

MDIP Keymaster WebUI Tutorial

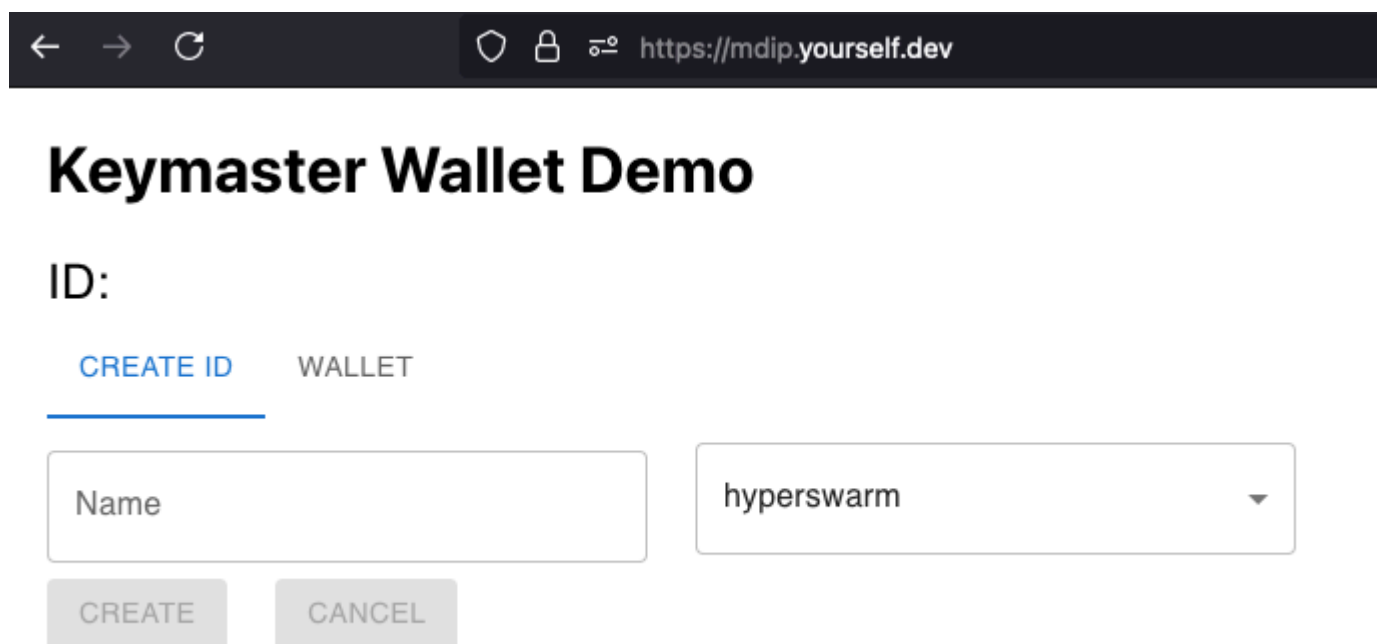
This document contains basic instructions to familiarize the reader with the use of MDIP's Keymaster WebUI.

The Keymaster WebUI is a client interface to the MDIP Keymaster Library, available in the "kc" (kay-cee) release. The WebUI is not intended to be a commercial wallet; it is a reference implementation of an MDIP wallet offering a web (React) user interface to the MDIP Keymaster library. Wallet creation and MDIP key operations are performed client-side. The server-side is running an MDIP Gatekeeper server, which exposes the Keymaster WebUI server components on port 4224.

An online version of the MDIP Keymaster WebUI is available here:
<https://mdip.yourself.dev/>

Creating your first DID

Upon visiting the link above, your browser will automatically generate a new MDIP Wallet. The keys and all information contained in an MDIP wallet is only available on the client-side. The screen below shows a blank MDIP wallet:



The screenshot shows a web browser window with the address bar displaying <https://mdip.yourself.dev>. The page title is "Keymaster Wallet Demo". Below the title, there are two tabs: "CREATE ID" (which is selected and underlined) and "WALLET". Under the "CREATE ID" tab, there is a form with a text input field labeled "Name" and a dropdown menu currently showing "hyperswarm". Below these fields are two buttons: "CREATE" and "CANCEL".

