Ethereum Decentralized Digital Identity

Ethereum as an open trusted identity provider

InTech
POST LUXEMBOURG Group

Hello!

I AM FABRICE CROISEAUX

CEO @ InTech, LUX
Chairman of the Board @ Infrachain, LUX

@fXzo

InTech
POST LUXEMBOURG Group

Hello!

I AM ANTOINE DETANTE

Blockchain architect @ InTech, LUX

@antoined

1.
Current state about digital identity

How is digital identity managed today?

Strong Identity
Digital certificates and PKI

- Compliant with EIDAS and accepted by any court as a proof
- X509 Certificates holds identity attributes and keys to prove the ownership
- Trusting the identity implies:
  - Trusting the certification process
  - Trusting the keys management process
  - Trusting the underlying technology

PKI are not flexible

- Tech complexity
  - TLS mutual auth. not widely used, alternative solutions are vendor specific
  - Complex to install and to use by end users
- Centralized
  - Importance of CAs, risks of failure or unavailability
- Expensive
  - Costs of certificate emission or renewal, service fees

Big players as identity providers

- Google, Apple, Facebook, ... have a lot of identity data
- They place themselves as Identity Provider
- Provide authentication services for third parties

Public identity providers drawbacks

- No shared identity between providers: not *really* single-sign on
- No validation of identity data
- Still a centralized model!
  - Censorship, resilience, ...

Blockchain based solutions

Ethereum Decentralized Digital Identity Trust Services

	PKI	Social Networks	EDDITS
Asymmetric cryptography	✔		✔
Strong Security	✔		✔
Ease of use		✔	✔
Deployed Everywhere		✔	✔
EIDAS Compliant	✔		✔

2.
A decentralized identity provider

Identity federation on Ethereum

What we need?

- An identity support, publicly accessible
- A way to request, store, verify identities attributes
- Strong authentication to prove identities ownership
- Standard SSO protocol

ERC-725 & ERC-735

- ERC-725 “Identity”
  - Standardized identity on Ethereum
  - Holds keys by purposes (management, actions, ...)
  - Act as a proxy (in chain) and as an unique identifier (contract address)
- ERC-735 “Claim holder”
  - Holds claims about an identity
  - Allows third parties to add claims

Claim issuers

- Link a digital certificate (X.509) delivered by a trusted CA to a blockchain identity
- Claim issuer is a Smart Contract, which parse and validate a standard RSA signature
  - using the new modexp precompiled implementation (EIP 198) available since Byzantium fork

Secured ECDSA keys

- Can be hardware wallets (Ledger, ...)
- We are working on a prototype with FIDO UAF authenticators
  - Open standards about 2nd factor auth

ECDSA signed JSON Web Tokens

- JSON Tokens signed by a private key registered in the identity contract
- Use to prove identity to off-chain applications

Building blocks

Identity support

ERC-725 contract per user, deployed in the Ethereum chain.

Standardised protocol (ERC-735) for requesting, adding and verifying claims.

In-chain claim issuer using digital certificates to get user's name.

Strong authentication

Hardware wallets or FIDO UAF authenticator to unlock a key linked to the identity.

