
eth-account Documentation

Release 0.8.0

The Ethereum Foundation

Mar 22, 2023

Contents

1	Contents	3
1.1	eth_account	3
1.1.1	Account	3
1.1.2	SignedTransaction & SignedMessage	12
1.1.3	Messages	13
1.2	Signers	15
1.2.1	Local Signer	16
1.2.2	Abstract Signer	17
1.3	Release Notes	18
1.3.1	eth-account v0.8.0 (2022-12-15)	18
1.3.2	eth-account v0.7.0 (2022-08-17)	18
1.3.3	eth-account v0.6.1 (2022-02-24)	19
1.3.4	eth-account v0.6.0 (2022-01-20)	19
1.3.5	eth-account v0.5.9 (2022-08-04)	19
1.3.6	eth-account v0.5.8 (2022-06-06)	19
1.3.7	eth-account v0.5.7 (2022-01-27)	20
1.3.8	eth-account v0.5.6 (2021-09-22)	20
1.3.9	eth-account v0.5.5 (2021-07-21)	20
1.3.10	v0.5.3 (2020-08-31)	21
1.3.11	v0.5.2 (2020-04-30)	21
1.3.12	v0.5.1	21
1.3.13	v0.5.0	21
1.3.14	v0.4.0	21
1.3.15	v0.3.0	22
1.3.16	v0.2.3	22
1.3.17	v0.2.2	22
1.3.18	v0.2.1	22
1.3.19	v0.2.0 (stable)	22
1.3.20	v0.2.0-alpha.0	22
1.3.21	v0.1.0-alpha.2	23
1.3.22	v0.1.0-alpha.1	23
2	Indices and tables	25
	Python Module Index	27
	Index	29

Sign Ethereum transactions and messages with local private keys

1.1 eth_account

1.1.1 Account

class `eth_account.account.Account`

The primary entry point for working with Ethereum private keys.

It does **not** require a connection to an Ethereum node.

create (*extra_entropy*=")

Creates a new private key, and returns it as a `LocalAccount`.

Parameters `extra_entropy` (*str* or *bytes* or *int*) – Add extra randomness to whatever randomness your OS can provide

Returns an object with private key and convenience methods

```
>>> from eth_account import Account
>>> acct = Account.create('KEYSMASH FJAFJKLDSKF7JKFDJ 1530')
>>> acct.address
'0x5ce9454909639D2D17A3F753ce7d93fa0b9aB12E'
>>> acct.key
HexBytes('0x8676e9a8c86c8921e922e61e0bb6e9e9689aad4c99082620610b00140e5f21b8')

# These methods are also available: sign_message(), sign_transaction(),
# encrypt().
# They correspond to the same-named methods in Account.*
# but without the private key argument
```

create_with_mnemonic (*passphrase*: *str* = "", *num_words*: *int* = 12, *language*: *str* = 'english', *account_path*: *str* = "m/44'/60'/0'/0/0") → `Tuple[eth_account.signers.local.LocalAccount, str]`

Create a new private key and related mnemonic.

Caution: This feature is experimental, unaudited, and likely to change soon

Creates a new private key, and returns it as a `LocalAccount`, alongside the mnemonic that can be used to regenerate it using any BIP39-compatible wallet.

Parameters

- **passphrase** (*str*) – Extra passphrase to encrypt the seed phrase
- **num_words** (*int*) – Number of words to use with seed phrase. Default is 12 words. Must be one of [12, 15, 18, 21, 24].
- **language** (*str*) – Language to use for BIP39 mnemonic seed phrase.
- **account_path** (*str*) – Specify an alternate HD path for deriving the seed using BIP32 HD wallet key derivation.

Returns A tuple consisting of an object with private key and convenience methods, and the mnemonic seed phrase that can be used to restore the account.

Return type (*LocalAccount*, *str*)

```
>>> from eth_account import Account
>>> Account.enable_unaudited_hdwallet_features()
>>> acct, mnemonic = Account.create_with_mnemonic()
>>> acct.address
'0x5ce9454909639D2D17A3F753ce7d93fa0b9aB12E'
>>> acct == Account.from_mnemonic(mnemonic)
True

# These methods are also available:
# sign_message(), sign_transaction(), encrypt()
# They correspond to the same-named methods in Account.*
# but without the private key argument
```

static decrypt (*keyfile_json*, *password*)

Decrypts a private key.

The key may have been encrypted using an Ethereum client or `encrypt()`.

Parameters

- **keyfile_json** (*dict* or *str*) – The encrypted key
- **password** (*str*) – The password that was used to encrypt the key

Returns the raw private key

Return type `HexBytes`

```
>>> encrypted = {
...   'address': '5ce9454909639d2d17a3f753ce7d93fa0b9ab12e',
...   'crypto': {'cipher': 'aes-128-ctr',
...   'cipherparams': {'iv': '482ef54775b0cc59f25717711286f5c8'},
...   'ciphertext':
↪ 'cb636716a9fd46adbb31832d964df2082536edd5399a3393327dc89b0193a2be', #
↪ noqa: E501
...   'kdf': 'scrypt',
...   'kdfparams': {},
...   'kdfparams': {'dklen': 32,
...   'n': 262144,
```

(continues on next page)

(continued from previous page)

```

...         'p': 8,
...         'r': 1,
...         'salt': 'd3c9a9945000fcb6c9df0f854266d573'},
...     'mac': '4f626ec5e7fea391b2229348a65bfef532c2a4e8372c0a6a814505a350a7689d
↪'}, # noqa: E501
...     'id': 'b812f3f9-78cc-462a-9e89-74418aa27cb0',
...     'version': 3}
>>> Account.decrypt(encrypted, 'password')
HexBytes('0xb25c7db31feed9122727bf0939dc769a96564b2de4c4726d035b36ecf1e5b364')

```

classmethod enable_unaudited_hdwallet_features()

Use this flag to enable unaudited HD Wallet features.

classmethod encrypt (*private_key, password, kdf=None, iterations=None*)

Creates a dictionary with an encrypted version of your private key. To import this keyfile into Ethereum clients like geth and parity: encode this dictionary with `json.dumps()` and save it to disk where your client keeps key files.

