member LFDECENTRALIZED TRUST webinar

ISBE - Building Europe's First Regulation-Compliant Blockchain Infrastructure on Besu

Miguel Angel Calero Fernández

Executive Director ISBE
Alastria Blockchain Ecosystem

Date: May 13 Time: 7AM PT/10AM ET/16:00 CEST/07:30 PM IST

ALASTRIA

I'm Miguel Calero

Executive Director ISBE @ Alastria

- Expert ISO/CEN-CENELEC
- 5x founder
- 1x exit
- 2x father

miguelcalero@alastria.io
@miguelcalero

isbe

ALASTRIA

Index

/01

Why we built ISBE

How do you unlock blockchain access for the 72% GDP in the EU27?

The need

42%

4,5B€/yr procurement

Public & NIS2 regulated Sectors (P+R)

30%

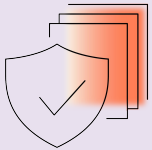
5B€/yr activity

SMEs depending on contracts with P+R

That 72% needs identifiable, auditable and contractible vendors.

Permissionless L1s structurally out

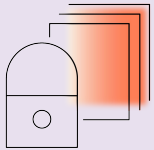
Cyber resilience, digital rights, and sovereignty in one architecture.
Not a market preference — a structural exclusion.



Cyber resilience

"They can't contract anyone"

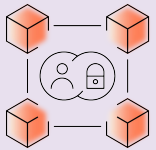
No legal entity means no audit, no contract, no exit strategy.
DORA · NIS2 · Spanish ENS



Digital rights

"They can't guarantee users' rights"

Immutability vs right to be forgotten.
No legal effect of records.
Non-compliant by design.
GDPR · Data Act · eIDAS2



Sovereignty

"They can't trust the infrastructure"

Commercial cloud outside EU jurisdiction. European law cannot reach back.
US Cloud Act

ISBE was built to close this gap

/02

This is ISBE

isbe

ALASTRIA

ALASTRIA

We didn't start with ISBE. We earned it — two networks, seven years, one ecosystem.

ISBE (Infraestructura de Servicios Blockchain de España) is Europe's first public-permissioned blockchain network built with compliance-by-design architecture, developed and operated by Alastria — Spain's national blockchain consortium, comprising over 400 member organizations across 15 nationalities, 19 economic sectors, and 42 public administrations; biggest public - private consortium globally, founded 2017.

T Network
(Quorum)

- **Released January 2019**
- 191 nodes
- **First public - permissioned** blockchain globally.

B Network
(Hyperledger Besu)

- **Restarted in early 2022**
- 49 regular nodes
- Inspiring European EBSI network and the Latin American LACCHAIN network.

Public - Private effort

3 Spanish regions

+30 Companies

+190 Blockchain people

90k Hours

10 Months

... and an undisclosed amount of coffee

New additions:

+3 European Regions

What’s ISBE

Public-permissioned blockchain infrastructure built in Spain for European use cases.

Operated by Alastria.

Runs on Hyperledger Besu — unmodified, Linux Foundation. QBFT consensus, immediate finality, no reorgs.

Backed by the Community of Madrid. Operates within the Alastria ecosystem — Spain's national blockchain consortium.

First infrastructure in Europe positioning as Qualified Distributed Ledger under EU Regulation 2025/2531.

Network Type	Public-permissioned, sovereign
Client	Hyperledger Besu (Linux Foundation)
Consensus	QBFT — Byzantine Fault Tolerant, PoA
Smart Contracts	EVM-compatible · Solidity
APIs	JSON-RPC · EBSI-compatible
Regulatory	qDLT under EU Reg. 2025/2531

Core capabilities

01 INSTITUTIONAL GOVERNANCE

Public - private governance, explicit anti - capture safeguards

02 COMPLIANCE BY DESIGN

Natively engineered for MiCA, GDPR, NIS2, ENS and DORA, plus eIDAS2 QEL

03 NETWORK OF NETWORKS

Bare (qDLT) + Main + build your own

04 FILTERING PROXY

GDPR logical deletion, global kill switch

05 DIGITAL IDENTITY FRAMEWORK

did:isbe, EBSI - compatible, trust registries, business wallet & credentials

06 SMART CONTRACT GOVERNANCE

Diamond Pattern (EIP - 2535), RBAC, pause, conformance audits

07 NETWORK OPERATOR

Institutional procurement - compatible contracts, responsible for compliance & management

