `'raw'` , `'pkcs8'` , `'spki'` , or `'jwk'` .
- `wrappedKey` : <ArrayBuffer> | <TypedArray> | <DataView> | <Buffer>
- `unwrappingKey` : <CryptoKey>

- `unwrapAlgo` : <AlgorithmIdentifier> | <RsaOaepParams> | <AesCtrParams> | <AesCbcParams> | <AesGcmParams>
- `unwrappedKeyAlgo` : <AlgorithmIdentifier> | <RsaHashedImportParams> | <EcKeyImportParams> | <HmacImportParams>

- `extractable` : <boolean>
- `keyUsages` : <string[]> See Key usages.
- Returns: <Promise> Fulfills with a <CryptoKey>

In cryptography, "wrapping a key" refers to exporting and then encrypting the keying material. The `subtle.unwrapKey()` method attempts to decrypt a wrapped key and create a <CryptoKey> instance. It is equivalent to calling `subtle.decrypt()` first on the encrypted key data (using the `wrappedKey` , `unwrapAlgo` , and `unwrappingKey` arguments as input) then passing the results in to the `subtle.importKey()` method using the `unwrappedKeyAlgo` , `extractable` , and `keyUsages` arguments as inputs. If successful, the returned promise is resolved with a <CryptoKey> object.

The wrapping algorithms currently supported include:

- `'RSA-OAEP'`
- `'AES-CTR'`
- `'AES-CBC'`
- `'AES-GCM'`
- `'AES-KW'`

The unwrapped key algorithms supported include:

- `'RSASSA-PKCS1-v1_5'`
- `'RSA-PSS'`
- `'RSA-OAEP'`
- `'ECDSA'`
- `'Ed25519'` [1]

- 'Ed448' [1]
- 'ECDH'
- 'X25519' [1]
- 'X448' [1]
- 'HMAC'
- 'AES-CTR'
- 'AES-CBC'
- 'AES-GCM'
- 'AES-KW'

```
subtle.verify(algorithm, key, signature, data)
```

▶ History

- algorithm : <AlgorithmIdentifier> | <RsaPssParams> | <EcdsaParams> | <Ed448Params>
- key : <CryptoKey>
- signature : <ArrayBuffer> | <TypedArray> | <DataView> | <Buffer>
- data : <ArrayBuffer> | <TypedArray> | <DataView> | <Buffer>
- Returns: <Promise> Fulfills with a <boolean>

Using the method and parameters given in algorithm and the keying material provided by key , subtle.verify() attempts to verify that signature is a valid cryptographic signature of data . The returned promise is resolved with either true or false .

The algorithms currently supported include:

- 'RSASSA-PKCS1-v1_5'
- 'RSA-PSS'
- 'ECDSA'
- 'Ed25519' [1]
- 'Ed448' [1]
- 'HMAC'

```
subtle.wrapKey(format, key, wrappingKey, wrapAlgo)
```

Added in: v15.0.0

- format : <string> Must be one of 'raw' , 'pkcs8' , 'spki' , or 'jwk' .
- key : <CryptoKey>
- wrappingKey : <CryptoKey>
- wrapAlgo : <AlgorithmIdentifier> | <RsaOaepParams> | <AesCtrParams> | <AesCbcParams> | <AesGcmParams>
- Returns: <Promise> Fulfills with an <ArrayBuffer>

In cryptography, "wrapping a key" refers to exporting and then encrypting the keying material. The `subtle.wrapKey()` method exports the keying material into the format identified by `format`, then encrypts it using the method and parameters specified by `wrapAlgo` and the keying material provided by `wrappingKey`. It is the equivalent to calling `subtle.exportKey()` using `format` and `key` as the arguments, then passing the result to the `subtle.encrypt()` method using `wrappingKey` and `wrapAlgo` as inputs. If successful, the returned promise will be resolved with an <ArrayBuffer> containing the encrypted key data.