Parameters

- **private_key** (hex str, bytes, int or `eth_keys.datatypes.PrivateKey`) – The raw private key
- **password** (*str*) – The password which you will need to unlock the account in your client
- **kdf** (*str*) – The key derivation function to use when encrypting your private key
- **iterations** (*int*) – The work factor for the key derivation function

Returns The data to use in your encrypted file

Return type `dict`

If `kdf` is not set, the default key derivation function falls back to the environment variable `ETH_ACCOUNT_KDF`. If that is not set, then ‘scrypt’ will be used as the default.

```

>>> from pprint import pprint
>>> encrypted = Account.encrypt(
...     0xb25c7db31feed9122727bf0939dc769a96564b2de4c4726d035b36ecf1e5b364,
...     'password'
... )
>>> pprint(encrypted)
{'address': '5ce9454909639d2d17a3f753ce7d93fa0b9ab12e',
 'crypto': {'cipher': 'aes-128-ctr',
            'cipherparams': {'iv': '...'},
            'ciphertext': '...',
            'kdf': 'scrypt',
            'kdfparams': {'dklen': 32,
                          'n': 262144,
                          'p': 8,
                          'r': 1,
                          'salt': '...'},
            'mac': '...'},
 'id': '...',
 'version': 3}

>>> with open('my-keyfile', 'w') as f:
...     f.write(json.dumps(encrypted))

```

from_key (*private_key*)

Returns a convenient object for working with the given private key.

Parameters **private_key** (hex str, bytes, int or `eth_keys.datatypes.PrivateKey`)

– The raw private key

Returns object with methods for signing and encrypting

Return type *LocalAccount*

```
>>> acct = Account.from_key(
... 0xb25c7db31feed9122727bf0939dc769a96564b2de4c4726d035b36ecf1e5b364)
>>> acct.address
'0x5ce9454909639D2D17A3F753ce7d93fa0b9aB12E'
>>> acct.key
HexBytes('0xb25c7db31feed9122727bf0939dc769a96564b2de4c4726d035b36ecf1e5b364')

# These methods are also available: sign_message(), sign_transaction(),
# encrypt(). They correspond to the same-named methods in Account.*
# but without the private key argument
```

from_mnemonic (*mnemonic: str, passphrase: str = "", account_path: str = "m/44'/60'/0'/0/0"*) →

`eth_account.signers.local.LocalAccount`

Generate an account from a mnemonic.

Caution: This feature is experimental, unaudited, and likely to change soon

Parameters

- **mnemonic** (*str*) – space-separated list of BIP39 mnemonic seed words
- **passphrase** (*str*) – Optional passphrase used to encrypt the mnemonic
- **account_path** (*str*) – Specify an alternate HD path for deriving the seed using BIP32 HD wallet key derivation.

Returns object with methods for signing and encrypting

Return type *LocalAccount*

```
>>> from eth_account import Account
>>> Account.enable_unaudited_hdwallet_features()
>>> acct = Account.from_mnemonic(
... "coral allow abandon recipe top tray caught video climb similar "
... "prepare bracket antenna rubber announce gauge volume "
... "hub hood burden skill immense add acid")
>>> acct.address
'0x9AdA5dAD14d925f4df1378409731a9B71Bc8569d'

# These methods are also available: sign_message(), sign_transaction(),
# encrypt(). They correspond to the same-named methods in Account.*
# but without the private key argument
```

Or, generate multiple accounts from a mnemonic.

```
>>> from eth_account import Account
>>> Account.enable_unaudited_hdwallet_features()
>>> iterator = 0
```

(continues on next page)

(continued from previous page)

```
>>> for i in range(10):
...     acct = Account.from_mnemonic(
...         "health embark april buyer eternal leopard "
...         "want before nominee head thing tackle",
...         account_path=f"m/44'/60'/0'/0/{iterator}")
...     iterator = iterator + 1
...     acct.address
'0x61Cc15522D06983Ac7aADe23f9d5433d38e78195'
'0x1240460F6E370f28079E5F9B52f9DcB759F051b7'
'0xd30dC9f996539826C646Eb48bb45F6ee1D1474af'
'0x47e64beb58c9A469c5eD086aD231940676b44e7C'
'0x6D39032ffEF9987988a069F52EF4d95D0770555'
'0x3836A6530D1889853b047799Ecd8827255072e77'
'0xed5490dEfF8d8FfAe45cb4066C3daC7C6BFF6a22'
'0xf04F9Ff322799253bcC6B12762AD127570a092c5'
'0x900F7fa9fbe85BB25b6cdB94Da24D807f7feb213'
'0xa248e118b0D19010387b1B768686cd9B473FA137'
```

Caution: For the love of Bob please do not use this mnemonic, it is for testing purposes only.

recover_message (*signable_message*: *eth_account.messages.SignableMessage*, *vrs*: *Optional[Tuple[VRS, VRS, VRS]] = None*, *signature*: *bytes = None*) → *NewType.<locals>.new_type*

Get the address of the account that signed the given message. You must specify exactly one of: *vrs* or *signature*

Parameters

- **signable_message** – the message that was signed
- **vrs** (*tuple(v, r, s)*, each element is hex str, bytes or int) – the three pieces generated by an elliptic curve signature
- **signature** (*hex str or bytes or int*) – signature bytes concatenated as r+s+v