08 INSTITUTIONAL GAS TOKEN

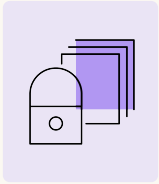
MiCA exempt utility token, Euro - denominated tiers, only served to identified accounts

09 MARKETPLACE & ECOSYSTEM

Network & Service Providers, Partners, Solutions & Infrastructure providers

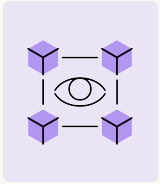
Strategic Pillars

ACTIVE



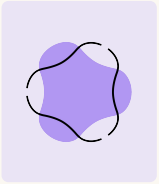
Evidence certification

ACTIVE



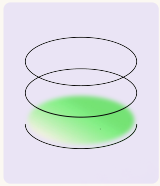
Verifiable business logic

ACTIVE



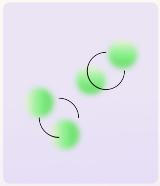
Trust registries

EARLY STAGE



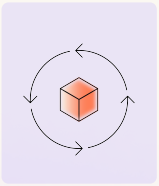
Digital Money

EARLY STAGE



RWA Tokenization

EMERGING



Permissioned DeFi / TradFi

Value Levers (The accelerators)

These are the value levers we are activating for the ecosystem.

- ➔ European Digital Sovereignty
- ➔ QEL as Qualified Service
- ➔ Standardised Interoperability Profile
- ➔ Privacy Framework
- ➔ Stablecoin Issuer

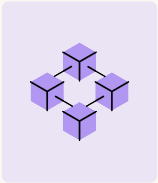
/03

Architecture

isbe

ALASTRIA

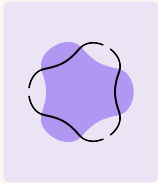
Dual network



Bare Network

Qualified Electronic Ledger

Curve:	secp256r1 / P-256 (ENISA)
Custody Key:	On-premises HSMs — CC EAL4+
Regulation:	EU Reg. 2025/2531 / eIDAS 2
Use Cases:	Evidence · Identity · Trust registries
Legal Effect:	Court-presumed data integrity



Main Network

EVM Compatibility Layer

Curve:	secp256k1 (Ethereum standard)
Tooling:	Hardhat · Foundry · Metamask
Languages:	Solidity — no changes
Use Cases:	Tokenization · DeFi · Smart contracts
Modification:	Besu unmodified — upstream patches

Why Hyperledger Besu

Six properties of the Besu QBFT stack that make it the right substrate for regulated workloads

- ➔ **Deterministic finality**
  no probabilistic re-orgs. Regulators don't accept maybe-final blocks.
- ➔ **Byzantine Fault Tolerance:**
  the network keeps producing blocks while up to one third of validators fail.
- ➔ **EVM-compatible**
  full Ethereum tooling, libraries and developer ecosystem.
- ➔ **Permissioned validator set**
  operated only by accredited entities under the ISBE Adhesion Agreement.
- ➔ **Open source**
  upstream in the Hyperledger Foundation, governed in the open.
- ➔ **Production-tested**
  running across European pilots and public-sector deployments.

Performance capabilities

2s
Block time

FIFO
Strict ordering

2/3+
Supermajority

0
Reorgs. Ever.

QBFT deterministic finality.

No probabilistic settlement.

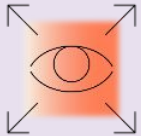
No mempool games.

The blockchain–GDPR paradox

Two fundamental tensions that permissionless chains cannot resolve

Immutability vs the right to be forgotten

Article 17 of GDPR grants data subjects the right to have personal data deleted but blockchain stores data forever.



