

# DIDroom

## Multistandard Modular SSI Solution

<https://forkbomb.solutions>

November 2023

**FORKBOMB**

:(){ :|:& };;

# Unique value proposition

- Focus on cryptography and interoperability
- 100% Open Source tech stack
- Core component (Zenroom) built in-house with 0 dependencies

# DidRoom:

## Multitenant, multistandard, modular identity solution

- W3C-DID and W3C-VC, eIDAS 2.0 (EUDI-ARF), OpenID4VCI (Verifiable Presentations, relying party, Federation) - maybe EBSI Credentials
- Document signatures PaDES/CaDES/JaDES signature via [DSS](#)
- Cryptography: hashes, sigs (ecdsa, eddsa, Schnorr, Dilithium, Ethereum,) zero knowledge proof (BBS+, Coconut), homomorphic multisig on BLS381
- Ethereum interop (signatures, smart contracts), Fabric interop
- Web, mobile (TEE support), browser extension (JS vanilla, WASM)
- Programmable/extendable in Zencode

FORKBOMB  
:0x:1:8:;:

# Architecture

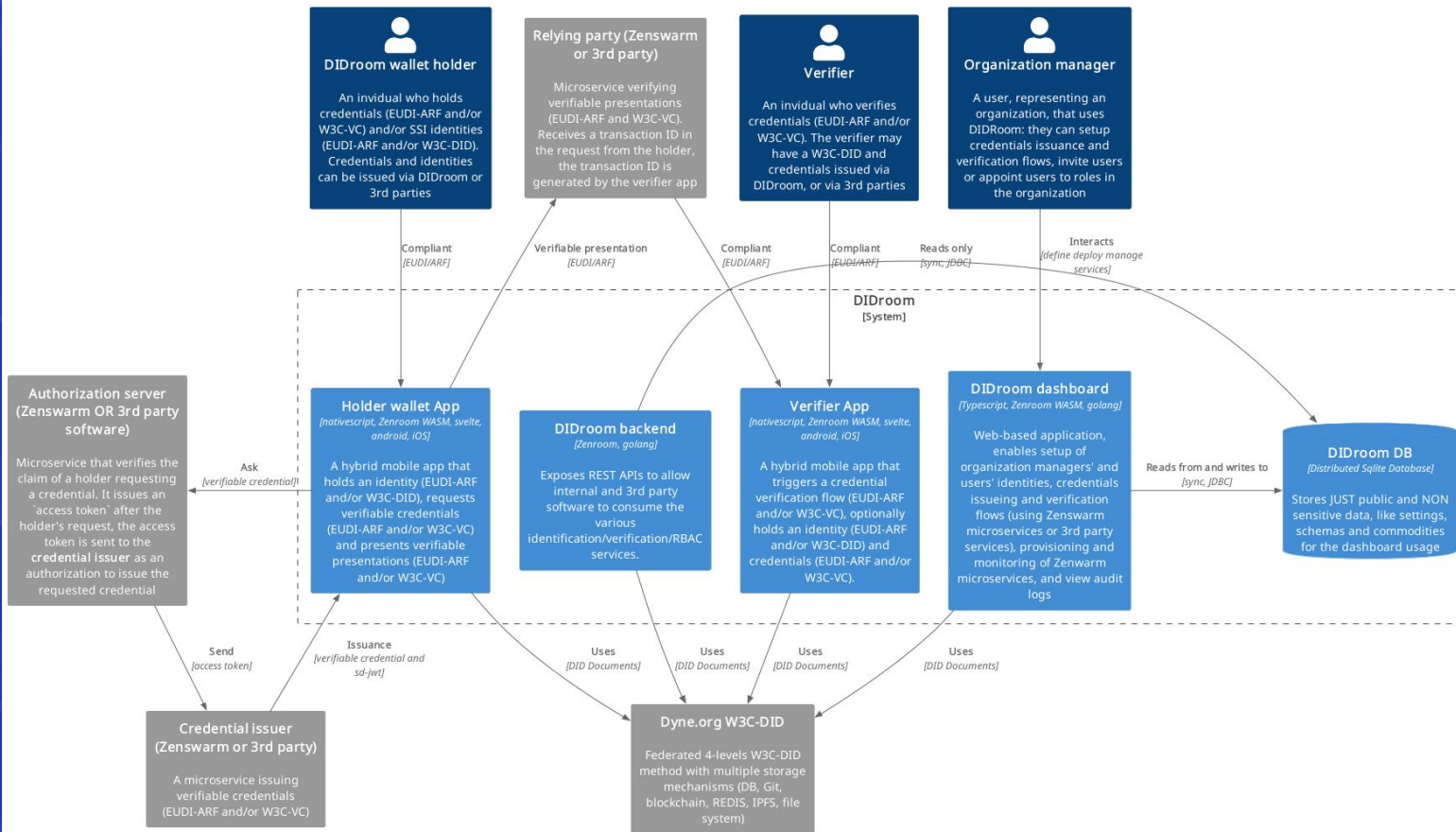
FORKBOMB  
:00:1:8 )::