Returns address of signer, hex-encoded & checksummed

Return type *str*

```
>>> from eth_account.messages import encode_defunct
>>> from eth_account import Account
>>> message = encode_defunct(text="ISF")
>>> vrs = (
...     28,
...     '0xe6ca9bba58c88611fad66a6ce8f996908195593807c4b38bd528d2cff09d4eb3',
...     '0x3e5bfbbf4d3e39b1a2fd816a7680c19ebabaf3a141b239934ad43cb33fcec8ce')
>>> Account.recover_message(message, vrs=vrs)
'0x5ce9454909639D2D17A3F753ce7d93fa0b9aB12E'

# All of these recover calls are equivalent:

# variations on vrs
>>> vrs = (
...     '0x1c',
```

(continues on next page)

(continued from previous page)

```

...     '0xe6ca9bba58c88611fad66a6ce8f996908195593807c4b38bd528d2cff09d4eb3',
...     '0x3e5bfbbf4d3e39b1a2fd816a7680c19ebdaf3a141b239934ad43cb33fcec8ce')
>>> Account.recover_message(message, vrs=vrs)
'0x5ce9454909639D2D17A3F753ce7d93fa0b9aB12E'

>>> # Caution about this approach: likely problems if there are leading 0s
>>> vrs = (
...     0x1c,
...     0xe6ca9bba58c88611fad66a6ce8f996908195593807c4b38bd528d2cff09d4eb3,
...     0x3e5bfbbf4d3e39b1a2fd816a7680c19ebdaf3a141b239934ad43cb33fcec8ce)
>>> Account.recover_message(message, vrs=vrs)
'0x5ce9454909639D2D17A3F753ce7d93fa0b9aB12E'

>>> vrs = (
...     b'\x1c',
...     b
↳ '\xe6\xca\x9b\xba\x86\x11\xfa\xd6j1\xe8\xf9\x96\x90\x81\x95Y8\x07\x04\xb3\x8b\xd5(\xc
↳ ', # noqa: E501
...     b'>[\xfb\xbfM>
↳ 9\xb1\xa2\xfd\x81jv\x80\xc1\x9e\xbe\xba\xfb\xa1\xb29\x93J\xd4<\xb3?
↳ \xc8\xce') # noqa: E501
>>> Account.recover_message(message, vrs=vrs)
'0x5ce9454909639D2D17A3F753ce7d93fa0b9aB12E'

# variations on signature
>>> signature =
↳ '0xe6ca9bba58c88611fad66a6ce8f996908195593807c4b38bd528d2cff09d4eb33e5bfbbf4d3e39b1a2fd816a
↳ ' # noqa: E501
>>> Account.recover_message(message, signature=signature)
'0x5ce9454909639D2D17A3F753ce7d93fa0b9aB12E'
>>> signature = b
↳ '\xe6\xca\x9b\xba\x86\x11\xfa\xd6j1\xe8\xf9\x96\x90\x81\x95Y8\x07\x04\xb3\x8b\xd5(\xc
↳ [\xfb\xbfM>9\xb1\xa2\xfd\x81jv\x80\xc1\x9e\xbe\xba\xfb\xa1\xb29\x93J\xd4
↳ <\xb3?\xc8\xce\x1c' # noqa: E501
>>> Account.recover_message(message, signature=signature)
'0x5ce9454909639D2D17A3F753ce7d93fa0b9aB12E'
>>> # Caution about this approach: likely problems if there are leading 0s
>>> signature =
↳ 0xe6ca9bba58c88611fad66a6ce8f996908195593807c4b38bd528d2cff09d4eb33e5bfbbf4d3e39b1a2fd816a
↳ # noqa: E501
>>> Account.recover_message(message, signature=signature)
'0x5ce9454909639D2D17A3F753ce7d93fa0b9aB12E'

```

recover_transaction (*serialized_transaction*)

Get the address of the account that signed this transaction.

Parameters *serialized_transaction* (*hex str*, *bytes* or *int*) – the complete signed transaction

Returns address of signer, hex-encoded & checksummed

Return type *str*

```

>>> raw_transaction =
↳ '0xf86a8086d55698372431831e848094f0109fc8df283027b6285cc889f5aa624eac1f55843b9aca008025a00
↳ ' # noqa: E501
>>> Account.recover_transaction(raw_transaction)
'0x2c7536E3605D9C16a7a3D7b1898e529396a65c23'

```

set_key_backend (*backend*)

Change the backend used by the underlying eth-keys library.

(The default is fine for most users)

Parameters **backend** – any backend that works in `eth_keys.KeyApi(backend)`

signHash (*message_hash*, *private_key*)

Sign the provided hash.

Warning: *Never* sign a hash that you didn't generate, it can be an arbitrary transaction. For example, it might send all of your account's ether to an attacker. Instead, prefer `sign_message()`, which cannot accidentally sign a transaction.

Caution: Deprecated for `sign_message()`. This method will be removed in v0.6

Parameters

- **message_hash** (*hex str*, *bytes* or *int*) – the 32-byte message hash to be signed
- **private_key** (*hex str*, *bytes*, *int* or `eth_keys.datatypes.PrivateKey`) – the key to sign the message with

Returns Various details about the signature - most importantly the fields: v, r, and s

Return type *SignedMessage*

sign_message (*signable_message*: `eth_account.messages.SignableMessage`, *private_key*: `Union[bytes, NewType.<locals>.new_type, int, eth_keys.datatypes.PrivateKey]`)
→ `eth_account.datastructures.SignedMessage`

Sign the provided message.

This API supports any messaging format that will encode to EIP-191 messages.