On-chain transparency vs data minimisation

Article 5 requires that only the minimum necessary data be processed. Public ledgers expose every transaction.

We know how to prevent PII on-chain, how to manage a GDPR breach?

Filtering proxy for GDPR compliance

Every organization running a validator node signs a contract to comply with running the filtering proxy

Client Request
Any app or tool

→

NGINX + Lua Proxy
JSON-RPC interception

→

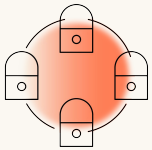
FastAPI Middleware
Rule application

→

On-Chain Smart Contract
Auditable filters

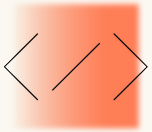
→

Hyperledger Besu
Unmodified node



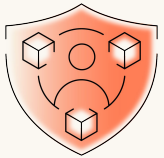
Logical Deletion

Data blocked at API layer — chain integrity preserved. GDPR right to erasure: satisfied.



On-Chain Filters

Filtering rules stored in a smart contract. Auditable, decentralised, tamper-resistant.



No Protocol Fork

Besu runs completely unmodified. Every upstream security patch available immediately.

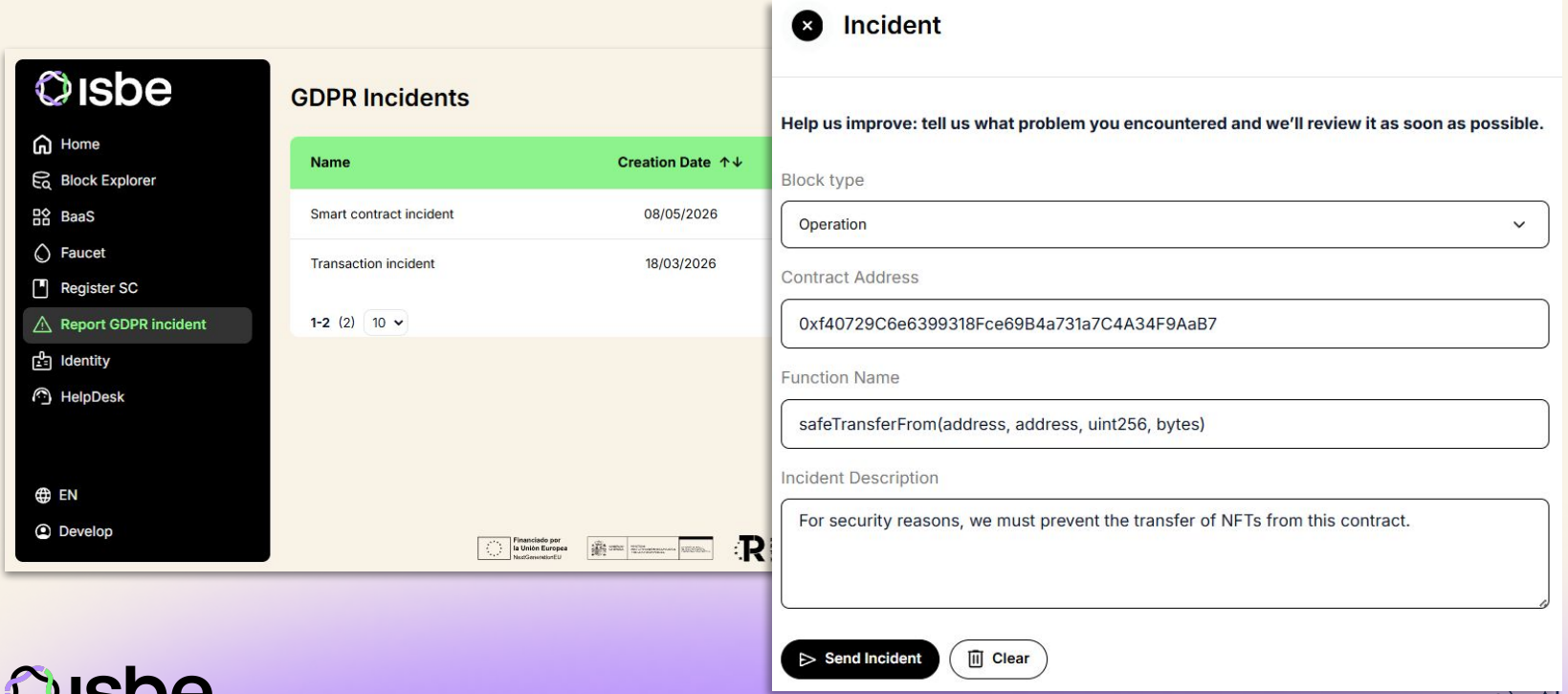
Defence-in-depth at the JSON-RPC layer

The Filtering Proxy smart contract acts as a middleware gate for every JSON-RPC call.
Filtering rules are themselves on-chain, auditable, versioned, and governed.

Block-range scoping	eth_getLogs, eth_getBlockByNumber and similar history-reaching calls are constrained to declared retention windows. Closes the historical-query bypass that breaks the right to be forgotten
Storage-slot opacity	When governance registers a redaction filter for eth_getStorageAt, the method is hidden for the affected ranges
Contract-creation policy	Deployment attempts are evaluated against the allowed-issuer list. No unauthorised bytecode reaches the chain
JSON-RPC method allow-list	Only methods relevant to the caller's role respond. Everything else returns a typed error

Breach reporting

GDPR Art. 33 requires breach notification within 72 hours. ISBE has the operator to do it.



Smart Contracts governance

Three deployment models · Five pre-certified templates · No gas fees.

Recommended

01 Diamond Proxy + ISBE Library

EIP-2535 Diamond Pattern.
RBAC + pausability built in.
Pre-certified templates.
Compliance done.
ERC-20 / ERC - 721 / ERC - 3643

Preferential pricing
Lower integration effort

Custom Logic

02 Own Contract Homologated

Your Solidity.
Passes ISBE conformance process (static analysis, tests, audits).