# Modular, microservice-based

## Multipatform, multipurpose DID/SSI wallet

- Web-based dashboard: Pocketbase, LiteFS, Zenroom/Slangroom/Restroom-mw
  - Setup of issuer and verification flows
  - Provisioning of microservices
  - Users/organization management
  - REST-APIs, logs, auditing, web-hooks
- Microservices for issuance (auth. server and issuer) and verifier (relying party), based on Zenswarm (programmable in Zencode) or 3rd party service (compatible OpenID4VCI)
- DSS back-end for PaDES/CaDES/JaDES signatures
- Mobile app Holder/Verifier: CapacitorJS, Android/iOS with TEE

Container diagram for DIDroom



# Commercialization

FORKBOMB  
:OC :|:8 }::

# Freemium, microservices, integration

- Free plan: 10 users, 3 credentials, 20 credentials/month (TBD), on our Zenswarm iss./ver., standard mob. app
- Paid plan: pay per user/credential/verification (TBD), can use Zenswarm on premises iss./ver. Or 3rd party, white label mob. app
- Solution hosted on premises (Zenswarm or 3rd party for iss./ver.), white labeled mob. app
- Microservices as a service:
  - hosted microservices (setup cost and pay per use)
  - Cloud images (AMI/Azure): pay per use
- Customization, integration with 3rd party software (both platform and microservices)

**FORKBOMB**  
:0{ :|:8 }::



# About Forkbomb BV

- Forkbomb BV (est. 2021) is a spin-off of Dyne.org (est. 2005)
- Team 15 ppl: 12 devs, sysadmins, PM, UX/UI designer
- Dyne.org received ca. 4M EUR in grants and tenders from the EC (DECODE, REFLOW, Ledger, EBSI PCP, Interfacer)
- Dyne.org/Forkbomb software entirely open-source



# Tech stack

FORKBOMB  
:00:1:8 )::

# Identity: W3C-DID/VC, EUDI-ARF, ZKP

- W3C-DID: federated 4-layers DID/SSI implementation ([source](#))
  - did:global:domain.context:12345
  - Multiple storage capabilities
  - Did [explorer](#)
- W3C-VC: native verifiable credentials support in Zenroom
- EUDI-ARF: SD-JWT and ISO 18013-5
- Zero knowledge proof:
  - BBS+: ABC, selective disclosure
  - Coconut: ABC, selective disclosure, blinding at issuance

FORKBOMB  
:0x:1:8 }::

# DID Explorer

<https://explorer.did.dyne.org/>

explorer.did.dyne.org

did:explorer by dyne.org

### DID

A decentralized identifier (DID) is a type of digital identifier that is designed to be self-sovereign, meaning that it is controlled and owned by the individual or entity it identifies, rather than by a central authority. DIDs are created and managed using blockchain technology, which enables them to be decentralized and resistant to tampering. DIDs are intended to be used as a way to identify and authenticate individuals and entities online, in a manner that is secure, private, and interoperable. They can be used to represent a wide variety of things, including people, organizations, devices, and even abstract concepts.