An MDIP wallet may contain multiple Agent DIDs, or identities. Each DID can be registered on a Registry of the user's choice. Local-only and Hyperswarm global DID

distribution are available along with an upcoming growing list of immutable ledgers like Bitcoin and many others.

[←](#) [→](#) [↺](#) [https://mdip.yourself.dev](#)

Keymaster Wallet Demo

ID: **Bob** did:test:z3v8AuaaSziQ2DHRXABNqMR3R99AdEcPfuyVCAGXhdQ8kmgQroK

IDENTITIES DIDS GROUPS SCHEMAS CREDENTIALS AUTH WALLET

Bob ▼

CREATE... REMOVE... BACKUP RECOVER...

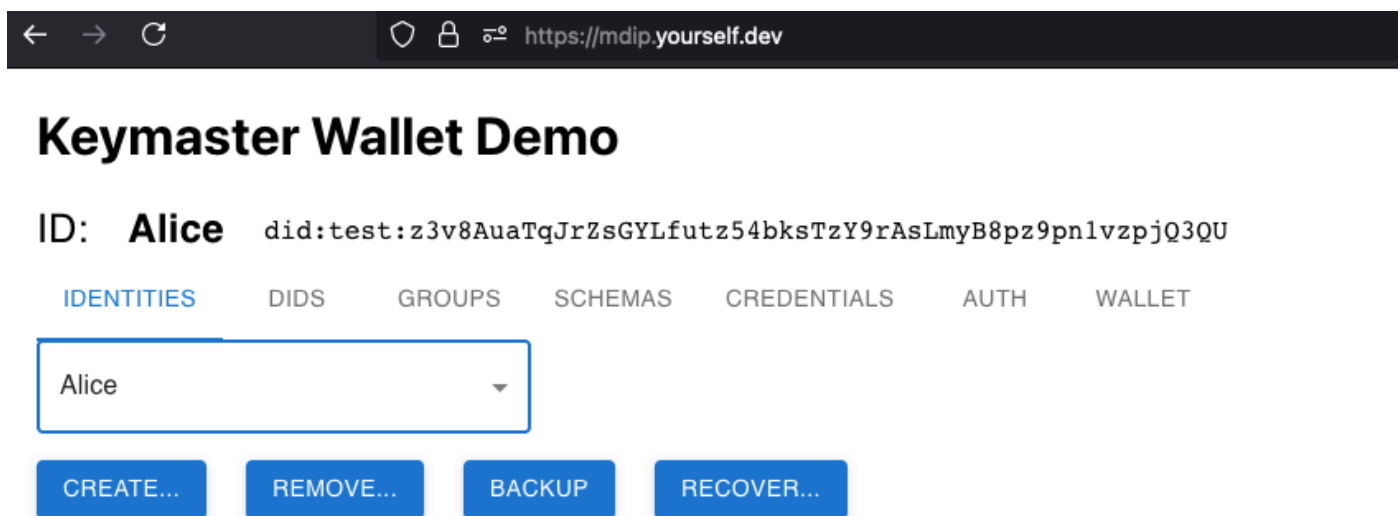
```
{
  "@context": "https://w3id.org/did-resolution/v1",
  "didDocument": {
    "@context": [
      "https://www.w3.org/ns/did/v1"
    ],
    "id": "did:test:z3v8AuaaSziQ2DHRXABNqMR3R99AdEcPfuyVCAGXhdQ8kmgQroK",
    "verificationMethod": [
      {
        "id": "#key-1",
        "controller": "did:test:z3v8AuaaSziQ2DHRXABNqMR3R99AdEcPfuyVCAGXhdQ8kmgQroK",
        "type": "EcdsaSecp256k1VerificationKey2019",
        "publicKeyJwk": {
          "kty": "EC",
          "crv": "secp256k1",
          "x": "So_yB6KZ1gU8JJwnGNLcszciERHlayB0Ydw5h0LGHzs",
          "y": "M7FzZP_zcf8x9XZ24mZQL0Zq8y_EE1_hnQIq1pRU51Y"
        }
      }
    ],
    "authentication": [
      "#key-1"
    ]
  },
  "didDocumentMetadata": {
    "created": "2024-06-25T15:53:57.509Z",
    "version": 1,
    "confirmed": true
  },
  "didDocumentData": {},
  "mdip": {
    "version": 1,
    "type": "agent",
    "registry": "local"
  }
}
```