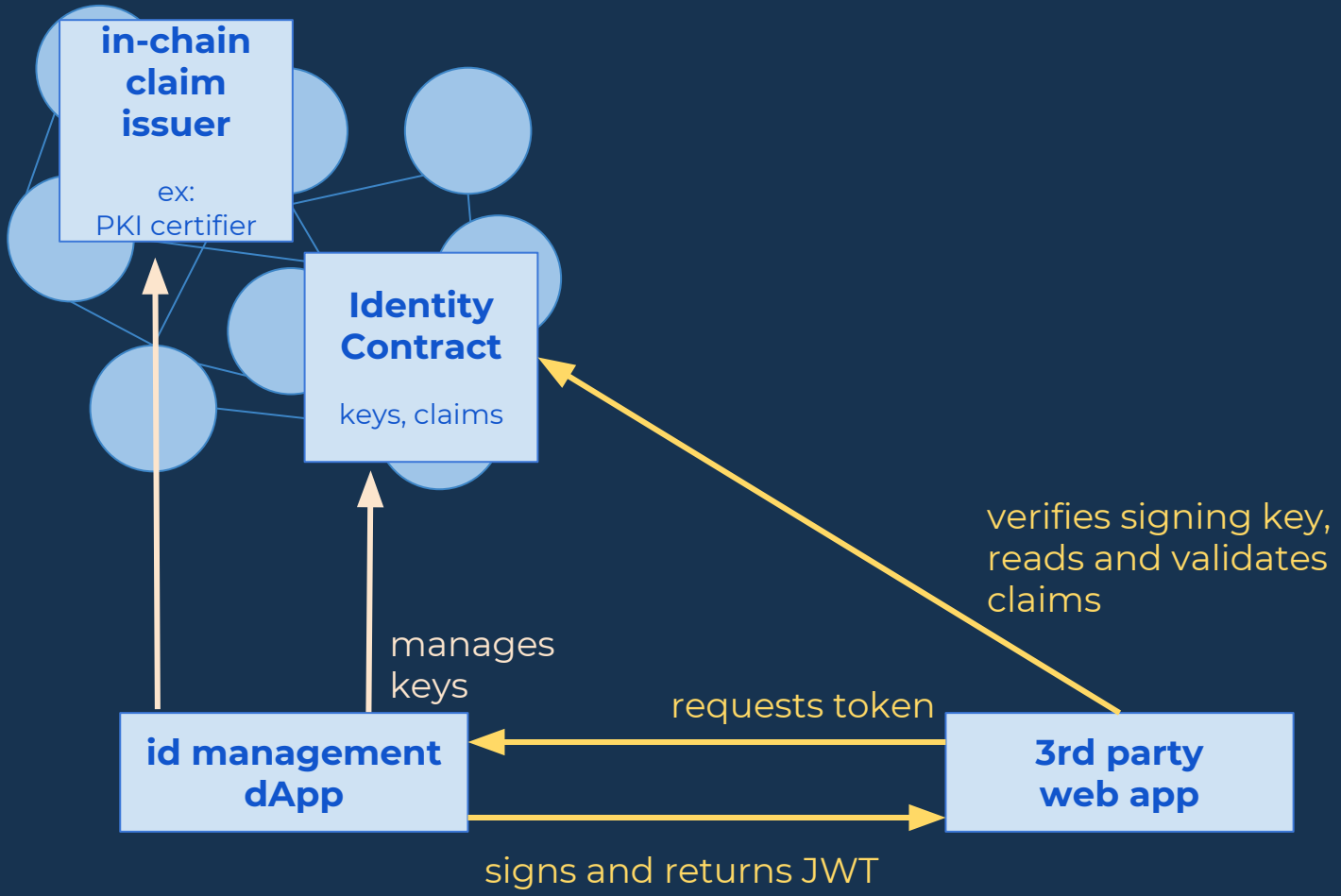
Standard assertions

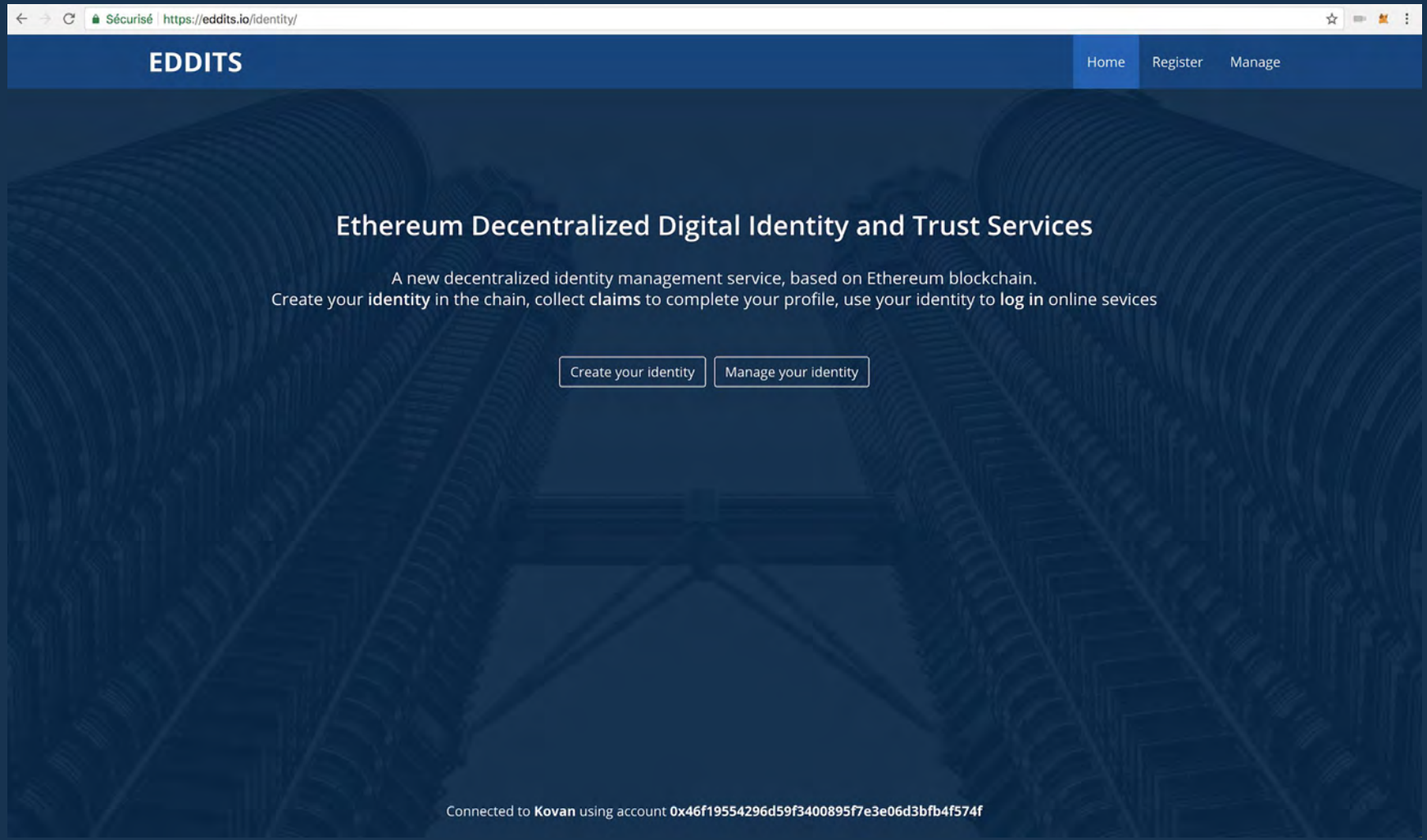
JWT signed with user's key, proving ownership of a key linked to the identity.