The wrapping algorithms currently supported include:

- `'RSA-OAEP'`
- `'AES-CTR'`
- `'AES-CBC'`
- `'AES-GCM'`
- `'AES-KW'`

Algorithm parameters

The algorithm parameter objects define the methods and parameters used by the various <SubtleCrypto> methods. While described here as "classes", they are simple JavaScript dictionary objects.

Class: `AlgorithmIdentifier`

`algorithmIdentifier.name`

Added in: v18.4.0, v16.17.0

- Type: <string>

Added in: v18.4.0, v16.17.0

Class: `AesCbcParams`

`aesCbcParams.iv`

Added in: v15.0.0

- Type: <ArrayBuffer> | <TypedArray> | <DataView> | <Buffer>

Added in: v15.0.0

Provides the initialization vector. It must be exactly 16-bytes in length and should be unpredictable and cryptographically random.

`aesCbcParams.name`

- Type: <string> Must be `'AES-CBC'`.

Added in: v15.0.0

Class: `AesCtrParams`

`aesCtrParams.counter`

Added in: v15.0.0

- Type: <ArrayBuffer> | <TypedArray> | <DataView> | <Buffer>

Added in: v15.0.0

The initial value of the counter block. This must be exactly 16 bytes long.

The `AES-CTR` method uses the rightmost `length` bits of the block as the counter and the remaining bits as the nonce.

`aesCtrParams.length`

Added in: v15.0.0

- Type: <number> The number of bits in the `aesCtrParams.counter` that are to be used as the counter.

`aesCtrParams.name`

Added in: v15.0.0

- Type: <string> Must be `'AES-CTR'`.

Class: `AesGcmParams`

`aesGcmParams.additionalData`

Added in: v15.0.0

Added in: v15.0.0

- Type: <ArrayBuffer> | <TypedArray> | <DataView> | <Buffer> | <undefined>

With the AES-GCM method, the `additionalData` is extra input that is not encrypted but is included in the authentication of the data. The use of `additionalData` is optional.

`aesGcmParams.iv`

Added in: v15.0.0

- Type: <ArrayBuffer> | <TypedArray> | <DataView> | <Buffer>

The initialization vector must be unique for every encryption operation using a given key.

Ideally, this is a deterministic 12-byte value that is computed in such a way that it is guaranteed to be unique across all invocations that use the same key. Alternatively, the initialization vector may consist of at least 12 cryptographically random bytes. For more information on constructing initialization vectors for AES-GCM, refer to Section 8 of NIST SP 800-38D.

`aesGcmParams.name`

Added in: v15.0.0

- Type: <string> Must be `'AES-GCM'`.

`aesGcmParams.tagLength`

Added in: v15.0.0

- Type: <number> The size in bits of the generated authentication tag. This values must be one of `32`, `64`, `96`, `104`, `112`, `120`, or `128`. **Default:** `128`.

Class: `AesKeyGenParams`

`aesKeyGenParams.length`

Added in: v15.0.0

- Type: <number>

The length of the AES key to be generated. This must be either `128`, `192`, or `256`.

Added in: v15.0.0

`aesKeyGenParams.name`

Added in: v15.0.0

- Type: <string> Must be one of `'AES-CBC'`, `'AES-CTR'`, `'AES-GCM'`, or `'AES-KW'`

Class: `EcdhKeyDeriveParams`

`ecdhKeyDeriveParams.name`

Added in: v15.0.0

- Type: <string> Must be `'ECDH'`, `'X25519'`, or `'X448'`.

Added in: v15.0.0

`ecdhKeyDeriveParams.public`

- Type: <CryptoKey>

Added in: v15.0.0

ECDH key derivation operates by taking as input one parties private key and another parties public key -- using both to generate a common shared secret. The `ecdhKeyDeriveParams.public` property is set to the other parties public key.

Class: `EcdsaParams`

`ecdsaParams.hash`

Added in: v15.0.0

- Type: <string> | <Object>

Added in: v15.0.0

If represented as a <string>, the value must be one of:

- `'SHA-1'`
- `'SHA-256'`
- `'SHA-384'`
- `'SHA-512'`

If represented as an <Object>, the object must have a `name` property whose value is one of the above listed values.

