# *Создание ключей*

**create/keys**

Параметры

method – метод для создания ключей

dsa, rsa, dh, ecdsa

*Для RSA*

keysize *– размер числа n*

*Для DSA*

keysize *– размер числа p*

*Для DH*

*Для ECDSA*

curve – кривая для создания ключей

secp256k1, secp112r1, secp128r1, secp160r1, secp192r1, secp224r1, secp384r1, secp256r1, secp521r1

Возвращает

**Пример**

Запрос

http://192.168.0.104:4430/create/keys?method=dsa&keysize=2048

Ответ

{

"id": "6693",

"public": ""

}

*Подпись сообщения*

**sign**

id *– номер ключа*

message *– сообщение для подписи*

http://192.168.0.104:4430/sign?message=sdsd&id=6693

{

"message": "sdsd",

"signature": "478d60acdd7153ca93954d8912de1115dde19ffa5d332256d61182b15f5496c5cd9303a9c28d80cedf2c2eacbfd8c06a1431ea01d5726c3c"

}

*Проверка подписи*

**verify**

message *– сообщение для проверки*

signature *– подпись сообщения*

*Формат в hex без символа 0х в начале и h в конце, можно с разделителем «:»*

method *– метод для проверки подписи*

dsa, rsa, dh, ecdsa

public *– публичный ключ, которым проверяется подпись сообщения*

*Формат в hex без символа 0х в начале и h в конце, можно с разделителем «:»*

**Пример**

http://192.168.0.104:4430/verify?method=dsa&message=sdsd&signature=478d60acdd7153ca93954d8912de1115dde19ffa5d332256d61182b15f5496c5cd9303a9c28d80cedf2c2eacbfd8c06a1431ea01d5726c3c&public=

{

"valid": "true"

}

import

http://192.168.0.104:4430/import?method=dsa&public=&private=474358e14264c4f030c87924c403eee50bc94efbc8ad73cde091f251

{

"id": "3637",

"public": ""

}

export/keys

http://192.168.0.104:4430/export/keys?id=6693

{

"private": "474358e14264c4f030c87924c403eee50bc94efbc8ad73cde091f251",

"public": ""

}

create/keys/secret

http://192.168.0.104:4430/create/keys/secret?id=302&public=af2044bf1c74c15aca9d5dce7285ec90be1a53322f99b7eaadfd36ea0e4ccf6e3291ddb7ec2f6ce7d7942b948387ffd9cc9da616cb677781af1f136d02a2d9740959c49cbad142b420a6e0caaf5eac6588fa4447dc3f59adaf73e9ecfb5a8bdc1ce5b2ef6f0dff2d306a803acf007b0907fb2e584a85f0c1a1ad9cf456ca4358

{

"secret\_id": "7028"

}

encrypt

http://192.168.0.104:4430/encrypt?message=saicryptomodule&id=7028

{

"cipher": "8a1032abf5e370e3cddce0f887470e186c6c349ef232e4a9b135fca195411d96",

"message": "saicryptomodule"

}

decrypt

http://192.168.0.104:4430/decrypt?cipher=8a1032abf5e370e3cddce0f887470e186c6c349ef232e4a9b135fca195411d96&id=5940

{

"cipher": "8a1032abf5e370e3cddce0f887470e186c6c349ef232e4a9b135fca195411d96",

"message": "saicryptomodule"

}

create/btc/keys

http://192.168.0.104:4430/create/btc/keys

{

"id": "5496",

"public": "0429300f9e306e4e81da8a398493e4d25c722ea1fb2351043967f2979ca872066a28cdce0e26987205206cff4e46e8ee7478c4e3a42bd4e4cc77320e2543813438"

}

create/btc/address

http://192.168.0.104:4430/create/btc/address?id=5496

{

"address": "1ePMGPq6vUg4vemVTsMq8GjHb2jVaJEXX"

}

sign/btc

http://192.168.0.104:4430/sign/btc?id=5496&message=ds

{

"message": "ds",

"signature": "f7188bfb6188023275c5ed93def9971090a822e41b138c78aec4c4845971953b004d0120552276a6308381f7ce810574785eab4ffcac77b37d5d488daa61952b"