The MDIP Wallet above now contains 1 Agent DID nicknamed "Bob". Once a DID is created, numerous new Keymaster wallet functions become available.

1. IDENTITIES: User can create new Agent DIDs, backup/recover and/or remove undesired Identities.
2. DIDS: User manage nicknames to known DIDs. Can be used to name any type of DIDs (agent, asset, groups, etc).

3. GROUPS: Manages groups of DIDs. Create groups of any types of DIDs. Note: Groups are public.
4. SCHEMAS: Manage JSON schemas to be used for attesting credentials. Note: Schemas are public and reusable.
5. CREDENTIALS - HOLD: User can accept (hold) a credential with option to view & decrypt prior to acceptance.
6. CREDENTIALS - ISSUE: Issue a credential schema to an agent DID. User can fill-in the schema values.
7. AUTH: Create and/or respond to MDIP authentication challenges. WebUI only supports DID validation at this time.
8. WALLET: Wallet-level backup and restore methods. 12-words, upload/download, or in-network backups are available.

IDENTITIES Screen



This screen offers the following functionality:

1. CREATE: Creates a new Agent DID and registers the document to the user-selected supported Registry.
2. REMOVE: Removes an Agent DID from the user's local wallet.
3. BACKUP: Backup an Agent DID to an encrypted DID Vault. Recovery is later possible using only wallet keys & DID identifier.
4. RECOVER: Recovers an Agent DID from its DID Identifier. This will recover the last Agent DID backup stored in the encrypted DID Vault.

Keymaster Wallet Demo

ID: **Alice** did:test:z3v8AuaTqJrZsGYLfutz54bksTzY9rAsLmyB8pz9pn1vzpjQ3QU

[IDENTITIES](#)[DIDS](#)[GROUPS](#)[SCHEMAS](#)[CREDENTIALS](#)[AUTH](#)[WALLET](#)

Alice ▲

Bob

Alice

BACKUP

RECOVER...

```
"@context": "https://w3id.org/did-resolution/v1",
"didDocument": {
  "@context": [
    "https://www.w3.org/ns/did/v1"
  ],
  "id": "did:test:z3v8AuaTqJrZsGYLfutz54bksTzY9rAsLmyB8pz9pn1vzpjQ3QU",
  "verificationMethod": [
    {
      "id": "#key-1",
      "controller": "did:test:z3v8AuaTqJrZsGYLfutz54bksTzY9rAsLmyB8pz9pn1vzpjQ3QU",
      "type": "EcdsaSecp256k1VerificationKey2019",
      "publicKeyJwk": {
        "kty": "EC",
        "crv": "secp256k1",
        "x": "p7M2hkqD38G3Z9l7fdHmAd2ejrNqMX6DAfJBTC_qMTs",
        "y": "tKIzPVsePyAsYfo7QEapKhNqZA8vv0KT8j9R5FkeUg"
      }
    }
  ],
  "authentication": [
    "#key-1"
  ]
},
"didDocumentMetadata": {
  "created": "2024-06-25T16:32:11.741Z",
  "version": 1,
  "confirmed": true
},
"didDocumentData": {},
"mdip": {
  "version": 1,
  "type": "agent",
  "registry": "hyperswarm"
}
```

DIDS Screen

The DIDs screen allow a user to manage named aliases to various DIDs. Named aliases are important to an MDIP wallet since they provide human-friendly context to the content of a DID. Named aliases are NOT part of a DID document; they are local to a user wallet.