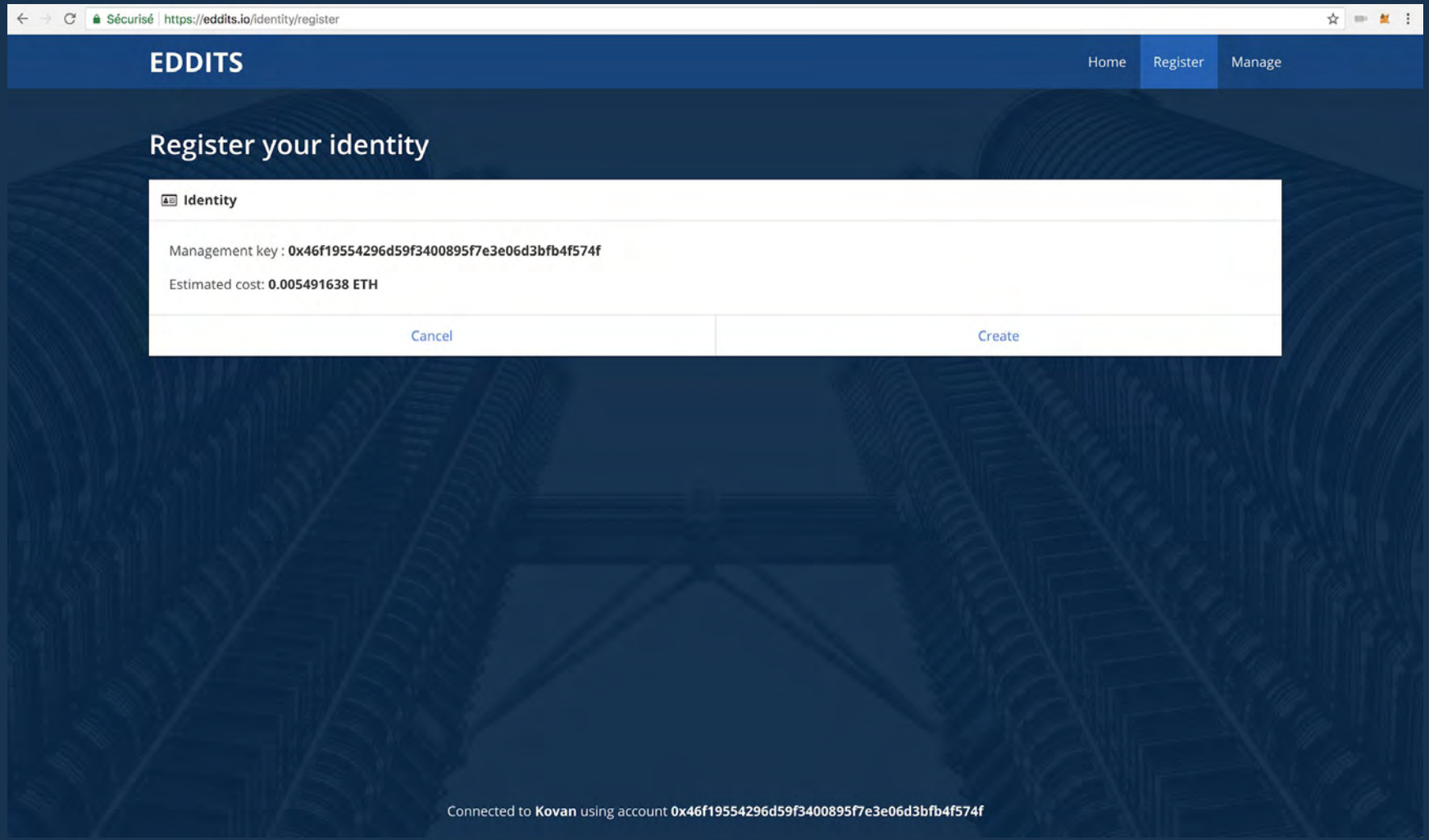
3.