ISBE in PAUSER role.

Conformance levels C / B / A

Highly regulated

03 Deployment As - is

Smart contracts approved by regulators or with high-complexity.
No ISBE PAUSER role.
Filtering proxy panic button.

Regulator - based trust

Smart Contracts requirements

01	**RBAC**	onlyRole (ROLE) on every state-changing function
02	**Pausability**	whenNotPaused · PAUSER role irrevocable by contract owner
03	**Diamond Storage**	Unstructured storage via keccak256 slot — no state vars in facets
04	**Traceability Events**	Every state change emits a fully traceable event
05	**Tests + Static Analysis**	Unit tests · Slither / MythX · Reproducible build required
06	**SUPER_ADMIN_ROLE**	Irrevocable externally — ISBE retains emergency access always

HashTimestamp.sol — canonical ISBE contract

```
// ① RBAC + ② Pausability
function timestampHash(bytes32 _hash)
    external
    whenNotPaused          // ②
    onlyRole(TIMESTAMPER_ROLE) // ①
{
    _timestampHash(_hash); // ④ emits event
}

// ③ Diamond Storage — keccak256 slot
bytes32 constant _SLOT = keccak256(
    "isbe.hashtimestamp.storage");
function _store() internal pure {
    assembly { s.slot := _SLOT }
}

// ⑥ SUPER_ADMIN_ROLE — irrevocable
function revokeRole(bytes32 role, address a)
    public override {
    require(role != SUPER_ADMIN_ROLE, "irrevocable");
    super.revokeRole(role, a); // ⑥
}
```

Decentralized Identifiers in ISBE (did:isbe)

Self-sovereign identity rooted on a regulated chain. The holder controls the keys; the network controls who can run validators.

- ➔ **What a DID actually is**
  A Decentralized Identifier is a public-key-based identifier registered on the chain and resolvable to a DID Document. The DID Document follows the W3C DID Core 1.0 specification. The holder controls the private key; the chain provides public, tamper-evident resolution.
- ➔ **Permissionless registration**
  Any holder can register a DID. Registration is a self-signed transaction, no central authority approves the identity. The chain that backs the registry is permissioned (validators are accredited), but the act of identifying yourself is not gatekept.
- ➔ **Composable with VCs**
  DIDs are the cryptographic anchor for Verifiable Credentials. The credential's subject is a DID; the issuer is a DID; verification reduces to public-key signature checks. No central registry is needed for verification.