If you would like historical compatibility with `w3.eth.sign()` you can use `encode_defunct()`.

Other options are the “validator”, or “structured data” standards. (Both of these are in *DRAFT* status currently, so be aware that the implementation is not guaranteed to be stable). You can import all supported message encoders in `eth_account.messages`.

Parameters

- **signable_message** – the encoded message for signing
- **private_key** (*hex str*, *bytes*, *int* or `eth_keys.datatypes.PrivateKey`) – the key to sign the message with

Returns Various details about the signature - most importantly the fields: v, r, and s

Return type *SignedMessage*

```
>>> msg = "ISF"
>>> from eth_account.messages import encode_defunct
>>> msghash = encode_defunct(text=msg)
>>> msghash
SignableMessage(version=b'E',
header=b'thereum Signed Message:\n6',
```

(continues on next page)

(continued from previous page)

```

body=b'I\xe2\x99\xa5SF')
>>> # If you're curious about the internal fields of SignableMessage, take a
↳look at EIP-191, linked above # noqa: E501
>>> key = "0xb25c7db31feed9122727bf0939dc769a96564b2de4c4726d035b36ecf1e5b364"
>>> Account.sign_message(msghash, key)
SignedMessage(messageHash=HexBytes(
↳'0x1476abb745d423bf09273f1afd887d951181d25adc66c4834a70491911b7f750'),
↳
↳r=104389933075820307925104709181714897380569894203213074526835978196648170704563,
↳
↳s=28205917190874851400050446352651915501321657673772411533993420917949420456142,
↳
↳v=28,
signature=HexBytes(
↳'0xe6ca9bba58c88611fad66a6ce8f996908195593807c4b38bd528d2cff09d4eb33e5bfbbf4d3e39b1a2fd816
↳'))

```

sign_transaction (*transaction_dict*, *private_key*)

Sign a transaction using a local private key.

It produces signature details and the hex-encoded transaction suitable for broadcast using `w3.eth.sendRawTransaction()`.

To create the transaction dict that calls a contract, use contract object: `my_contract.functions.my_function().buildTransaction()`

Note: For non-legacy (typed) transactions, if the transaction type is not explicitly provided, it may be determined from the transaction parameters of a well-formed transaction. See below for examples on how to sign with different transaction types.

Parameters

- **transaction_dict** (*dict*) – the transaction with available keys, depending on the type of transaction: `nonce`, `chainId`, `to`, `data`, `value`, `gas`, `gasPrice`, `type`, `accessList`, `maxFeePerGas`, and `maxPriorityFeePerGas`
- **private_key** (hex str, bytes, int or `eth_keys.datatypes.PrivateKey`) – the private key to sign the data with

Returns Various details about the signature - most importantly the fields: `v`, `r`, and `s`

Return type `AttributeDict`

```

>>> # EIP-1559 dynamic fee transaction (more efficient and preferred over
↳legacy txn) # noqa: E501
>>> dynamic_fee_transaction = {
    "type": 2, # optional - can be implicitly determined based on max
↳fee params # noqa: E501
    "gas": 100000,
    "maxFeePerGas": 2000000000,
    "maxPriorityFeePerGas": 2000000000,
    "data": "0x616263646566",
    "nonce": 34,
    "to": "0x09616C3d61b3331fc4109a9E41a8BDB7d9776609",
    "value": "0x5af3107a4000",
    "accessList": ( # optional
        {
            "address": "0x0000000000000000000000000000000000000001",

```

(continues on next page)

(continued from previous page)

```

        "storageKeys": (
            ↪ "0x0100000000000000000000000000000000000000000000000000000000000000", # ↪
            ↪ noqa: E501
        )
    },
    ↪ ),
    ↪ "chainId": 1900,
    ↪ }
>>> key = '0x4c0883a69102937d6231471b5dbb6204fe5129617082792ae468d01a3f362318'
>>> signed = Account.sign_transaction(dynamic_fee_transaction, key)
{'hash': HexBytes(
    ↪ '0x126431f2a7fda003aada7c2ce52b0ce3cbdbb1896230d3333b9eea24f42d15b0'),
    ↪
    ↪ 'r': ↪
    ↪ 110093478023675319011132687961420618950720745285952062287904334878381994888509,
    ↪
    ↪ 'rawTransaction': HexBytes(
    ↪ '0x02f8b282076c2284773594008477359400830186a09409616c3d61b3331fc4109a9e41a8bdb7d9776609865
    ↪ '),
    ↪ 's': ↪
    ↪ 33674551144139401179914073499472892825822542092106065756005379322302694600392,
    ↪
    ↪ 'v': 0}
>>> w3.eth.sendRawTransaction(signed.rawTransaction)

```

```

>>> # legacy transaction (less efficient than EIP-1559 dynamic fee txn)
>>> legacy_transaction = {
    ↪ # Note that the address must be in checksum format or native bytes:
    ↪ 'to': '0xF0109fC8DF283027b6285cc889F5aA624EaC1F55',
    ↪ 'value': 1000000000,
    ↪ 'gas': 2000000,
    ↪ 'gasPrice': 234567897654321,
    ↪ 'nonce': 0,
    ↪ 'chainId': 1
    ↪ }
>>> key = '0x4c0883a69102937d6231471b5dbb6204fe5129617082792ae468d01a3f362318'
>>> signed = Account.sign_transaction(legacy_transaction, key)
{'hash': HexBytes(
    ↪ '0x6893a6ee8df79b0f5d64a180cd1ef35d030f3e296a5361cf04d02ce720d32ec5'),
    ↪ 'r': ↪
    ↪ 4487286261793418179817841024889747115779324305375823110249149479905075174044,
    ↪
    ↪ 'rawTransaction': HexBytes(
    ↪ '0xf86a8086d55698372431831e848094f0109fc8df283027b6285cc889f5aa624eac1f55843b9aca008025a00
    ↪ '),
    ↪ 's': ↪
    ↪ 30785525769477805655994251009256770582792548537338581640010273753578382951464,
    ↪
    ↪ 'v': 37}
>>> w3.eth.sendRawTransaction(signed.rawTransaction)