Keymaster Wallet Demo

ID: **Alice** did:test:z3v8AuaXNsYfcrMPjRHmq91cmkS2FjL9pXZmYcha7LeVPDQREZC

IDENTITIES DIDS GROUPS SCHEMAS CREDENTIALS AUTH WALLET

Charlie

did:test:z3v8AuaW5P49cN4gowuvt9kUH29yEFWW2vxogyg8fQRMCMwF1e

RESOLVE

REMOVE

Name

DID

RESOLVE

ADD

```
{
  "@context": "https://w3id.org/did-resolution/v1",
  "didDocument": {
    "@context": [
      "https://www.w3.org/ns/did/v1"
    ],
    "id": "did:test:z3v8AuaW5P49cN4gowuvt9kUH29yEFWW2vxogyg8fQRMCMwF1e",
    "verificationMethod": [
      {
        "id": "#key-1",
        "controller": "did:test:z3v8AuaW5P49cN4gowuvt9kUH29yEFWW2vxogyg8fQRMCMwF1e",
        "type": "EcdsaSecp256k1VerificationKey2019",
        "publicKeyJwk": {
          "kty": "EC",
          "crv": "secp256k1",
          "x": "i5dmKuYIL4DFICS0rMteSEx30DIT19waS6u-5SJ8aUE",
          "y": "0WN3gD3naUKNwINDwILUVfzRR91lMVtuuLMxJuvxtyU"
        }
      }
    ]
  }
},
```

GROUPS Screen

The Groups screen allows a user to create groups of DIDs. Groups can also contain DIDs of other groups, enabling the creation of complex organizational structures for a collection of DIDs.

Keymaster Wallet Demo

ID: **Bob** `did:test:z3v8AuaZ8w7HqCC7MXYLmR7vyGFvAhGe9ofL5iZNU9U3UA2bxPq`

IDENTITIES DIDS **GROUPS** SCHEMAS CREDENTIALS AUTH WALLET

Group Name

my-friends ▾

CREATE GROUP

EDIT GROUP

Editing: my-friends

DID

RESOLVE

ADD

`did:test:z3v8AuaYRXcdG5W4YaMe6Enj6FW7pitMP3v3xRnogRqTrvtats`

RESOLVE

REMOVE

`did:test:z3v8AuaXNsYfcrMPjRHmq9lcmkS2FjL9pXZmYcha7LeVPDQREZC`

RESOLVE

REMOVE

SCHEMA Screen

The Schema screen allows a user to manage a local collection of credential schemas. MDIP does not impose restriction on a schema's data structures.

Keymaster Wallet Demo

ID: **Bob** did:test:z3v8AuaZ8w7HqCC7MXYLmR7vyGFvAhGe9ofL5iZNU9U3UA2bxPq

IDENTITIES DIDS GROUPS **SCHEMAS** CREDENTIALS AUTH WALLET

Editing: "Membership"

```
{
  "$schema": "http://json-schema.org/draft-07/schema#",
  "type": "object",
  "properties": {
    "isMember": {
      "type": "boolean"
    }
  },
  "required": [
    "isMember"
  ]
}
```

CREDENTIALS Screen

The Credentials screen allows a user to decrypt, accept, or issue verifiable credentials. Users must have created a Schema before a Credential can be issued. The credentials subjects are listed from known Agent DIDs contained in the wallet (from IDENTITIES and DIDS screens).

Keymaster Wallet Demo

ID: **Alice** did:test:z3v8AuaXGjATKpR4UDkQCEyPRkNuxqSje2xgpk6wJhABzy1UADi

IDENTITIES DIDS GROUPS SCHEMAS **CREDENTIALS** AUTH WALLET

HELD ISSUE ISSUED

The credential screen also allows the issuing user to "fill-in" the credential with recipient-specific content. The credential below attests Bob's membership to Alice.