Digital Identity Framework

Only legal entities get onboarded

ONBOARDING FLOW

1. **KYB verification**
   Off-chain identity check — legal entity confirmed
2. **Qualified eIDAS certificate**
   Links the organisation to its did:isbe identifier
3. **DID Document on-chain**
   Two keys: secp256k1 (Main) + P-256 (Bare) · alsoKnownAs → eIDAS cert
4. **LEAR Credential issued**
   W3C VC to legal rep — digital power of attorney · EUDI Wallet ARF
5. **Employee Credentials**
   Issued by LEAR to staff · Revoked via Bitstring Status List (privacy-preserving)

WHAT LIVES WHERE

ON CHAIN

- → did:isbe identifier
- → DID Document (dual keys + eIDAS link)
- → Trust registry (Bitstring Status List)

OFF-CHAIN — holder's wallet

- → LEAR Credential
- → Employee Credentials
- → Personal data — never touches the chain

WALLET COMPATIBILITY

EUDI Wallet	Business Wallet (LEAR)	EBSI-compatible

isbe

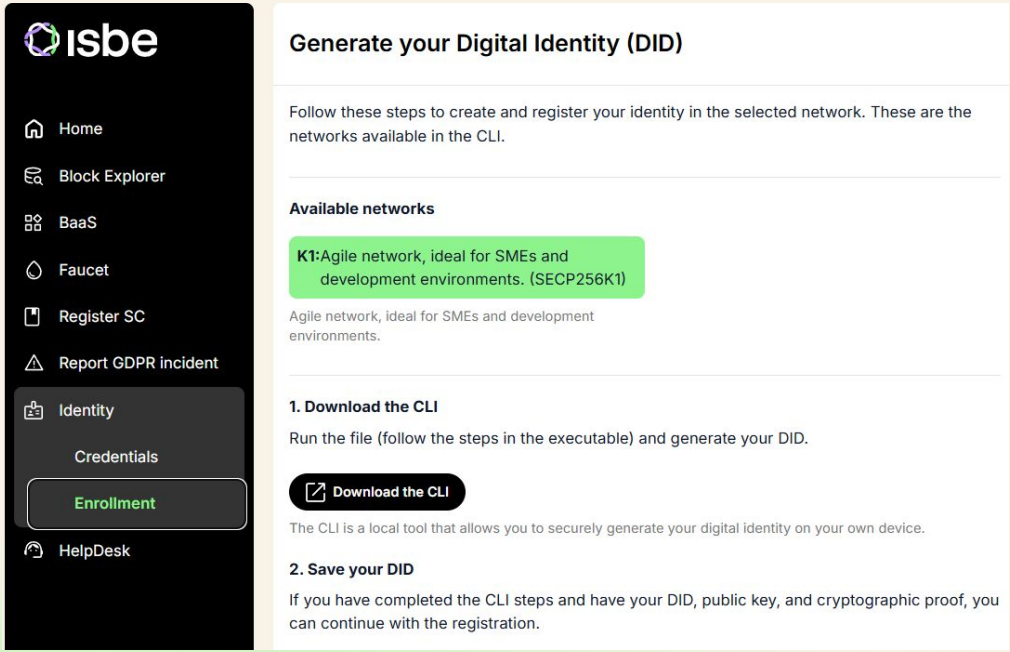
ALASTRIA

DID generation

The holder generates a key pair locally, signs the registration request, and the network records the DID Document.

