DOCUMENTATION

API SERENITY SHIELD

# AuthController

POST /auth/login

This function is used to connect when the user is already known.

It will return a Json Web Token .

|  |  |
| --- | --- |
| Parameter | TYPE |
| publicKey | string |
| code | string |
| buffer | Object buffert |

In the request body

{

"publicKey": "string",

"code": "string",

"buffer": {

"type": "string",

"data": [

0

]

}

}

POST /auth/authorized

This function verify if the publicKey is registered in whitelist.

Return a Boolean.

|  |  |
| --- | --- |
| Parameter | TYPE |
| publicKey | string |

In the request body

{

"publicKey": "string"

}

POST /auth/verify-code-email

This function need bearer token in header.

This function verify if the code sended by email is registered in database.

Return a Boolean.

|  |  |
| --- | --- |
| Parameter | TYPE |
| code | string |

In the request body

{

"code": "string"

}

POST /auth/verify-code-sms

This function need bearer token in header.

This function verify if the code sended by sms is registered in database.

Return a Boolean.

|  |  |
| --- | --- |
| Parameter | TYPE |
| code | string |

In the request body

{

"code": "string"

}

POST /auth/ activate after verification

This function need bearer token in header.

This function activate the user after codes verifications in database.

Return a Boolean.

POST /cryptage/encrypt Encrypt Function

This function is used to encrypt the input parameter using a key. and convert data in Base64 string

It will return encrypted datas.

|  |  |
| --- | --- |
| Parameter | TYPE |
| Data1 | string |
| Data2 | string |

In the request body

{

"data1": "string",

"data2": "string"

}

POST /cryptage/decrypt

This function is used to decrypt the input parameter using a key and encode data to Unicode string.

It will return decrypted datas.

|  |  |
| --- | --- |
| Parameter | TYPE |
| Data1 | string |
| Data2 | string |

In the request body

{

"data1": "string",

"data2": "string"

}

POST /cryptage/encryptHexa

This function is used to encrypt the input parameter using a key. and convert data in Hexadecimal string

It will return encrypted datas.

|  |  |
| --- | --- |
| Parameter | TYPE |
| Data1 | string |
| Data2 | string |

In the request body

{

"data1": "string",

"data2": "string"

}

POST /cryptage/decryptHexa

This function is used to decrypt the input parameter using a key and encode data to Unicode string.

It will return decrypted datas.

|  |  |
| --- | --- |
| Parameter | TYPE |
| Data1 | string |
| Data2 | string |

In the request body

{

"data1": "string",

"data2": "string"

}

# GetController

GET /me

This function need bearer token in header.

This function get the current IUser.

POST/me

This function create a new user.

It will return a Json Web Token.

|  |  |
| --- | --- |
| Parameter | TYPE |
| publicKey | string |
| typeWallet | string |
| idTypeWallet | string |
| phone | string |
| email | string |
| firstName | string |
| lastName | string |
| idCard | string |
| passport | string |
| addedSecurity | string |

In the request body

{

"publicKey": "string",

"typeWallet": "string",

"idTypeWallet": "string",

"phone": "string",

"email": "string",

"firstName": "string",

"lastName": "string",

"idCard": "string",

"passport": "string",

"addedSecurity": "string"

}

POST/me/send-code-email

This function need bearer token in header.

This function resend code email

POST/me/send-code-mobile

This function need bearer token in header.

This function resend code sms

POST/me/desactive

This function need bearer token in header.

This function is especially for developers when we need to disable a user.

POST/me/wallet/secret

This function need bearer token in header.

This function check if the user have a secret wallet and if not, insert it.

Return a Boolean .

|  |  |
| --- | --- |
| Parameter | TYPE |
| secretPublicKey | string |

In the request body

{

" secretPublicKey": "string"

}

POST/me/wallet/metamask

This function insert.metamask publicKey en chain id from web3.

Return a Boolean .

|  |  |
| --- | --- |
| Parameter | TYPE |
| metamaskPublicKey | string |
| chainId | string |

In the request body

{

"metamaskPublicKey": "string",

"chainId": "string"

}

POST/me/wallet/exist-secret-wallet

This function make a verification in database to know if secret wallet exist..

Return a Boolean .

|  |  |
| --- | --- |
| Parameter | TYPE |
| secretPublicKey | string |
| solanaPublicKey | string |
| idUser |  |

In the request body

{ {

"secretPublicKey": "string",

"solanaPublicKey": "string",

"idUser": "string"

}

POST/me/wallet/exist-metamask-wallet

This function make a verification in database to know if metamask wallet exist..