```

```

>>> access_list_transaction = {
    ↪ "type": 1, # optional - can be implicitly determined based on
    ↪ 'accessList' and 'gasPrice' params # noqa: E501

```

(continues on next page)

(continued from previous page)

```

        "gas": 100000,
        "gasPrice": 1000000000,
        "data": "0x616263646566",
        "nonce": 34,
        "to": "0x09616C3d61b3331fc4109a9E41a8BDB7d9776609",
        "value": "0x5af3107a4000",
        "accessList": (
            {
                "address": "0x0000000000000000000000000000000000000001",
                "storageKeys": (
                    ↪ "0x0100000000000000000000000000000000000000000000000000000000000000", # ↪
                    ↪ noqa: E501
                )
            },
        ),
        "chainId": 1900,
    }
>>> key = '0x4c0883a69102937d6231471b5dbb6204fe5129617082792ae468d01a3f362318'
>>> signed = Account.sign_transaction(access_list_transaction, key)
{'hash': HexBytes(
    ↪ '0x2864ca20a74ca5e044067ad4139a22ff5a0853434f5f1dc00108f24ef5f1f783'),
 'r': ↪
    ↪ 105940705063391628472351883894091935317142890114440570831409400676736873197702,
    ↪
    'rawTransaction': HexBytes(
    ↪ '0x01f8ad82076c22843b9aca00830186a09409616c3d61b3331fc4109a9e41a8bdb7d9776609865af3107a400
    ↪ '), # noqa: E501
 's': ↪
    ↪ 37050226636175381535892585331727388340134760347943439553552848647212419749796,
    ↪
    'v': 0}
>>> w3.eth.sendRawTransaction(signed.rawTransaction)

```

See [Signers](#) for alternative signers.

1.1.2 SignedTransaction & SignedMessage

class `eth_account.datastructures.SignedMessage` (*messageHash, r, s, v, signature*)

Bases: `tuple`

messageHash

Alias for field number 0

r

Alias for field number 1

s

Alias for field number 2

signature

Alias for field number 4

v

Alias for field number 3

class `eth_account.datastructures.SignedTransaction` (*rawTransaction, hash, r, s, v*)

Bases: `tuple`

hash
Alias for field number 1

r
Alias for field number 2

rawTransaction
Alias for field number 0

s
Alias for field number 3

v
Alias for field number 4

1.1.3 Messages

class `eth_account.messages.SignableMessage`

Bases: `tuple`

A message compatible with EIP-191 that is ready to be signed.

The properties are components of an EIP-191 signable message. Other message formats can be encoded into this format for easy signing. This data structure doesn't need to know about the original message format. For example, you can think of EIP-712 as compiling down to an EIP-191 message.

In typical usage, you should never need to create these by hand. Instead, use one of the available `encode_*` methods in this module, like:

- `encode_structured_data()`
- `encode_intended_validator()`
- `encode_defunct()`

body
Alias for field number 2

header
Alias for field number 1

version
Alias for field number 0

`eth_account.messages.defunct_hash_message` (*primitive: bytes = None, *, hexstr: str = None, text: str = None*) → `hexbytes.main.HexBytes`

Convert the provided message into a message hash, to be signed.

Caution: Intended for use with the deprecated `eth_account.account.Account.signHash()`. This is for backwards compatibility only. All new implementations should use `encode_defunct()` instead.

Parameters

- **primitive** (*bytes* or *int*) – the binary message to be signed
- **hexstr** (*str*) – the message encoded as hex
- **text** (*str*) – the message as a series of unicode characters (a normal Py3 str)

Returns The hash of the message, after adding the prefix

`eth_account.messages.encode_defunct` (*primitive: bytes = None, *, hexstr: str = None, text: str = None*) → `eth_account.messages.SignableMessage`

Encode a message for signing, using an old, unrecommended approach.

Only use this method if you must have compatibility with `w3.eth.sign()`.

EIP-191 defines this as “version E”.

Supply exactly one of the three arguments: bytes, a hex string, or a unicode string.

Parameters

- **primitive** (*bytes* or *int*) – the binary message to be signed
- **hexstr** (*str*) – the message encoded as hex
- **text** (*str*) – the message as a series of unicode characters (a normal Py3 str)

Returns The EIP-191 encoded message, ready for signing

```
>>> from eth_account.messages import encode_defunct
>>> from eth_utils.curried import to_hex, to_bytes

>>> message_text = "ISF"
>>> encode_defunct(text=message_text)
SignableMessage(version=b'E',
                  header=b'thereum Signed Message:\n6',
                  body=b'I\xe2\x99\xa5SF')

These four also produce the same hash:
>>> encode_defunct(to_bytes(text=message_text))
SignableMessage(version=b'E',
                  header=b'thereum Signed Message:\n6',
                  body=b'I\xe2\x99\xa5SF')

>>> encode_defunct(bytes(message_text, encoding='utf-8'))
SignableMessage(version=b'E',
                  header=b'thereum Signed Message:\n6',
                  body=b'I\xe2\x99\xa5SF')

>>> to_hex(text=message_text)
'0x49e299a55346'
>>> encode_defunct(hexstr='0x49e299a55346')
SignableMessage(version=b'E',
                  header=b'thereum Signed Message:\n6',
                  body=b'I\xe2\x99\xa5SF')

>>> encode_defunct(0x49e299a55346)
SignableMessage(version=b'E',
                  header=b'thereum Signed Message:\n6',
                  body=b'I\xe2\x99\xa5SF')
```

`eth_account.messages.encode_intended_validator` (*validator_address: Union[NewType.<locals>.new_type, str], primitive: bytes = None, *, hexstr: str = None, text: str = None*) → `eth_account.messages.SignableMessage`

Encode a message using the “intended validator” approach (ie~ version 0) defined in [EIP-191](#).