Keymaster Wallet Demo

ID: **Bob** did:test:z3v8AuaZ8w7HqCC7MXYLmR7vyGFvAhGe9ofL5iZNU9U3UA2bxPq

IDENTITIES DIDS GROUPS SCHEMAS CREDENTIALS AUTH WALLET

HELD ISSUE

Alice ▾

Membership ▾

EDIT CREDENTIAL

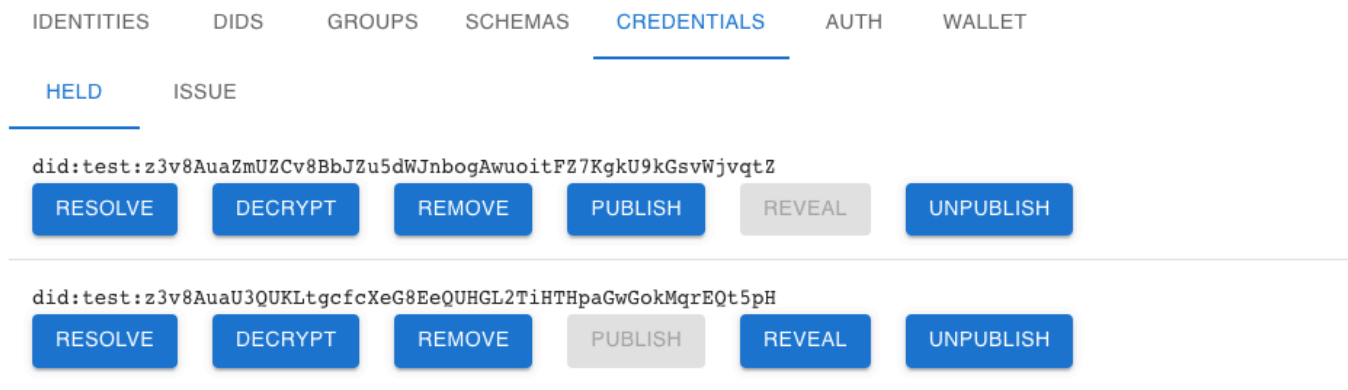
Editing Membership credential for Alice

```
{
  "@context": [
    "https://www.w3.org/ns/credentials/v2",
    "https://www.w3.org/ns/credentials/examples/v2"
  ],
  "type": [
    "VerifiableCredential",
    "did:test:z3v8AuaCMPLsGuVyxc3KJRvBB9XDk6Vs75NKcitmnWumXKBYs8Z"
  ],
  "issuer": "did:test:z3v8AuaZ8w7HqCC7MXYLmR7vyGFvAhGe9ofL5iZNU9U3UA2bxPq",
  "validFrom": "2024-06-25T20:03:44.879Z",
  "validUntil": null,
  "credentialSubject": {
    "id": "did:test:z3v8AuaTqJrZsGYLfutz54bksTzY9rAsLmyB8pz9pn1vzpjQ3QU"
  },
  "credential": {
    "isMember": true
  }
}
```

ISSUE CREDENTIAL

CREDENTIALS - HELD Screen

In the "HELD" Credentials screen, a user can chose from a variety of options.



- Resolve: This will display the *public* (encrypted) view of the credential. Resolving a credential confirms it exists in the MDIP Gatekeeper node.
- Decrypt: If the credential is encrypted to the current DID, this will decrypt the cypher_receiver field using the DID keys.
- Remove: This removes a credential from the user's wallet.
- Publish: This publishes the existence of the credential to the DID manifest, which is visible to the public. The content of the credential is nulled, but the header contains valuable information, notably the DID of the issuer and the DID of the credential schema.
- Reveal: This reveals the full content of a credential to the DID manifest, which is visible to the public. The content of the credential is decrypted and included in the DID manifest.
- Unpublish: This removes the credential from a DID manifest. Note: other nodes on the network may retain the *history* of a DID; once published or revealed a credential has been witnessed by other nodes.

The image below shows a portion of Bob's Agent DID with a revealed "isMember: true" credention in the visible portion of his DID document.

Keymaster Wallet Demo

ID: **Bob** did:test:z3v8AuaYMjwTFBxqSnCMCq1JQwhMkxwBQ7TqvrFRL4Pwz1WUSVj

IDENTITIES

DIDS

GROUPS

SCHEMAS

CREDENTIALS

AUTH

WALLET

Bob

CREATE...