Return a Boolean .

|  |  |
| --- | --- |
| Parameter | TYPE |
| secretPublicKey | string |
| solanaPublicKey | string |
| idUser |  |

In the request body

{ {

"secretPublicKey": "string",

"solanaPublicKey": "string",

"idUser": "string"

}

# HistoryController

GET/wallet/listHistory

This function need bearer token in header.

This function list user history.

Return a list of histoty object .

GET/insertHistory

This function is called by clicking link in the sended Email from Activity Verification.

It will update the history connection of the User

# ManageHeirController

GET/heir/{id}

This function need bearer token in header.

This function get a heir from idHeir.

GET/heir/{id}

This function need bearer token in header.

This function get the user list of heir .

POST/heir

This function need bearer token in header.

This function insert a new heir.

Return a heir object .

|  |  |
| --- | --- |
| Parameter | TYPE |
| lastName | string |
| firstName | string |
| phone | string |
| email | string |
| publicKey | string |
| idTypeWallet | string |

In the request body

{

"lastName": "string",

"firstName": "string",

"phone": "string",

"email": "string",

"publicKey": "string",

"idTypeWallet": "string"

}

PACTH/heir

This function need bearer token in header.

This function update heir.

Return a heir object .

|  |  |
| --- | --- |
| Parameter | TYPE |
| idHeir | string |
| lastName | string |
| firstName | string |
| phone | string |
| email | string |
| publicKey | string |
| idTypeWallet | string |

In the request body

{

"idHeir": "string",

"lastName": "string",

"firstName": "string",

"phone": "string",

"email": "string",

"publicKey": "string",

"idTypeWallet": "string"

}

DELETE/heir

This function need bearer token in header.

This function delete heir.

Return a boolean.

|  |  |
| --- | --- |
| Parameter | TYPE |
| idHeir | string |

In the request body

{

"idHeir": "string",

}

# PersonnalStrongboxController

POST/personal-strongbox

This function need bearer token in header.

This function insert a personal strongbox

Return a personal strongbox object .

|  |  |
| --- | --- |
| Parameter | TYPE |
| label | string |
| scPK | string |
| codeID | string |
| payingPK | string |
| secretPK | string |
| solanaPK | string |
| solUsrNftPK | string |
| solSereNftPK | string |
| solHeirNftPKs | string |
| CONTENT | object |
| label | string |
| provider | string |
| type | string |
| idTypeWallet | string |

In the request body

{

"label": "string",

"scPK": "string",

"codeID": "string",

"payingPK": "string",

"secretPK": "string",

"solanaPK": "string",

"solUsrNftPK": "string",

"solSereNftPK": "string",

"solHeirNftPKs": "string",

"content": [

{

"label": "string",

"type": "string",

"provider": "string",

"idTypeWallet": "string",

"seed": "string"

}

]

}

PATCH/personal-strongbox

This function need bearer token in header.

This function update a personal strongbox

Return a boolean .

|  |  |
| --- | --- |
| Parameter | TYPE |
| id | string |
| walletPublicKeyOwner | string |
| label | string |
| scPK | string |
| codeID | string |
| payingPK | string |
| secretPK | string |
| solanaPK | string |
| solUsrNftPK | string |
| solSereNftPK | string |
| solHeirNftPKs | string |
| CONTENT | object |
| label | string |
| provider | string |
| type | string |
| idTypeWallet | string |

In the request body

{

"label": "string",

"walletPublicKeyOwner": "string",

"scPK": "string",

"codeID": "string",

"payingPK": "string",

"secretPK": "string",

"solanaPK": "string",

"solUsrNftPK": "string",

"solSereNftPK": "string",

"solHeirNftPKs": "string",

"id": "string",

"content": [

{

"label": "string",

"type": "string",

"provider": "string",

"idTypeWallet": "string",

"seed": "string"

}

]

}

GET/personal-strongbox

This function need bearer token in header.

This function return the user personal strongbox list.

GET/personal-strongbox/{id}

This function need bearer token in header.

This function return the user personal strongbox by id.

DELETE/personal-strongbox/{id}

This function need bearer token in header.

This function delete the user personal strongbox by id.

# PolicyActivationController

All these functions will be used by the policy-activation service

POST/reactive

This function is used to reactivate the period monitoring of the inactivity of the user

Return a boolean.

|  |  |
| --- | --- |
| Parameter | TYPE |
| idUser | string |
| idStrongboxheir | string |

In the request body

{

" idUser ": "string",

idStrongboxheir ": "string",

}

POST/declared-deceaded

This function is used to declare a user deceaded.

Return a boolean.

|  |  |
| --- | --- |
| Parameter | TYPE |
| idUser | string |
| idStrongboxheir | string |

In the request body

{

" idUser ": "string",

idStrongboxheir ": "string",

}

POST/unlocke-strongboxforheir/{id}

This function is used to unlock the strongbox for heir.

