Security & Privacy, Trustworthiness Perspectives to Secure Data Platforms in a competitive Digital Single Market

Alessandro Amicone

GLOBAL VISION: IoT TODAY AND BEYOND

IOT Week
Dublin — June 20-23, 2022
Promote **INTEROPERABILITY**

ensuring **SECURITY**

and **PRIVACY**
Security

When removing the barriers security must be increased

We need to **know** who wants to access

We can give a **key** to enter and **control** what a person is doing

So we’ll have enough **trust** but...

Are the **benefits** higher then **costs**?
And what about **privacy**?
Privacy

When increasing the security the privacy could be an issue

GDPR compliance for PII (Personal Identifiable Information)

Data Breach risks

Let’s the users own and manage PII and use anonymized credentials to control access to the data
Security & Privacy by design

Blockchain Technology & Self sovereign Identity provides security and trust preserving Privacy

- **Tamper-proof Ledger**: Transactions are recorded in a chain of related blocks and a malicious attack would break the chain integrity.
- **Consensus-based Governance**: Changes to the system must be approved by the majority of participants.
- **Cryptographic keys**: All transactions are signed with Cryptographic keys which provide security and reliability.
- **Verifiable credentials**: All stakeholders are identified by tamper-evident credentials that have authorship that can be cryptographically verified.
- **Non-repudiation protocol**: Data exchanges and payments are made through a P2P communication protocol with cryptographically signed proofs.
I3-Market Solution

As **Data Marketplace** I can have more data to provide to my users

As **Data Provider** I can sell my data on more Data Marketplaces

As **Data Consumer** I can find interesting data on a single Data Marketplace

As **Data Owner** I can give my consent and control data sharing
I3-Market Pillars

Self-sovereign Identity
User-Centric Auth
Explicit user consent
Distributed control
Secure Auditing
SLS Smart Contracts
Crypto payment

Semantic Engine
Standards
Open API

SECURITY
Software Wallet
Hardware Wallet
Verifiable Credentials

PRIVACY
Self-sovereign Identity
User-Centric Auth
Explicit user consent

TRUST
Distributed control
Secure Auditing
SLS Smart Contracts
Crypto payment

INTEROPERABILITY
Semantic Engine
Standards
Open API

I3-Market Backplane
BLOCKCHAIN
I3-Market Identity & Access Management

- HW/SW Wallet
  - Consent sharing
  - Login i3-market
  - Onboard i3-market
  - Accept vc

- OIDC SSI Auth Service
  - Request vc
  - Request access token
  - Verify vc
  - Issue vc

- VC Service
  - Verify vc
  - Issue vc

- Hyperledger Besu

- Onboarding
- Login
I3-Market Login

**Data Marketplace**

**I3Market Auth Service**

Request I3-Market VC

**HW/SW Wallet**

Disclose I3-Market VC

**I3-Market Verifiable Credential JWT**

```
{
    "sub": "did:ethr:i3m:0x03a98f6055a418be6d73b...",
    "verified_claims": {
        "trusted": [
            "eyJhbGciOiJFUzI1NksiLCJ0eXAiOiJKV1QifQ....."
        ],
        "untrusted": []
    },
    "at_hash": "fpphOPsmm-4pp4tcaoqGxp...",
    "aud": "oidcRpAcg_SpaNativeApps",
    "exp": 1644326884,
    "iat": 1644323284,
    "iss": "https://identity1.i3-market.eu"
}
```

**Check Access token**

Access token

```
eyjhbbGcOiJRTQSlisInRScl6kpkXCVlSmtpZCI6ikRkLXwuUJhrZzdVb0lRZG9mXaMmstY3I5M9oyYXRULVESfY3cm8fQ...…….
```

**ID token**

```
eyjhbbGcOiJRTQSlisInRScl6kpkXCVlSmtpZCI6ikRkLXwuUJhrZzdVb0lRZG9mXaMmstY3I5M9oyYXRULVESfY3cm8fQ...…….
```

**Backplane API**

**I3-Market Verifiable Credential JWT**

**I3-Market Auth server**

Check Access token
I3-Market Verifiable Credential JWT

```json
{
    "vc": {
        "credentialSubject": {
            "role": "provider",
            "profile": {
                "name": .....,
                "surname": .....,
                ...
            }
        },
        "@context": [https://www.w3.org/2018/credentials/v1],
        "type": ["VerifiableCredential"]
    },
    "sub": "did:ethr:i3m:0x03a98f6055a418be6d73b6caf6.....",
    "nbf": 1637597151,
    "iss": "did:ethr:i3m:0x2e3592788eb9154914f87e4bb820110...."
}
...
```
Future works

Evaluate integration with EBSI (European Blockchain Service Infrastructure) and ESSIF (European Self Sovereign Identity Framework)

Evaluate the use of eIDAS bridge credentials for Marketplace onboarding
Thank you!

Find more:
https://www.i3-market.eu/