### SSI

Self-sovereign identity (SSI) is a decentralized approach to identity management that empowers individuals and organizations to own, control, and manage their own digital identity, rather than relying on a central authority.

### VC

A verifiable credential (VC) is a digital certificate or token that contains

Search for a DID

← 1 →

- did:dyne:sandbox.test:  
96RTfnQzr7Kc7RbMooHzRV7ckSceCNkoYN3VPv5S5K
- did:dyne:sandbox.test:  
CpnGmMayhGUB1Ag3ZCpJBFjoBqaALZsBiqNFzK2Gh7WV
- did:dyne:sandbox.test:  
G83YCVZNH8aHHAUaVDDdsqyy7KvDcQ1DwxX81AGspSb
- did:dyne:sandbox.test:  
z72Mt4zrxWZ7V1LJDkZFhP4b4SvWbUQVXv1GcJYKV
- did:dyne:sandbox.test:  
AFDw7kqR3DB3SMX8Xwj7TYcYwRhhQQYkzY9FzZYdwR47
- did:dyne:sandbox.test:  
5xXXQx7W2TYM3RU483mjUKEO1wmZGnxKwGwuBL62JGU
- did:dyne:sandbox.test:  
HV4erjgSviWuiQ5ECh1GVVbp3NZr83nn1ZZgTCsLTybz
- did:dyne:sandbox.test:  
B2ugGLSPnscynZKRGCouBoUhwBsynGFzsbhsCul1sQr6W
- did:dyne:sandbox.test:

**VIEW RAW**

```

ID
did:dyne:sandbox.test:AFDw7kqR3DB3SMX8Xwj7TYcYwRhhQQYkzY9FzZYdwR47
DESCRIPTION
sandbox_test_from_js_updated
ALSOKNOWNAS
URL
PROOF
{
  "created": "1678443917078",
  "jws": "eyJhbGciOiJIUzI1NiIsInR5cGU6IjY9FzZYdwR47#cedh_public_key",
  "proofPurpose": "assertionMethod",
  "type": "EcdsaSecp256k1Signature2019",
  "verificationMethod": "did:dyne:sandbox.test_A:DS2dM2NRedWJ5TMUezPJCzjX8FwAL3tBPAPkbtP"
}
VERIFICATIONMETHOD
CONTROLLER did:dyne:sandbox.test:AFDw7kqR3DB3SMX8Xwj7TYcYwRhhQQYkzY9FzZYdwR47
ID did:dyne:sandbox.test:AFDw7kqR3DB3SMX8Xwj7TYcYwRhhQQYkzY9FzZYdwR47#cedh_public_key
PUBLICKEYBASE58 R5ARSQ53u6FodEST6UTRSBy1FP6wucBo1mM5GeBvmYnYmrmP6TmHBU7C8eAA75CNDPAFAnegu
TYPE EcdsaSecp256k1VerificationKey2019

CONTROLLER did:dyne:sandbox.test:AFDw7kqR3DB3SMX8Xwj7TYcYwRhhQQYkzY9FzZYdwR47
ID did:dyne:sandbox.test:AFDw7kqR3DB3SMX8Xwj7TYcYwRhhQQYkzY9FzZYdwR47#reF1ow_public_key
PUBLICKEYBASE58 8EZ514Cz3qH1j3b89m2kxDmdGokcUF6mfgDBk3ymU6jgX8j6z41CbBPPGCLAgasDsigJYzQ8JFme
TYPE ReF1owBLS12381VerificationKey

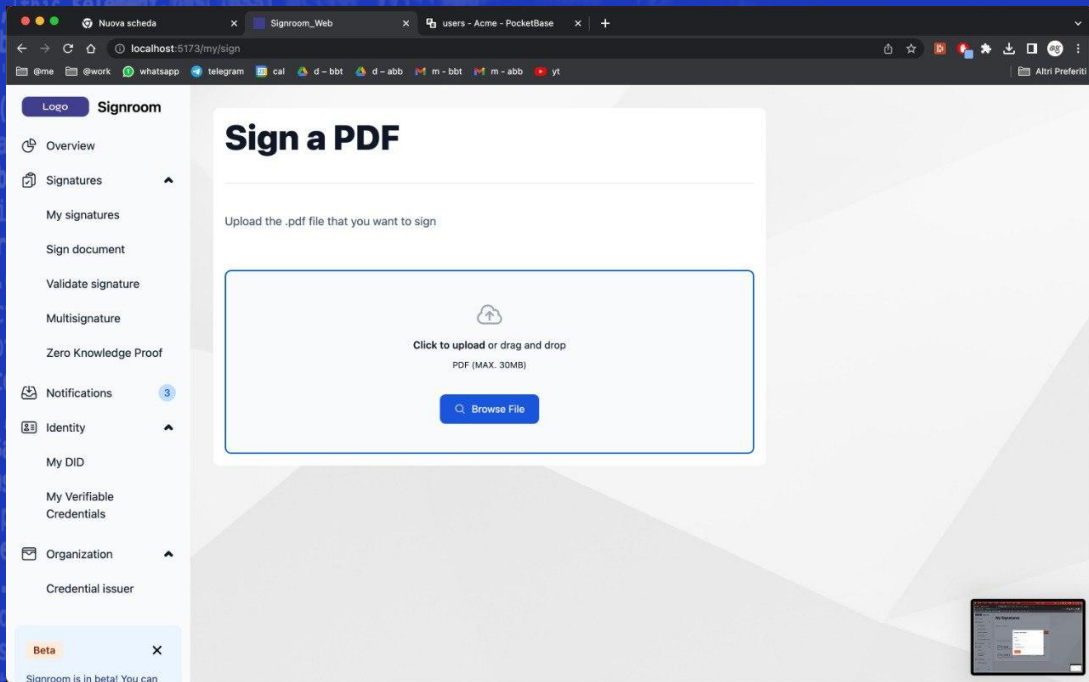
CONTROLLER did:dyne:sandbox.test:AFDw7kqR3DB3SMX8Xwj7TYcYwRhhQQYkzY9FzZYdwR47
ID did:dyne:sandbox.test:AFDw7kqR3DB3SMX8Xwj7TYcYwRhhQQYkzY9FzZYdwR47#btcoin_public_key
PUBLICKEYBASE58 21dEav2KwAaak8SgTbLuwGZPhdjs1zkvPyDBjYzY9CkA
TYPE EcdsaSecp256k1VerificationKey2019