Supply the message as exactly one of these three arguments: bytes as a primitive, a hex string, or a unicode string.

Warning: Note that this code has not gone through an external audit. Also, watch for updates to the format, as the EIP is still in DRAFT.

Parameters

- **validator_address** – which on-chain contract is capable of validating this message, provided as a checksummed address or in native bytes.
- **primitive** (*bytes* or *int*) – the binary message to be signed
- **hexstr** (*str*) – the message encoded as hex
- **text** (*str*) – the message as a series of unicode characters (a normal Py3 str)

Returns The EIP-191 encoded message, ready for signing

```
eth_account.messages.encode_structured_data (primitive: Union[bytes, int, collections.abc.Mapping] = None, *, hexstr: str = None, text: str = None) → eth_account.messages.SignableMessage
```

Encode an [EIP-712](#) message.

EIP-712 is the “structured data” approach (ie~ version 1 of an EIP-191 message).

Supply the message as exactly one of the three arguments:

- primitive, as a dict that defines the structured data
- primitive, as bytes
- text, as a json-encoded string
- hexstr, as a hex-encoded (json-encoded) string

Warning: Note that this code has not gone through an external audit, and the test cases are incomplete. Also, watch for updates to the format, as the EIP is still in DRAFT.

Parameters

- **primitive** (*bytes* or *int* or *Mapping* (eg~ *dict*)) – the binary message to be signed
- **hexstr** – the message encoded as hex
- **text** – the message as a series of unicode characters (a normal Py3 str)

Returns The EIP-191 encoded message, ready for signing

1.2 Signers

These classes abstract away the private key, as opposed to `eth_account.account.Account`, which explicitly requires the private key on each usage.

All the signer classes in this package must meet the interface specified by `BaseAccount`.

Currently there is only one Local Signer. Some upcoming alternatives to the basic local signer include hierarchical deterministic (HD) wallets and hardware wallets.

1.2.1 Local Signer

class `eth_account.signers.local.LocalAccount` (*key*, *account*)

Bases: `eth_account.signers.base.BaseAccount`

A collection of convenience methods to sign and encrypt, with an embedded private key.

Variables `key` (*bytes*) – the 32-byte private key data

```
>>> my_local_account.address
"0xF0109fC8DF283027b6285cc889F5aA624EaC1F55"
>>> my_local_account.key
b"\x01\x23..."
```

You can also get the private key by casting the account to `bytes`:

```
>>> bytes(my_local_account)
b"\x01\x23..."
```

address

The checksummed public address for this account.

```
>>> my_account.address
"0xF0109fC8DF283027b6285cc889F5aA624EaC1F55"
```

encrypt (*password*, *kdf=None*, *iterations=None*)

Generate a string with the encrypted key.

This uses the same structure as in `encrypt()`, but without a private key argument.

key

Get the private key.

signHash (*message_hash*)

Sign the hash of a message.

This uses the same structure as in `signHash()` but without specifying the private key.

Caution: Deprecated for `sign_message()`. To be removed in v0.6

Parameters `message_hash` (*bytes*) – 32 byte hash of the message to sign

signTransaction (*transaction_dict*)

Sign a transaction dict.

This uses the same structure as in `sign_transaction()` but without specifying the private key.

Caution: Deprecated for `sign_transaction()`. This method will be removed in v0.6

Parameters `transaction_dict` (*dict*) – transaction with all fields specified

sign_message (*signable_message*)

Generate a string with the encrypted key.

This uses the same structure as in `sign_message()`, but without a private key argument.

sign_transaction (*transaction_dict*)

Sign a transaction dict.

This uses the same structure as in `sign_transaction()` but without specifying the private key.

Parameters `transaction_dict` (*dict*) – transaction with all fields specified

1.2.2 Abstract Signer

class `eth_account.signers.base.BaseAccount`

Bases: `abc.ABC`

Specify convenience methods to sign transactions and message hashes.

address

The checksummed public address for this account.

```
>>> my_account.address
"0xF0109fC8DF283027b6285cc889F5aA624EaC1F55"
```

signHash (*message_hash*)

Sign the hash of a message.

This uses the same structure as in `signHash()` but without specifying the private key.

Caution: Deprecated for `sign_message()`. To be removed in v0.6

Parameters `message_hash` (*bytes*) – 32 byte hash of the message to sign

signTransaction (*transaction_dict*)

Sign a transaction dict.

This uses the same structure as in `sign_transaction()` but without specifying the private key.

Caution: Deprecated for `sign_transaction()`. This method will be removed in v0.6

Parameters `transaction_dict` (*dict*) – transaction with all fields specified

sign_message (*signable_message*: `eth_account.messages.SignableMessage`) → `eth_account.datastructures.SignedMessage`

Sign the EIP-191 message.

This uses the same structure as in `sign_message()` but without specifying the private key.

Parameters `signable_message` – The encoded message, ready for signing

sign_transaction (*transaction_dict*)

Sign a transaction dict.

This uses the same structure as in `sign_transaction()` but without specifying the private key.