REMOVE...

BACKUP

RECOVER...

```
{
  "confirmed": false,
  "updated": "2024-06-26T00:44:46.178Z"
},
"didDocumentData": {
  "manifest": {
    "did:test:z3v8AuaWCbbDEqCnxYJYvzgWkuFT6oYfwiLijK59YcobH7d1DBt": {
      "@context": [
        "https://www.w3.org/ns/credentials/v2",
        "https://www.w3.org/ns/credentials/examples/v2"
      ],
      "type": [
        "VerifiableCredential",
        "did:test:z3v8AuaamqQ2ZXLHwdKBdcPNfm7fiNci8vvuo4Mxu6ybtbMcqKHA"
      ],
      "issuer": "did:test:z3v8AuaYMjwTFBxqSnCMCq1JQwhMkxwBQ7TqvrFRL4Pwz1WUSVj",
      "validFrom": "2024-06-26T00:44:23.766Z",
      "validUntil": null,
      "credentialSubject": {
        "id": "did:test:z3v8AuaYMjwTFBxqSnCMCq1JQwhMkxwBQ7TqvrFRL4Pwz1WUSVj"
      },
      "credential": {
        "isMember": true
      },
      "signature": {
        "signer": "did:test:z3v8AuaYMjwTFBxqSnCMCq1JQwhMkxwBQ7TqvrFRL4Pwz1WUSVj",
        "signed": "2024-06-26T00:44:29.690Z",
        "hash": "beec6549d4c978f24767a8bf9c8ea5dec202c2c8f3cec0ed4cbd07ce98f1ad19",
        "value":
"2d65e4808685835d11f758bee15a8a9c238d396c265dd98dfd7912085e51a39f5124c29311acabd65e9ca71683e781e7bbfe37a0f5ea2effd3d339ed29b6f37d"
      }
    }
  }
},
"mdip": {
  "version": 1,
  "type": "agent",
  "registry": "hyperswarm"
}
```

AUTHENTICATION Screen

The Auth screen allows a user to issue and/or respond to MDIP challenges. A Challenge DID is entered (or generated) to the Challenge text field; the user can create a Response DID to the provided challenge. The Response to a Challenge will prove to the challenger that the responder controls the private keys of a particular DID.

MDIP Authentication is SECURE, like 2FA because it involves more than 1 channel of communication for authenticating a user. MDIP Authentication is PRIVATE, unlike OAuth

because it does not expose authentication events to 3rd parties.

https://mdip.yourself.dev

Keymaster Wallet Demo

ID: Bob

did:test:z3v8AuaZ8w7HqCC7MXYLmR7vyGFvAhGe9ofL5iZNU9U3UA2bxPq

IDENTITIES

DIDS

GROUPS

SCHEMAS

CREDENTIALS

AUTH

WALLET

Challenge

did:test:z3v8Aua2NQThxkTktrqFsvLixGgQHCj2MChQkTe2uUbLHLJdWe

NEW

Response

did:test:z3v8Auaex2Cufue6ASLLw2q8gukJc54BbrYvEMvk66o7MDePQni

VERIFY

CLEAR

WALLET Screen

The Wallet screen allows a user to backup their wallet. 3 different backup/restore paths are provided:

- Download / Upload of a wallet to/from local storage
- Recover a wallet keys from 12-words mnemonic
- Restore a wallet content from an encrypted on-network backup

https://mdip.yourself.dev

Keymaster Wallet Demo

ID: Bob

did:test:z3v8AuaZ8w7HqCC7MXYLmR7vyGFvAhGe9ofL5iZNU9U3UA2bxPq

IDENTITIES

DIDS

GROUPS

SCHEMAS

CREDENTIALS

AUTH

WALLET

NEW...

IMPORT...

BACKUP

RECOVER...

SHOW MNEMONIC

SHOW WALLET

DOWNLOAD

UPLOAD...