```



# Signroom: customizable DID/SSI back-end

- Modular, white-labeled
- Identity based on W3C-DID
- JSON object signatures (ECDSA, EDDSA, Schnor, BBS, Quantum-Proof)
- PADES, XADES, JADES, CADES for PDF, DOC, img



FORKBOMB  
:O{ :|:8 }::

# Zenroom ecosystem

- Zenroom: cryptographic virtual machine, cryptography, SC, blockchain interop
- Restroom-mw/Slangroom: JS based Zencode extender, wraps Zenroom (WASM)
- Zenswarm: oracles, off-chain cryptography, blockchain interop and computation
- Apiroom: online IDE for Zenroom, rapid microservice creation and deployment
- Zenflows: GraphQL based backend for DPP, end-to-end crypto
- Zenswarm-storage: distributed storage, trusted CDN with signed data

The logo consists of the word "FORKBOMB" in a bold, white, sans-serif font, positioned above a stylized representation of a bomb. The bomb is depicted with a lit fuse and a small flame at the tip, all in white. The entire logo is contained within a dark blue rectangular box with a white border and a slight drop shadow.

FORKBOMB  
:00 :1:8 }::

# Track record

FORKBOMB  
:00:1:8 ::

# Selected Projects

- EBSI PCP
- DECODE, REFLOW (success stories)
- Interfacier



# Selected clients and partners

- European Commission
- Partito Democratico (Italian democratic party)
- Gemeente Amsterdam
- Infocert

# Members of:

- ISO TC/307 (Blockchain standardization)
- Inatba
- NEN (Dutch Standardization Body)
- Rome Call

**Thank you!**

**FORKBOMB**  
:OC:|:8 }::