Parameters `transaction_dict` (*dict*) – transaction with all fields specified

1.3 Release Notes

1.3.1 eth-account v0.8.0 (2022-12-15)

Features

- update all references to deprecated `eth_abi.encode_abi` to `eth_abi.encode` (#200)

Performance improvements

- Reduce the number of pbkdf2 iterations to speed up tests (#77)

Deprecations and Removals

- remove deprecated methods that were noted to go in v0.5 (#195)

Internal Changes - for eth-account Contributors

- add coverage reporting to pytest (#192)
- Use updated circleci Python images, fix Sphinx warning (#194)

Miscellaneous changes

- #197, #198, #199, #202, #203, #204, #206

1.3.2 eth-account v0.7.0 (2022-08-17)

Bugfixes

- bump ansi-regex to 5.0.1 to fix minor ReDos vulnerability (#129)
- Enable lint runs again on CI (#166)
- fix DoS-able regex pattern (#178)
- Allow towncrier to build the release notes again (#185)

Improved Documentation

- Add example to generate multiple accounts from a mnemonic (#153)
- Pin Jinja2 at $\geq 3.0.0, < 3.1.0$; pin towncrier $\geq 18.5.0$; open up Sphinx requirement to allow $\geq 1.6.5, < 5$. (#156)
- added missing quotes to readme dev environment setup example (#172)

Miscellaneous changes

- #79, #155, #162, #164, #165

Breaking changes

- Change bitarray dependency requirement to be `>=2.4,<3` since 2.4 has wheels for all platform types. (#154)
- Fix errors in EIP-712 signing (#175)

1.3.3 eth-account v0.6.1 (2022-02-24)

Bugfixes

- Allow encoding of structured data containing `bytes` (#91)

Miscellaneous changes

- #68, #144

1.3.4 eth-account v0.6.0 (2022-01-20)

Features

- Update dependencies: - eth-abi - eth-keyfile - eth-keys - eth-rlp - pyrlp - eth-utils (#138)
- Add support for Python 3.9 and 3.10 (#139)

Deprecations and Removals

- Drop support for Python 3.6 (#139)

1.3.5 eth-account v0.5.9 (2022-08-04)

Bugfixes

- fix DoS-able regex pattern (#178)

Miscellaneous changes

- #183, #184

1.3.6 eth-account v0.5.8 (2022-06-06)

Miscellaneous changes

- #163, #168

1.3.7 eth-account v0.5.7 (2022-01-27)

Features

- Add support for Python 3.9 and 3.10 (#139)

Bugfixes

- `recover_message` now raises an `eth_keys.exceptions.BadSignature` error if the `v`, `r`, and `s` points are invalid (#142)

1.3.8 eth-account v0.5.6 (2021-09-22)

Features

- An explicit transaction type is no longer required for signing a transaction if we can implicitly determine the transaction type from the transaction parameters (#125)

Bugfixes

- When signing a transaction, the regular JSON-RPC structure is now expected as input and is converted to the appropriate rlp transaction structure when signing (#125)
- Fix string interpolation in `ValidationError` message of `_hash_eip_191_message` (#128)

Improved Documentation

- Updated docs for `sign_transaction` to show that transaction type can be implicitly determined based on transaction parameters if one is not provided (#126)
- Add `encode_defunct` to list of example message encoders (#127)

1.3.9 eth-account v0.5.5 (2021-07-21)

Features

- Added support for EIP-2718 (Typed Transaction) and EIP-2939 (Access List Transaction) (#115)
- Added support for EIP-1559 (Dynamic Fee Transaction) (#117)

Bugfixes

- Structured messages (EIP-712) now permit leaving some (but not all) domain fields undefined. (#72)

Internal Changes - for eth-account Contributors

- Upgrade project template, of note: a new mypy & pydocstyle, and types being exported correctly. (#121)

Miscellaneous changes

- [#116](#)

1.3.10 v0.5.3 (2020-08-31)

Performance improvements

- RLP encoding/decoding speedup by using rlp v2alpha1, which has a rust implementation. ([#104](#))

1.3.11 v0.5.2 (2020-04-30)

Bugfixes

- Makes sure that the raw txt files needed for Mnemonics get packaged with the release. ([#99](#))

1.3.12 v0.5.1

Released 2020-04-23

- Fix a crash in signing typed messages with arrays [#97](#)
- Replace attrdict with NamedTuple to silence a deprecation warning [#76](#)
- Run more doctests & improve docs [#94](#)

1.3.13 v0.5.0

Released 2020-03-30

- Add Python 3.8 support [#86](#)
- Add opt-in support for Mnemonic seed phrases [#87](#) (NOTE: This API is unaudited and likely to change)
- Dependency change: support eth-keys v0.3.* [#69](#)

1.3.14 v0.4.0

Released 2019-05-06

- BREAKING CHANGE: drop python 3.5 (and therefore pypy3 support). [#60](#) (includes other housekeeping)
- New message signing API: `sign_message()` and `recover_message`. [#61](#)
 - New `eth_account.messages.encode_intended_validator()` for EIP-191's Intended Validator message-signing format. [#56](#)
 - New `eth_account.messages.encode_structured_data()` for EIP-712's Structured Data message-signing format. [#57](#)
- Add optional param iterations to `encrypt()` [#52](#)
- Add optional param kdf to `encrypt()`, plus env var `ETH_ACCOUNT_KDF`. Default kdf switched from `hmac-sha256` to `scrypt`. [#38](#)
- Accept "to" addresses formatted as `bytes` in addition to checksummed, hex-encoded. [#36](#)

1.3.15 v0.3.0

Released July 24, 2018

- Support `eth_keys.datatypes.PrivateKey` in params that accept a private key.
- New docs for *Signers*
- Under the hood: add a new *BaseAccount* abstract class, so that upcoming signing classes can implement it (be on the lookout for upcoming hardware wallet support)

1.3.16 v0.2.3

Released May 27, 2018

- Implement `__eq__` and `__hash__` for *LocalAccount*, so that accounts can be used in `set`, or as keys in `dict`, etc.