}

verify/btc

http://192.168.0.104:4430/verify/btc?public=0429300f9e306e4e81da8a398493e4d25c722ea1fb2351043967f2979ca872066a28cdce0e26987205206cff4e46e8ee7478c4e3a42bd4e4cc77320e2543813438&message=ds&signature=f7188bfb6188023275c5ed93def9971090a822e41b138c78aec4c4845971953b004d0120552276a6308381f7ce810574785eab4ffcac77b37d5d488daa61952b

{

"valid": "true"

}

import/btc/keys

http://192.168.0.104:4430/import/btc/keys?public=0429300f9e306e4e81da8a398493e4d25c722ea1fb2351043967f2979ca872066a28cdce0e26987205206cff4e46e8ee7478c4e3a42bd4e4cc77320e2543813438&private=f5597c7e97413e587fad12a2ec5d3a02f04649c1e3909fa402807d7974b0356e

{

"id": "1527",

"public": "0429300f9e306e4e81da8a398493e4d25c722ea1fb2351043967f2979ca872066a28cdce0e26987205206cff4e46e8ee7478c4e3a42bd4e4cc77320e2543813438"

}

export/btc/keys

http://192.168.0.104:4430/export/btc/keys?id=5496

{

"private": "f5597c7e97413e587fad12a2ec5d3a02f04649c1e3909fa402807d7974b0356e",

"public": "0429300f9e306e4e81da8a398493e4d25c722ea1fb2351043967f2979ca872066a28cdce0e26987205206cff4e46e8ee7478c4e3a42bd4e4cc77320e2543813438"

}

create/eth/keys

http://192.168.0.104:4430/create/eth/keys

{

"id": "6087",

"public": "867fd332897e685120a415cc9bad02b92b02aea550b22850884f7f5b0020539a68b36aac3ce456568088d814196fe47747d358628357ea3063af5ffff46bc6f0"

}

create/eth/address

http://192.168.0.104:4430/create/eth/address?id=4540

{

"address": "0dcc289a8fab3fab67c848b91a84fb6215427630"

}

sign/eth

http://192.168.0.104:4430/sign/eth?id=4540&message=aaa

{

"message": "aaa",

"signature": "d96891564654d4747b9dae4fcef16b0f7b44888859cf3a44d4ab650d9942bb0a88761fc492015fd61113210e367959c93c5ad5917843fb9d45fcd15d18258d1e"

}

verify/eth

http://192.168.0.104:4430/verify/eth?signature=d96891564654d4747b9dae4fcef16b0f7b44888859cf3a44d4ab650d9942bb0a88761fc492015fd61113210e367959c93c5ad5917843fb9d45fcd15d18258d1e&message=aaa&public=bb68092b4f5eb174e2e6a370028c82a913ff395b6913feab8a73087d174a4bb1740f96beb9ee93cd39239f31fdd96a332772526e02c1e036455fecd5f73c368c

{

"valid": "true"

}

export/eth/keys

http://192.168.0.104:4430/export/eth/keys?id=6087

{

"private": "731fa524bdde2798ff338d4bd19d859540b78ac40e27b86999581adf7041ce71",

"public": "867fd332897e685120a415cc9bad02b92b02aea550b22850884f7f5b0020539a68b36aac3ce456568088d814196fe47747d358628357ea3063af5ffff46bc6f0"

}

import/eth/keys

http://192.168.0.104:4430/import/eth/keys?private=731fa524bdde2798ff338d4bd19d859540b78ac40e27b86999581adf7041ce71&public=867fd332897e685120a415cc9bad02b92b02aea550b22850884f7f5b0020539a68b36aac3ce456568088d814196fe47747d358628357ea3063af5ffff46bc6f0

{

"id": "1314",

"public": "867fd332897e685120a415cc9bad02b92b02aea550b22850884f7f5b0020539a68b36aac3ce456568088d814196fe47747d358628357ea3063af5ffff46bc6f0"

}

admin