`ecdsaParams.name`

- Type: <string> Must be `'ECDSA'`.

Added in: v15.0.0

Class: `EcKeyGenParams`

`ecKeyGenParams.name`

Added in: v15.0.0

- Type: <string> Must be one of `'ECDSA'` or `'ECDH'`.

Added in: v15.0.0

`ecKeyGenParams.namedCurve`

Added in: v15.0.0

- Type: <string> Must be one of `'P-256'` , `'P-384'` , `'P-521'` .

Class: `EcKeyImportParams`

Added in: v15.0.0

`ecKeyImportParams.name`

Added in: v15.0.0

- Type: <string> Must be one of `'ECDSA'` or `'ECDH'` .

`ecKeyImportParams.namedCurve`

Added in: v15.0.0

- Type: <string> Must be one of `'P-256'` , `'P-384'` , `'P-521'` .

Class: `Ed448Params`

Added in: v15.0.0

`ed448Params.name`

Added in: v18.4.0, v16.17.0

- Type: <string> Must be `'Ed448'` .

`ed448Params.context`

Added in: v18.4.0, v16.17.0

- Type: <ArrayBuffer> | <TypedArray> | <DataView> | <Buffer> | <undefined>

The `context` member represents the optional context data to associate with the message. The Node.js Web Crypto API implementation only supports zero-length context which is equivalent to not providing context at all.

Class: `HkdfParams`

Added in: v15.0.0

`hkdfParams.hash`

Added in: v15.0.0

- Type: <string> | <Object>

If represented as a <string> , the value must be one of:

- `'SHA-1'`
- `'SHA-256'`
- `'SHA-384'`
- `'SHA-512'`

If represented as an <Object> , the object must have a `name` property whose value is one of the above listed values.

`hkdfParams.info`

Added in: v15.0.0

- Type: <ArrayBuffer> | <TypedArray> | <DataView> | <Buffer>

Provides application-specific contextual input to the HKDF algorithm. This can be zero-length but must be provided.

`hkdfParams.name`

Added in: v15.0.0

- Type: <string> Must be `'HKDF'` .

`hkdfParams.salt`

Added in: v15.0.0

- Type: <ArrayBuffer> | <TypedArray> | <DataView> | <Buffer>

The salt value significantly improves the strength of the HKDF algorithm. It should be random or pseudorandom and should be the same length as the output of the digest function (for instance, if using `'SHA-256'` as the digest, the salt should be 256-bits of random data).

Class: `HmacImportParams`

Added in: v15.0.0

`hmacImportParams.hash`

Added in: v15.0.0

- Type: <string> | <Object>

If represented as a <string> , the value must be one of:

- `'SHA-1'`
- `'SHA-256'`
- `'SHA-384'`
- `'SHA-512'`

If represented as an <Object> , the object must have a `name` property whose value is one of the above listed values.

`hmacImportParams.length`

Added in: v15.0.0

- Type: <number>

The optional number of bits in the HMAC key. This is optional and should be omitted for most cases.

`hmacImportParams.name`

Added in: v15.0.0

- Type: <string> Must be `'HMAC'` .

Class: `HmacKeyGenParams`

Added in: v15.0.0

`hmacKeyGenParams.hash`

Added in: v15.0.0

- Type: <string> | <Object>

If represented as a <string>, the value must be one of:

- `'SHA-1'`
- `'SHA-256'`
- `'SHA-384'`
- `'SHA-512'`

If represented as an <Object>, the object must have a `name` property whose value is one of the above listed values.

`hmacKeyGenParams.length`

Added in: v15.0.0

- Type: <number>

The number of bits to generate for the HMAC key. If omitted, the length will be determined by the hash algorithm used. This is optional and should be omitted for most cases.

`hmacKeyGenParams.name`

Added in: v15.0.0

- Type: <string> Must be `'HMAC'`.