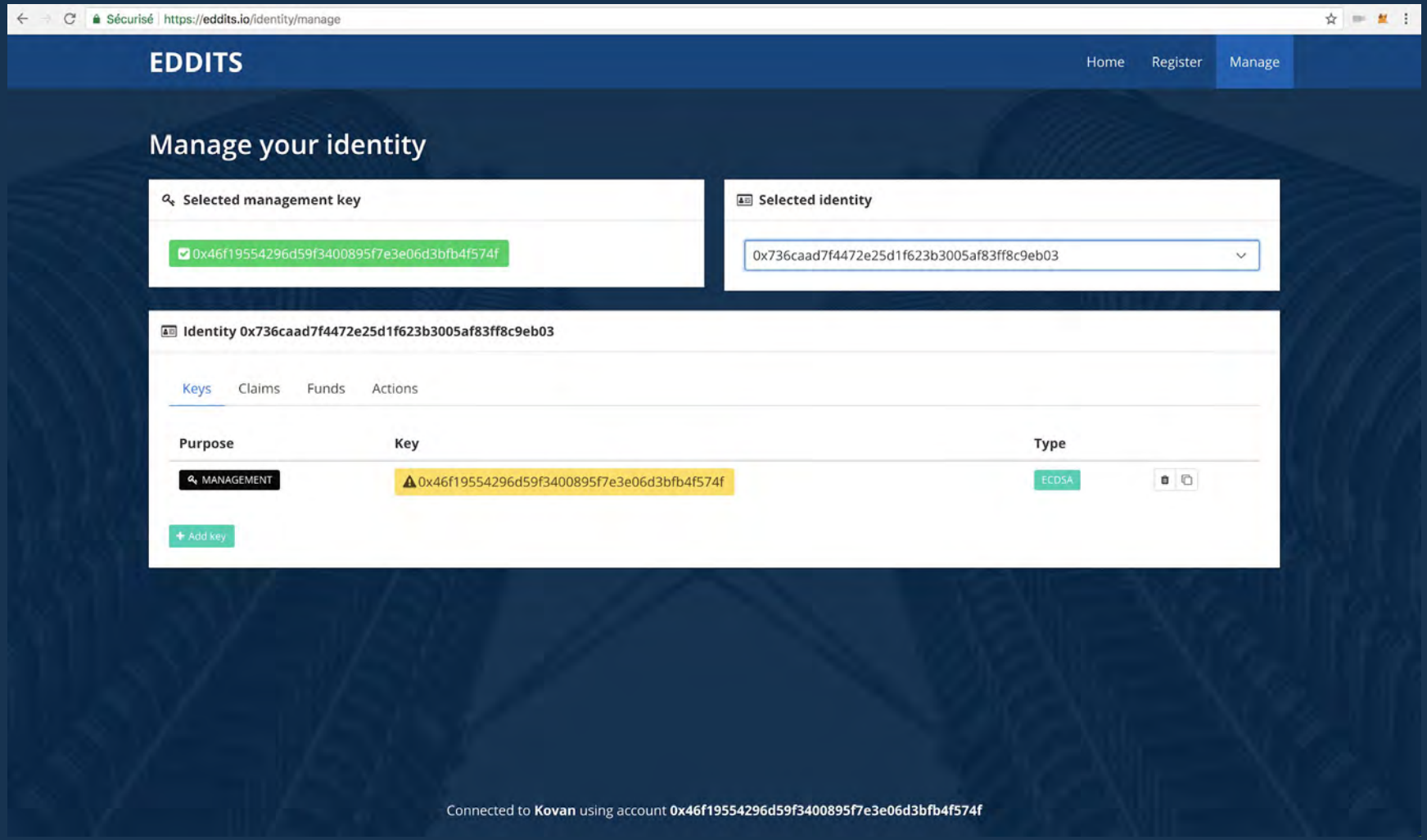
EDDITS Prototype

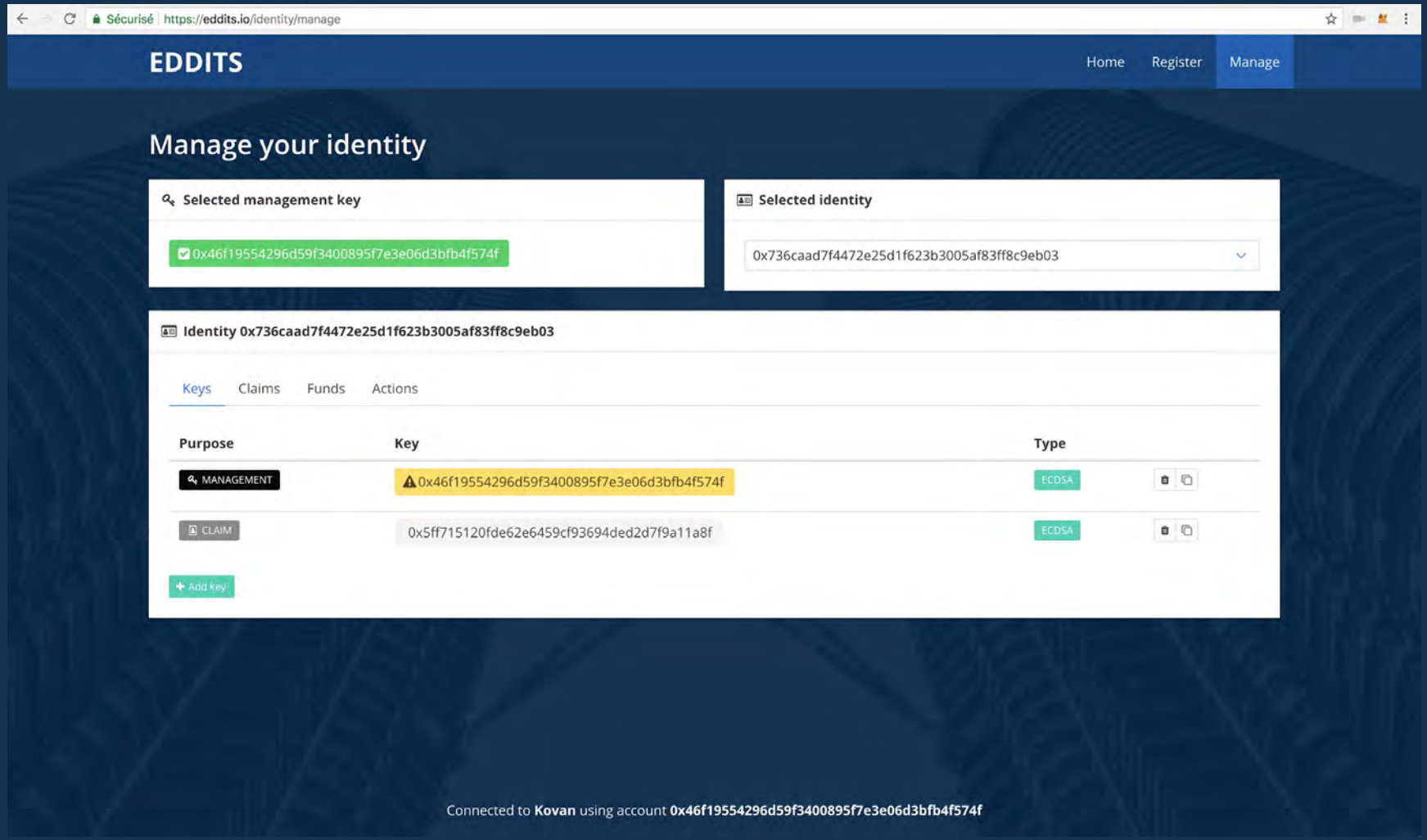
What does it look like?