1.3.17 v0.2.2

Released Apr 25, 2018

- Compatibility with `pyrlp` v0 and v1

1.3.18 v0.2.1

Released Apr 23, 2018

- Accept 'from' in `signTransaction`, if it matches the sending private key's address

1.3.19 v0.2.0 (stable)

Released Apr 19, 2018

- Audit cleanup is complete
- Stopped requiring `chainId`, until tooling to automatically derive it gets better (Not that transactions without `chainId` are potentially replayable on fork chains)

1.3.20 v0.2.0-alpha.0

Released Apr 6, 2018

- Ability to sign an already-hashed message
- Moved `eth_sign`-style message hashing to `eth_account.messages.defunct_hash_message()`
- Stricter transaction input validation, and better error messages. Including: `to` field must be checksummed.
- PyPy3 support & tests
- Upgrade dependencies
- Moved non-public interfaces to *internal* module
- Documentation
 - use `getpass` instead of typing in password manually

- `eth_account.signers.local.LocalAccount` attributes
- readme improvements
- more

1.3.21 v0.1.0-alpha.2

- Imported the local signing code from `web3.py`'s `w3.eth.account`
- Imported documentation and added more
- Imported tests and pass them

1.3.22 v0.1.0-alpha.1

- Launched repository, claimed names for pip, RTD, github, etc

CHAPTER 2

Indices and tables

- `genindex`
- `modindex`

e

`eth_account.account`, [3](#)

`eth_account.datastructures`, [12](#)

`eth_account.messages`, [13](#)

`eth_account.signers.base`, [17](#)

`eth_account.signers.local`, [16](#)

A

`Account` (class in `eth_account.account`), 3
`address` (`eth_account.signers.base.BaseAccount` attribute), 17
`address` (`eth_account.signers.local.LocalAccount` attribute), 16

B

`BaseAccount` (class in `eth_account.signers.base`), 17
`body` (`eth_account.messages.SignableMessage` attribute), 13

C

`create()` (`eth_account.account.Account` method), 3
`create_with_mnemonic()`
 (`eth_account.account.Account` method), 3

D

`decrypt()` (`eth_account.account.Account` static method), 4
`defunct_hash_message()` (in module `eth_account.messages`), 13

E

`enable_unaudited_hdwallet_features()`
 (`eth_account.account.Account` class method), 5
`encode_defunct()` (in module `eth_account.messages`), 14
`encode_intended_validator()` (in module `eth_account.messages`), 14
`encode_structured_data()` (in module `eth_account.messages`), 15
`encrypt()` (`eth_account.account.Account` class method), 5
`encrypt()` (`eth_account.signers.local.LocalAccount` method), 16
environment variable
 `ETH_ACCOUNT_KDF`, 5, 21

`eth_account.account` (module), 3
`eth_account.datastructures` (module), 12
`eth_account.messages` (module), 13
`eth_account.signers.base` (module), 17
`eth_account.signers.local` (module), 16
`ETH_ACCOUNT_KDF`, 5, 21

F

`from_key()` (`eth_account.account.Account` method), 5
`from_mnemonic()` (`eth_account.account.Account` method), 6

H

`hash` (`eth_account.datastructures.SignedTransaction` attribute), 12
`header` (`eth_account.messages.SignableMessage` attribute), 13

K

`key` (`eth_account.signers.local.LocalAccount` attribute), 16

L

`LocalAccount` (class in `eth_account.signers.local`), 16

M

`messageHash` (`eth_account.datastructures.SignedMessage` attribute), 12

R

`r` (`eth_account.datastructures.SignedMessage` attribute), 12
`r` (`eth_account.datastructures.SignedTransaction` attribute), 13
`rawTransaction` (`eth_account.datastructures.SignedTransaction` attribute), 13
`recover_message()` (`eth_account.account.Account` method), 7

```
recover_transaction()  
    (eth_account.account.Account      method),  
    8
```

S

```
s (eth_account.datastructures.SignedMessage attribute),  
    12  
s (eth_account.datastructures.SignedTransaction attribute), 13  
set_key_backend() (eth_account.account.Account  
    method), 8  
sign_message() (eth_account.account.Account  
    method), 9  
sign_message() (eth_account.signers.base.BaseAccount  
    method), 17  
sign_message() (eth_account.signers.local.LocalAccount  
    method), 16  
sign_transaction()  
    (eth_account.account.Account      method),  
    10  
sign_transaction()  
    (eth_account.signers.base.BaseAccount  
    method), 17  
sign_transaction()  
    (eth_account.signers.local.LocalAccount  
    method), 16  
SignableMessage (class in eth_account.messages),  
    13  
signature (eth_account.datastructures.SignedMessage  
    attribute), 12  
SignedMessage (class in eth_account.datastructures),  
    12  
SignedTransaction (class in  
    eth_account.datastructures), 12  
signHash() (eth_account.account.Account method), 9  
signHash() (eth_account.signers.base.BaseAccount  
    method), 17  
signHash() (eth_account.signers.local.LocalAccount  
    method), 16  
signTransaction()  
    (eth_account.signers.base.BaseAccount  
    method), 17  
signTransaction()  
    (eth_account.signers.local.LocalAccount  
    method), 16
```

V

```
v (eth_account.datastructures.SignedMessage attribute),  
    12  
v (eth_account.datastructures.SignedTransaction attribute), 13  
version (eth_account.messages.SignableMessage attribute), 13
```