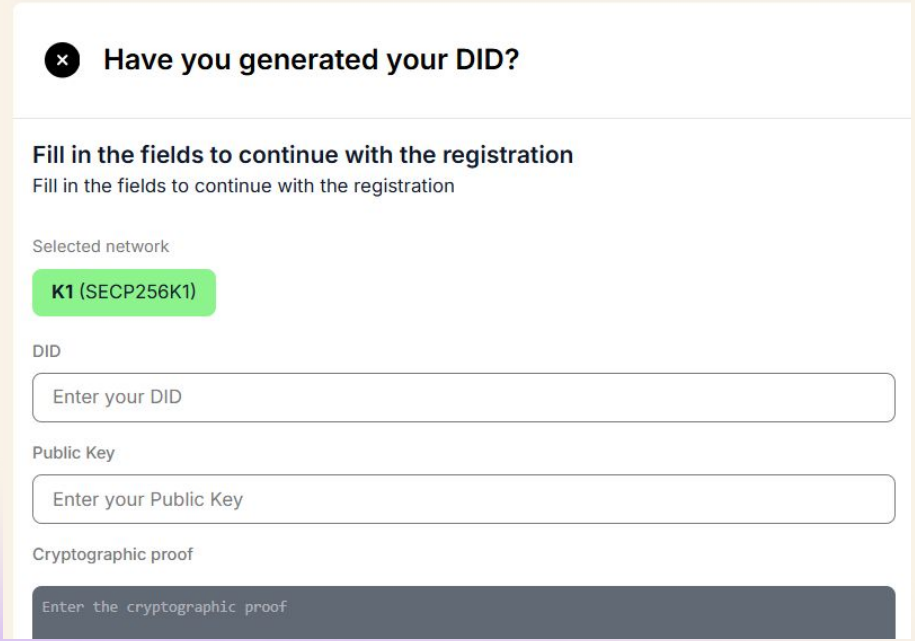
No central authority approves. The chain backing the registry is permissioned; the act of identifying yourself is not gatekept.

Every interaction with ISBE is ready to use DIDs.



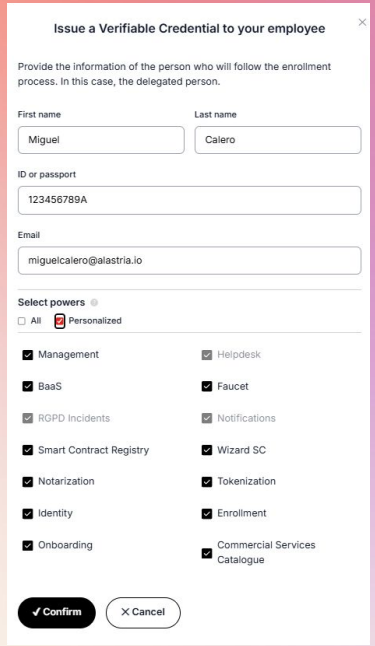
DID registration

```
Private Key (hex):
0x41654e192a3e2084ea93eff98e335cf378837c33f06a794c3edf7f7d117811f6

Public Key (hex):
0x047a2dfea0da6f613f12be05bef0c15225b00807bee0918b54ea995f9a9a408665bd068f33a5a48d2c

Private Key (JWK):
{
  "kty": "EC",
  "crv": "secp256k1",
  "alg": "ES256K",
  "x": "ei3-oNpvYT8SvgW-8MFSJbAIB77gkYtU6plfmppAhmU",
  "y": "vQaPM6WkjSx0pkWKM9UkUMxg-W1jHeYmqfQI62aBx8Y",
  "d": "QWVOGSo-IITqk-_5jjNc83iDFDPwanlMPt9_fRF4EfY"
}

Public Key (JWK):
{
  "kty": "EC",
  "crv": "secp256k1",
  "alg": "ES256K",
  "x": "ei3-oNpvYT8SvgW-8MFSJbAIB77gkYtU6plfmppAhmU",
  "y": "vQaPM6WkjSx0pkWKM9UkUMxg-W1jHeYmqfQI62aBx8Y"
}

PS C:\Users\velae\Downloads\isbe-identity-did-gen-2.0.0\isbe-identity-did-gen-2.0.0>

DID:
did:isbe:uc:z1ewX92nb9K8hvKLxhL3od4fwmhm

Public Key:
0x047a2dfea0da6f613f12be05bef0c15225b00807bee0918b54ea995f9a9a408665bd068f33a5a48d2c

Proof:
0x023650c955176c3b5f6cdbad2480ce6dfc4462f0aa228bca7a206d16f0d6992b33adfead195f2df1b7
```