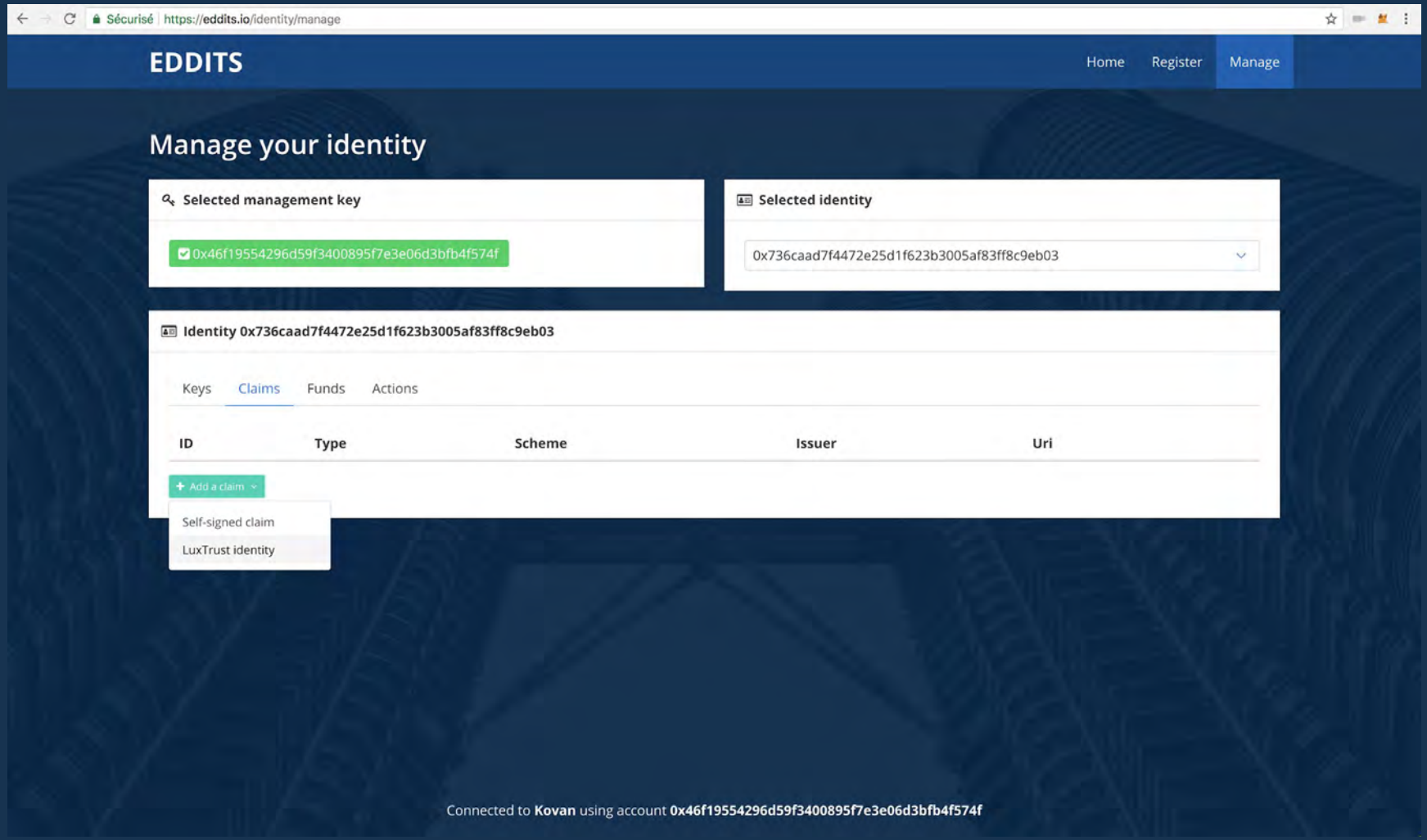

in-chain claim issuer
ex: PKI certifier
Identity Contract
keys, claims
verifies signing key, reads and validates claims
manages keys
requests token
id management dApp
3rd party web app
signs and returns JWT


Sécurisé https://eddits.io/identity/
EDDITS
Home
Register
Manage
Ethereum Decentralized Digital Identity and Trust Services
A new decentralized identity management service, based on Ethereum blockchain.
Create your identity in the chain, collect claims to complete your profile, use your identity to log in online sevices
Create your identity
Manage your identity
Connected to Kovan using account 0x46f19554296d59f3400895f7e3e06d3bfb4f574f


Sécurisé https://eddits.io/identity/register
EDDITS
Home
Register
Manage
Register your identity
Identity
Management key : 0x46f19554296d59f3400895f7e3e06d3bfb4f574f
Estimated cost: 0.005491638 ETH
Cancel
Create
Connected to Kovan using account 0x46f19554296d59f3400895f7e3e06d3bfb4f574f


Sécurisé https://eddits.io/identity/manage
EDDITS
Home
Register
Manage
Manage your identity
Selected management key
0x46f19554296d59f3400895f7e3e06d3bfb4f574f
Selected identity
0x736caad7f4472e25d1f623b3005af83ff8c9eb03
Identity 0x736caad7f4472e25d1f623b3005af83ff8c9eb03
Keys
Claims
Funds
Actions
Purpose
Key
Type
MANAGEMENT
0x46f19554296d59f3400895f7e3e06d3bfb4f574f
ECDSA
Add key
Connected to Kovan using account 0x46f19554296d59f3400895f7e3e06d3bfb4f574f


