Export Description

The following data should be exported:

- Identities
- Accounts
- Recipients

The data should be exported to a file with extension ".concordiumwallet". The content of a file is a JSON object which contains an encrypted JSON object and some metadata for the encryption.

Export Encryption

To encrypt data, a password must be requested from the user. Based on the password, a 256 bit key must be created with PKDF2 using HMAC-SHA256 with a random salt.

The key is for an AES encryption in CBC mode with PKCS7 padding and a random initialization vector.

To be able to decrypt again, the initialization vector, salt, and number of iterations is needed together with the cipher and a password requested from the user. These data must be inserted into a JSON object with the following structure:

Field	Type	Optional /Mandatory	Comment
metaData	EncryptionMetaData	Mandatory	An object describing the encryption method
cipherText	String	Mandatory	The encrypted exported json data. Base64 encoded

EncryptionMetaData

EncryptionMetaData contains the following information:

Field	Type	Optional /Mandatory	Comment
encryptionMethod	String	Mandatory	The mobile wallet will only support "AES-256"
keyDerivationMethod	String	Mandatory	The mobile wallet will only support "PBKDF2WithHmacSHA256"
iterations	Int	Mandatory	Number of iterations performed when generating the key
salt	String	Mandatory	The random-generated salt (32 bytes) used to create the key. Base64 encoded
initializationVector	String	Mandatory	The random-generated initialization vector (16 bytes) used to encrypt data. Base64 encoded

Sample JSON


```
{
  "metadata": {
    "encryptionMethod": "AES-256",
    "keyDerivationMethod": "PBKDF2WithHmacSHA256",
    "iterations": 100000,
    "salt": "Lb9ul7JP2FzxZITi+5PebOM0VMZPyl/ogzRUIZBg3zM=",
    "initializationVector": "EzLwzT6VSw1bp3wJGmQrng==",
  }
  "cipherText": "xA7oExZLXrtYJtfm6P8h81W23f/ZAX7DDCJVsmqJki+HCin9FDjNQo2am3/rc0zgRBjyg33Fp1HX8IJdh2pg/UH0dcBAl
[...]"
}
```


Export Format

The cipherText described above is an encrypted JSON object. The JSON object contains the following data:

Field	Type	Optional /Mandatory	Comment
value	ExportValue	Mandatory	Exported data. See description below
v	Int	Mandatory	A number describing the version of the exported data. Can be used to ensure data can be imported in later versions of the app. In the first version, the number inserted will be '1'

type	String	Mandatory	always "concordium-mobile-wallet-data"

ExportValue

Field	Type	Optional /Mandatory	Comment
identities	[IdentityData]	Mandatory	All identities that exists on the phone. See description below
recipients	[Recipient]	Mandatory	All recipients that exists on the phone. See description below

IdentityData

Field	Type	Optional /Mandatory	Comment
nextAccountNumber	Int	Mandatory	This number is used for "accountNumber" next time an account is created for the identity.
identityProvider	IdentityProviderInfo	Mandatory	This is the exact object retrieved by calling the /ipInfo endpoint, containing "ipInfo" and "metadata"
identityObject	IdentityObject	Mandatory	This is the exact "identityObject" object retrieved from the identity provider, containing "signature", "attributeList" and "preIdentityObject"
privateIdObjectData	PrivateIdObjectData	Mandatory	This is the exact "privateIdObjectData" object that was returned by the create_id_request_and_private_data library call, containing "aci" and "randomness"
name	String	Mandatory	Identity name entered by user (if this is added to our scope)
accounts	[Account]	Mandatory	All accounts that has been created for the identity. See description below.

Account

Field	Type	Optional /Mandatory	Comment
name	String	Mandatory	Account name entered by the user
address	String	Mandatory	The account address
submissionId	String	Mandatory	The submissionId received when creating the account. This is used for retrieving the transaction status for the account. Including this in the export makes it possible to also export non-finalized accounts
accountData	AccountData	Mandatory	This is the exact "accountData" object retrieved by calling the /create_credential endpoint
revealedAttributes	Dictionary	Mandatory	A collection of keys and values of all the attributes that the user has selected
credential	Credential	Mandatory	This is the exact "credential" object retrieved by calling the /create_credential endpoint, containing "account", "arData", "ipIdentity", "policy", "proofs", "regId", and "revocationThreshold"

Recipients

Field	Type	Optional /Mandatory	Comment
name	String	Mandatory	Recipient name entered by the user
address	String	Mandatory	The account address

Sample JSON

```
{
  "type": "concordium-mobile-wallet-data",
  "v": 1,
  "value": {
    "identities": [
      {
        "nextAccountNumber": 5,
        "identityProvider": {
          //This is the exact object retrieved by calling the /ipInfo endpoint
          "ipInfo": {},
          "metadata": {}
        },
        "identityObject": {
          //This is the exact object retrieved from the identity provider
          "signature": "",
          "attributeList": {},
          "preIdentityObject": {}
        },
        "privateIdObjectData": {
          //This is the exact object that was returned by the
          //create_id_request_and_private_data library call
          "aci": {},
          "randomness": ""
        },
        "name": "My identity",
        "accounts": [
          {
            "name": "My account",
            "address": "3GF7RhgCKew8CwCpuLDww4MB2vTKNqFpmHTwpgGAmoVS15Tnsr",
            "submissionId": "a386e91a0662267f004facc2cce7b7e3b9ff7dbf5568037257deb36c3ac42661",
            "accountData": {
              //This is the exact object retrieved by calling the /create_credential endpoint
              "keys": {},
              "threshold": 1
            },
            "revealedAttributes": {
              "dob": "19800229",
              "countryOfResidence": "DE"
            },
            "credential": {
              //This is the exact object retrieved by calling the /create_credential endpoint
              "account": {},
              "arData": {},
              "ipIdentity": 0,
              "policy": {},
              "proofs": "",
              "regId": "",
              "revocationThreshold": 0
            }
          }
        ]
      }
    ],
    "recipients": [
      {
        "name": "recipient-a",
        "address": "3GF7RhgCKew8CwCpuLDww4MB2vTKNqFpmHTwpgGAmoVS15Tnsr",
      }
    ]
  }
}
```