Class: `Pbkdf2Params`

Added in: v15.0.0

`pbkdb2Params.hash`

Added in: v15.0.0

- Type: <string> | <Object>

If represented as a <string>, the value must be one of:

- `'SHA-1'`
- `'SHA-256'`
- `'SHA-384'`
- `'SHA-512'`

If represented as an <Object>, the object must have a `name` property whose value is one of the above listed values.

`pbkdf2Params.iterations`

Added in: v15.0.0

- Type: <number>

The number of iterations the PBKDF2 algorithm should make when deriving bits.

`pbkdf2Params.name`

Added in: v15.0.0

- Type: <string> Must be `'PBKDF2'`.

`pbkdf2Params.salt`

Added in: v15.0.0

- Type: <ArrayBuffer> | <TypedArray> | <DataView> | <Buffer>

Should be at least 16 random or pseudorandom bytes.

Class: `RsaHashedImportParams`

Added in: v15.0.0

`rsaHashedImportParams.hash`

Added in: v15.0.0

- Type: <string> | <Object>

If represented as a <string>, the value must be one of:

- `'SHA-1'`
- `'SHA-256'`
- `'SHA-384'`
- `'SHA-512'`

If represented as an <Object>, the object must have a `name` property whose value is one of the above listed values.

`rsaHashedImportParams.name`

Added in: v15.0.0

- Type: <string> Must be one of `'RSASSA-PKCS1-v1_5'`, `'RSA-PSS'`, or `'RSA-OAEP'`.

Class: `RsaHashedKeyGenParams`

Added in: v15.0.0

`rsaHashedKeyGenParams.hash`

Added in: v15.0.0

- Type: <string> | <Object>

If represented as a <string>, the value must be one of:

- `'SHA-1'`
- `'SHA-256'`
- `'SHA-384'`
- `'SHA-512'`

If represented as an <Object>, the object must have a `name` property whose value is one of the above listed values.

`rsaHashedKeyGenParams.modulusLength`

Added in: v15.0.0

- Type: <number>

The length in bits of the RSA modulus. As a best practice, this should be at least `2048`.

`rsaHashedKeyGenParams.name`

Added in: v15.0.0

- Type: <string> Must be one of `'RSASSA-PKCS1-v1_5'` , `'RSA-PSS'` , or `'RSA-OAEP'` .

`rsaHashedKeyGenParams.publicExponent`

Added in: v15.0.0

- Type: <Uint8Array>

The RSA public exponent. This must be a <Uint8Array> containing a big-endian, unsigned integer that must fit within 32-bits. The <Uint8Array> may contain an arbitrary number of leading zero-bits. The value must be a prime number. Unless there is reason to use a different value, use `new Uint8Array([1, 0, 1])` (65537) as the public exponent.

Class: `RsaOaepParams`

Added in: v15.0.0

`rsaOaepParams.label`

Added in: v15.0.0

- Type: <ArrayBuffer> | <TypedArray> | <DataView> | <Buffer>

An additional collection of bytes that will not be encrypted, but will be bound to the generated ciphertext.

The `rsaOaepParams.label` parameter is optional.

`rsaOaepParams.name`

Added in: v15.0.0

- Type: <string> must be `'RSA-OAEP'` .

Class: `RsaPssParams`

Added in: v15.0.0

`rsaPssParams.name`

Added in: v15.0.0

- Type: <string> Must be `'RSA-PSS'` .

`rsaPssParams.saltLength`

Added in: v15.0.0

- Type: <number>

The length (in bytes) of the random salt to use.

Footnotes

1. An experimental implementation of Secure Curves in the Web Cryptography API as of 30 August 2023 ↩ ↩2 ↩3 ↩4 ↩5 ↩6 ↩7 ↩8 ↩9 ↩10 ↩11 ↩12 ↩13 ↩14 ↩15 ↩16 ↩17 ↩18 ↩19 ↩20 ↩21 ↩22 ↩23 ↩24 ↩25 ↩26 ↩27 ↩28 ↩29 ↩30