Sécurisé https://eddits.io/identity/manage
EDDITS
Home
Register
Manage
Manage your identity
Selected management key
0x46f19554296d59f3400895f7e3e06d3bfb4f574f
Selected identity
0x736caad7f4472e25d1f623b3005af83ff8c9eb03
Identity 0x736caad7f4472e25d1f623b3005af83ff8c9eb03
Keys
Claims
Funds
Actions
Purpose
Key
Type
MANAGEMENT
0x46f19554296d59f3400895f7e3e06d3bfb4f574f
ECDSA
CLAIM
0x5ff715120fde62e6459cf93694ded2d7f9a11a8f
ECDSA
Add key
Connected to Kovan using account 0x46f19554296d59f3400895f7e3e06d3bfb4f574f


Sécurisé https://eddits.io/identity/manage
EDDITS
Home
Register
Manage
Manage your identity
Selected management key
0x46f19554296d59f3400895f7e3e06d3bfb4f574f
Selected identity
0x736caad7f4472e25d1f623b3005af83ff8c9eb03
Identity 0x736caad7f4472e25d1f623b3005af83ff8c9eb03
Keys
Claims
Funds
Actions
ID
Type
Scheme
Issuer
Uri
+ Add a claim
Self-signed claim
LuxTrust identity
Connected to Kovan using account 0x46f19554296d59f3400895f7e3e06d3bfb4f574f

