**BSNC Javascript API v1.0.0 Document**

This is a BSNC Javascript API Document for HerIOT web & mobile service.

CreateEncryptKeypairs(password)

: Create compressed & uncompressed public key and encrypted private key pairs using password.

Parameters

|  |  |  |
| --- | --- | --- |
| Name | Type | Description |
| password | String | Password for creating encryption private key |

Returns

|  |  |  |
| --- | --- | --- |
| Name | Type | Description |
| keypairs | Object | Return an key pairs object |
| Return example | | |
| {  compressedPubkey: [value],  uncompressedPubkey: [value],  encryptPrivkey: [value]  } | | |

CreateKeypairs()

: Create compressed & uncompressed public key and private key pairs

Parameters

|  |  |  |
| --- | --- | --- |
| Name | Type | Description |
| Null |  |  |

Returns

|  |  |  |
| --- | --- | --- |
| Name | Type | Description |
| Keypairs | Object | Return an key pairs object |
| Return example | | |
| {  compressedPubkey: [value],  uncompressedPubkey: [value],  privatekey: [value]  } | | |

Sign(encryptedPrivKey, message)

: Sign to message using encrypted private key.

Parameters

|  |  |  |
| --- | --- | --- |
| Name | Type | Description |
| encryptedPrivKey | String | Encrypted private key for sign message |
| message | String | Message to sign |

Returns

|  |  |  |
| --- | --- | --- |
| Name | Type | Description |
| sigExport | Promise<buffer> | A promise that resolves with the signature and rejects on bad key or message |
| Return example | | |
|  | | |

Verify(uncompressedPubKey, message, signedData)

: Verify signed Data using uncompressed public key with message

Parameters

|  |  |  |
| --- | --- | --- |
| Name | Type | Description |
| uncompressedPubkey | String | Uncompressesed public key to verify signed data |
| message | String | Message that signed to private key |
| signedData | String | Singed Data using private key |

Returns

|  |  |  |
| --- | --- | --- |
| Name | Type | Description |
| verifyExport | Promise<buffer> | A promise that resolves on correct signature and rejects on bad key or signature |
| Return example | | |
|  | | |