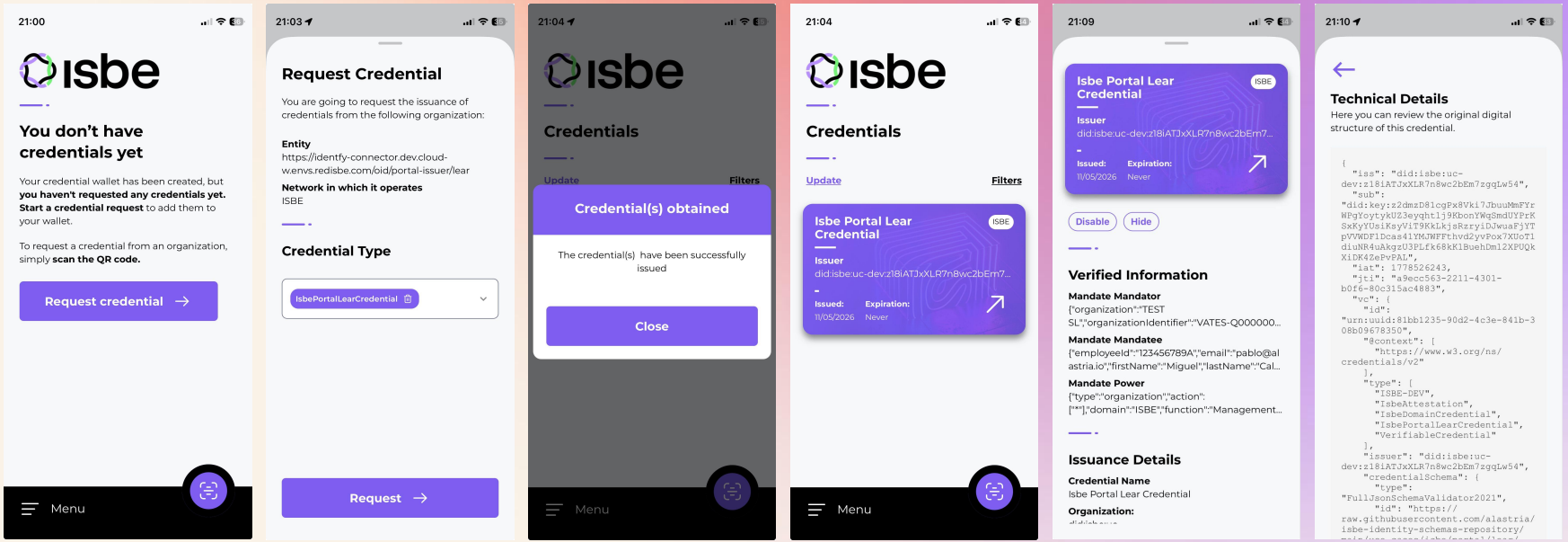


LEAR credentials to access ISBE

The issuer signs a credential bound to the holder's DID. The verifier requests a presentation; the holder reveals only the requested attributes. The verifier checks the signature and resolves revocation status against the chain.