Sécurisé https://orely.test.luxtrust.com/FederatedServiceFrontEnd/saml/dss/req

FR

LUXTRUST

SÉLECTIONNEZ VOTRE DISPOSITIF


Token

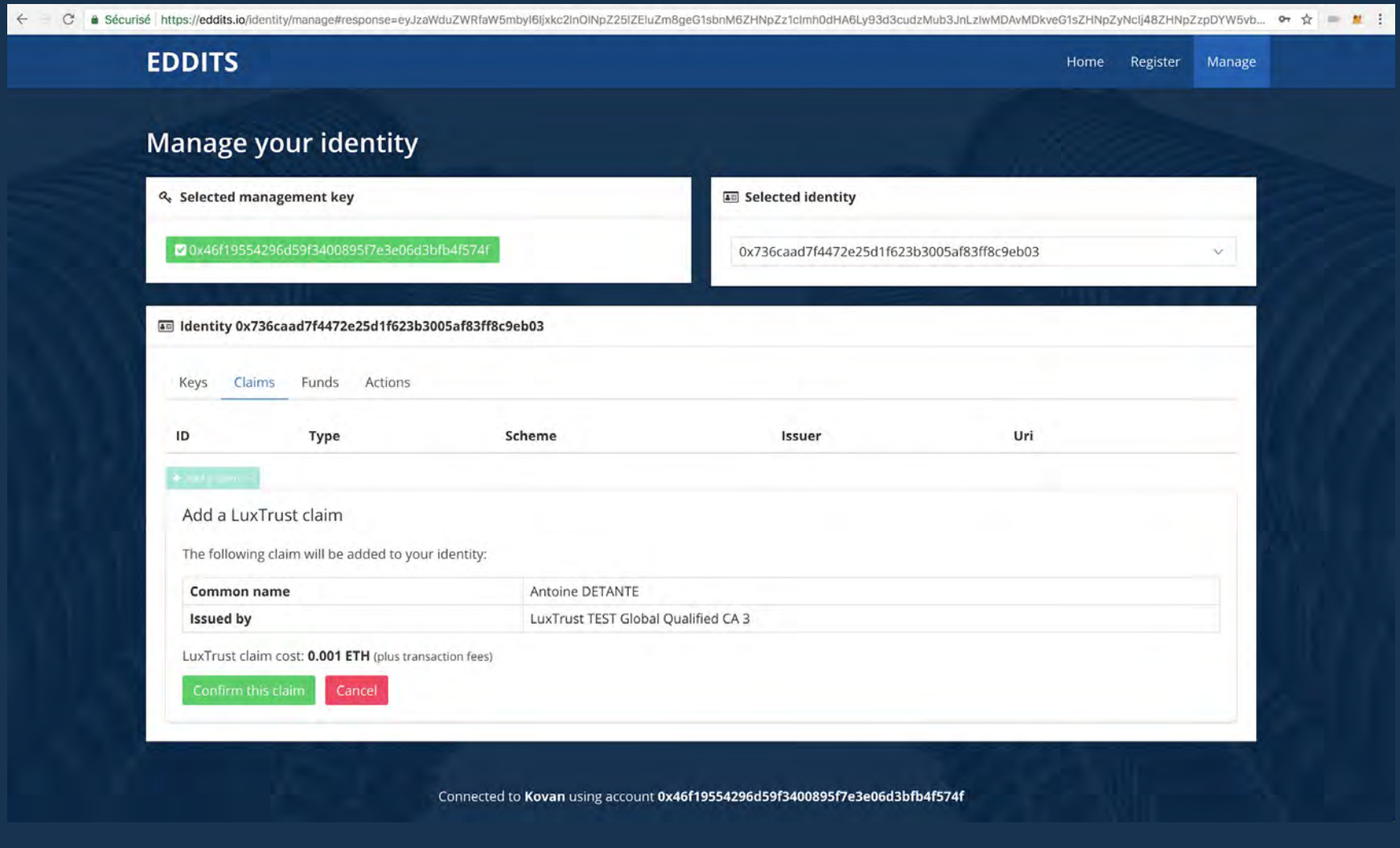

Smartcard

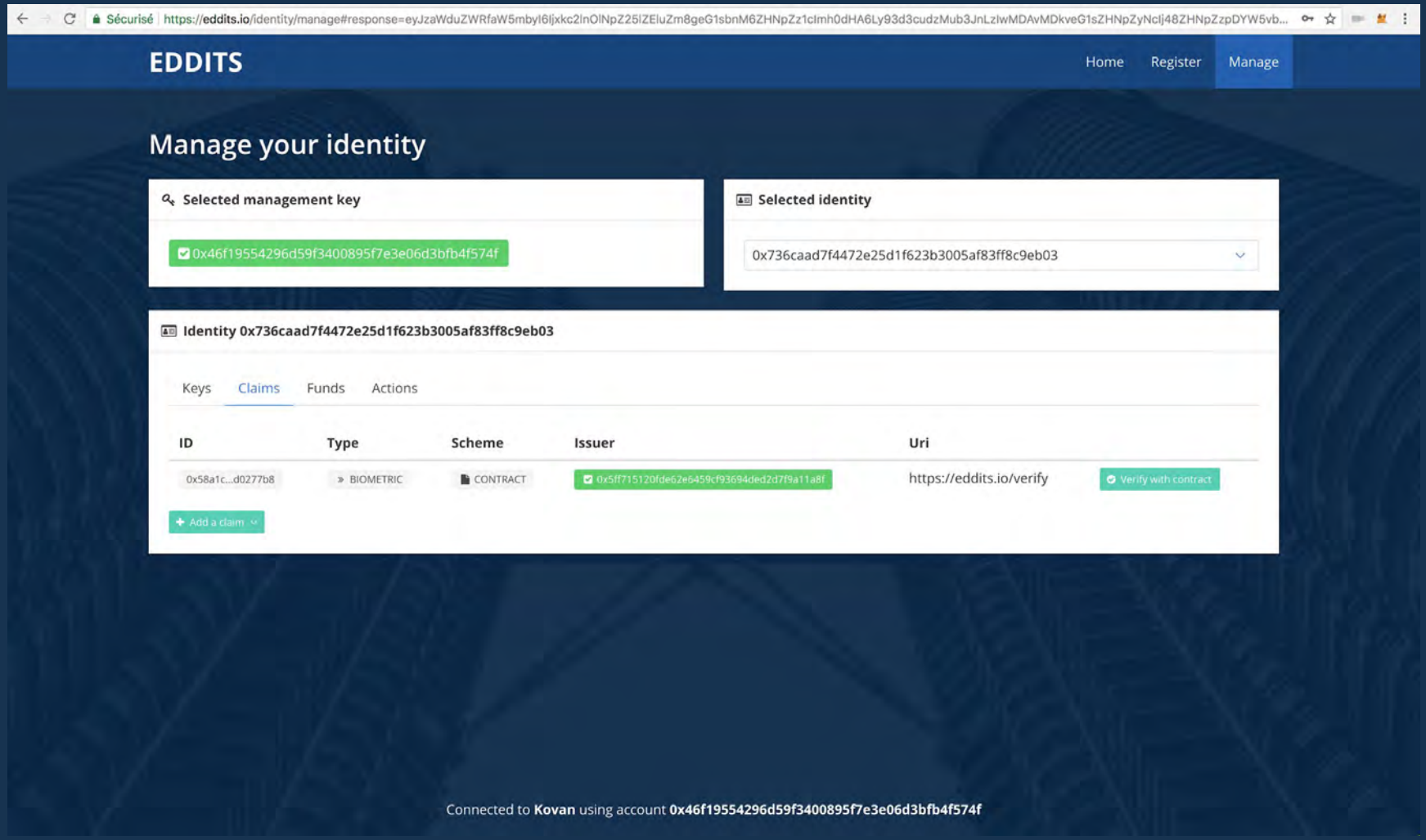

Signing Stick

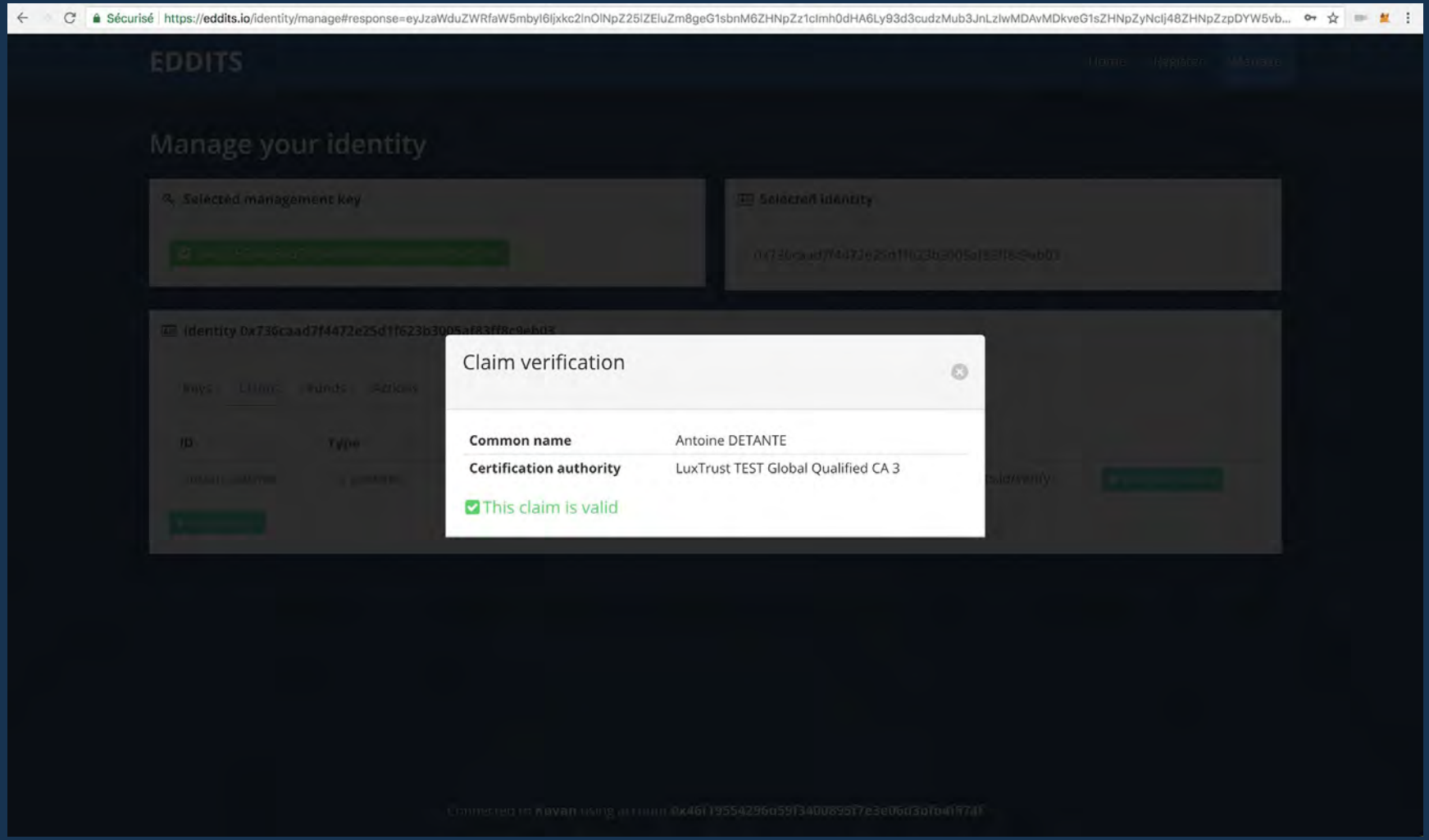

Carte d'identité


LuxTrust Scan


LuxTrust Mobile


Sécurisé https://eddits.io/identity/manage#response=eyJzaWduZWRfaW5mbyI6IjxkC2lnOlNpZ25lZEluZm8geG1sbnM6ZHNpZz1clmh0dHA6Ly93d3cudzMub3JnLzIwMDAvMDkveG1sZHNpZyNclj48ZHNpZzpDYW5vb...
EDDITS
Home
Register
Manage
Manage your identity
Selected management key
0x46f19554296d59f3400895f7e3e06d3bfb4f574f
Selected identity
0x736caad7f4472e25d1f623b3005af83ff8c9eb03
Identity 0x736caad7f4472e25d1f623b3005af83ff8c9eb03
Keys
Claims
Funds
Actions
ID
Type
Scheme
Issuer
Uri
Add a LuxTrust claim
The following claim will be added to your identity:
Common name
Antoine DETANTE
Issued by
LuxTrust TEST Global Qualified CA 3
LuxTrust claim cost: 0.001 ETH (plus transaction fees)
Confirm this claim
Cancel
Connected to Kovan using account 0x46f19554296d59f3400895f7e3e06d3bfb4f574f