Return a boolean.

|  |  |
| --- | --- |
| Parameter | TYPE |
| idStrongboxheir | string |

In the request body

{

idStrongboxheir ": "string",

}

POST/lock-strongboxforheir/{id}

This function is used to lock the strongbox for heir.

Return a boolean.

|  |  |
| --- | --- |
| Parameter | TYPE |
| idStrongboxheir | string |

In the request body

{

idStrongboxheir ": "string",

}

POST/paid-strongboxforheir/{id}

This function is used to update the paid state of the strongbox for heir.

Return a boolean.

|  |  |
| --- | --- |
| Parameter | TYPE |
| idStrongboxheir | string |

In the request body

{

idStrongboxheir ": "string",

}

# ShamirController

POST/shamir/secret-sharing

This function is used to get the keys for nft creation..

Return 3 keys encrypted.

|  |  |
| --- | --- |
| Parameter | TYPE |
| formulation | string |

In the request body

{

formulation ": "string",

}

POST/shamir/secret-sharing-revolving

This function is used to get get the original formulation from two keys..

Return original formulation.

|  |  |
| --- | --- |
| Parameter | TYPE |
| Key1 | string |
| Key2 | string |

In the request body

{

formulation ": "string",

}

# StrongBoxForHeirController

POST/Strongbox-for-heir

This function need bearer token in header.

This function is used to insert to insert strongbox for heir .  
Returns the newly created item

{

"idInactivePeriod": "string",

"label": "string",

"messageForHeirs": "string",

"display": true,

"prepayedInherence": true,

"scPK": "string",

"codeID": "string",

"payingPK": "string",

"secretPK": "string",

"solanaPK": "string",

"solUsrNftPK": "string",

"solSereNftPK": "string",

"solHeirNftPKs": "string",

"content": [

{

"label": "string",

"type": "string",

"provider": "string",

"idTypeWallet": "string",

"seed": "string"

}

],

"heirs": [

{

"idUser": "string",

"idHeir": "string",

"lastName": "string",

"firstName": "string",

"phone": "string",

"email": "string",

"publicKey": "string",

"walletType": {

"id": "string",

"label": "string",

"type": "string",

"supported": true

},

"creation\_Date": "string"

}

]

}

PAcTH/Strongbox-for-heir

Update the strongbox.

Return a boolean

{

"id": "string",

"label": "string",

"walletPublicKeyOwner": "string",

"scPK": "string",

"codeID": "string",

"payingPK": "string",

"secretPK": "string",

"solanaPK": "string",

"solUsrNftPK": "string",

"solSereNftPK": "string",

"solHeirNftPKs": "string",

"idInactivePeriod": "string",

"messageForHeirs": "string",

"display": true,

"prepayedInherence": true,

"content": [

{

"label": "string",

"type": "string",

"provider": "string",

"idTypeWallet": "string",

"seed": "string"

}

],

"heirs": [

{

"idUser": "string",

"idHeir": "string",

"lastName": "string",

"firstName": "string",

"phone": "string",

"email": "string",

"publicKey": "string",

"walletType": {

"id": "string",

"label": "string",

"type": "string",

"supported": true

},

"creation\_Date": "string"

}

]

}

GET/Strongbox-for-heir

This function need bearer token in header.

Return the user strongbox for heir list

DELETE/Strongbox-for-heir/{id}

This function need bearer token in header.

This function delete strongbox by id

Return a boolean

GET/Strongbox-for-heir/{id}

This function need bearer token in header.

This function get strongbox by id

Return a strongbox for heir

GET/Strongbox-for-heir/{id}

This function need bearer token in header.

This function get strongbox list

Return a strongbox for heir

GET/Strongbox-heritage

This function need bearer token in header.

This function get the strongbox heritage list

Return a strongbox heritage

GET/Strongbox-heritage/{id}

This function need bearer token in header.

This function get strongbox heritage by id (strongbox where user is heir)

Return a strongbox heritage

# SubscriptionPlanController

POST/plan

This function insert payment plan ;

Return a boolean

|  |  |
| --- | --- |
| idPlan | string |
| transaction | string |
| currency | string |
| paiementType | string |

Request body

{

"idPlan": "string",

"transaction": "string",

"currency": "string",

"paiementType": "string"

}

PATCH/plan

This function update payment plan ;

Return a boolean

|  |  |
| --- | --- |
| idPlan | string |
| transaction | string |
| currency | string |
| paiementType | string |

Request body

{

"idPlan": "string",

"transaction": "string",

"currency": "string",

"paiementType": "string"

}

GET/Plan

This function return list plan

GET/invoices

This function return list plan