Sécurisé https://eddits.io/identity/manage#response=eyJzaWduZWRfaW5mbyI6IjxkC2lnOlNpZ25lZEluZm8geG1sbnM6ZHNpZz1cImh0dHA6Ly93d3cudzMub3JnLzIwMDAvMDkveG1sZHNpZyNcIj48ZHNpZzpDYW5vb...
EDDITS
Home
Register
Manage
Manage your identity
Selected management key
0x46f19554296d59f3400895f7e3e06d3bfb4f574f
Selected identity
0x736caad7f4472e25d1f623b3005af83ff8c9eb03
Identity 0x736caad7f4472e25d1f623b3005af83ff8c9eb03
Keys
Claims
Funds
Actions
ID
Type
Scheme
Issuer
Uri
0x58a1c...d0277b8
BIOMETRIC
CONTRACT
0x5ff715120fde62e6459cf93694ded2d7f9a11a8f
https://eddits.io/verify
Verify with contract
Add a claim
Connected to Kovan using account 0x46f19554296d59f3400895f7e3e06d3bfb4f574f


Sécurisé https://eddits.io/identity/manage#response=eyJzaWduZWRfaW5mbyI6IjxkC2lnOlNpZ25lZEluZm8geG1sbnM6ZHNpZz1cImh0dHA6Ly93d3cudzMub3JnLzIwMDAvMDkveG1sZHNpZyNcIj48ZHNpZzpDYW5vb...
EDDITS
Manage your identity
Selected management key
Selected identity
identity 0x736caad7f4472e25d1f623b3005af83ff8c9eb03
Claim verification
Common name
Antoine DETANTE
Certification authority
LuxTrust TEST Global Qualified CA 3
This claim is valid

THANKS!

Any questions?

You can find us at:
@fXzo / @antoined
contact@eddits.io

https://eddits.io
(work in progress!)