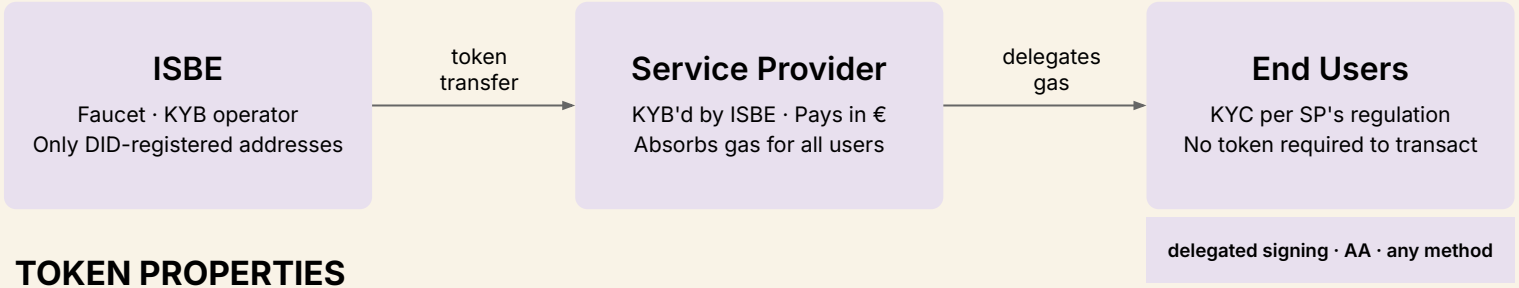


LEAR credentials to access ISBE



Institutional native token

Cost predictability meets strict auditability. Built for institutional procurement.



TOKEN PROPERTIES

Pure gas utility
Not a financial instrument

Non-refundable
Consumed on execution

Fixed value
No price volatility

Not listed
No exchange, no speculation

Liability attribution by design
Token transfers only flow from ISBE's faucet to DID-registered addresses. Every on-chain transaction is attributable to a KYB'd Service Provider. In case of malicious use, ISBE can identify the responsible SP immediately — and has the tools to act: cut the faucet, pause contracts, activate address-level filtering.

/04

Ecosystem

isbe

ALASTRIA

Who builds on ISBE

All intermediaries. ISBE never sells to end users.

Builders

Tech companies & startups building products on ISBE to sell to third parties.

Digital identity · RegTech · Wallet providers · Asset tokenisation · DeFi for regulated markets

- → Accelerate time-to-market for regulated use cases
- → Pre-certified templates — compliance done
- → Cost predictability — no gas fees
- → Access EU institutional markets without extra requirements

Web3 Adopters

Corporations & public bodies deploying blockchain for internal or sectoral use.

Banking · Insurance · Logistics · Energy · Healthcare · Public administration

- → GDPR, NIS2, DORA, MiCA, ISO27001 compliance
- → OPEX vs CAPEX — no infrastructure to own
- → Sovereign, audit-ready, institutional-grade
- → TCO lower than building own compliant infra

Ecosystem Leaders

Public administrations & institutions building shared infrastructure for their ecosystem.

Regional governments · Sectoral regulators · Public universities · Infrastructure operators

- → Sovereign, compliance-first public infrastructure
- → EU funding programme alignment
- → Interterritorial interoperability
- → Governance participation in the network

Network Providers

Territorial operators running validator nodes — clients and distribution channel simultaneously.

Regional tech operators · Public-private digital consortia · Sovereign cloud operators

- → Consolidated ecosystem
- → Revenue model on top of the network
- → Governance rights in ISBE

Partners & Ecosystem

Web3 Natives

Co-builders & technical distributors.

Reach audiences traditional integrators don't.

Solutions Integrators

Enterprise IT consultancies.

Bring clients with identified need and budget.

Regulatory Enablers

Law firms / consultancies (eIDAS 2, MiCA, DORA).

Prescribe ISBE before competitors enter.

Investors & Builders Networks

VCs, accelerators.

One fund = 10–30 portfolio companies.

Sandbox access as value exchange.

Network Access Providers

Node operators.

Simultaneously client and channel.

Committed capacity, reselling to their ecosystem.

Ecosystem Solutions

Partners from the Alastria network with solutions built on ISBE

Solution Partners bring ISBE inside their own institutional product

Qualification-based: active solution, institutional pipeline, certified agreement

Infrastructure Partners

Providers with a bidirectional commercial relationship with ISBE

They position ISBE as their blockchain layer for shared institutional clients

Governed by mutual co-reference rights, not revenue share

/05

Service model

isbe

ALASTRIA

Predictable cost. No gas volatility.

CFOs can anticipate TCO from day one.

Blockchain as a Service	Setup fee Network availability fee Transaction bundles fee
Trust Framework & Registries	Setup fee Registry availability fee Operation bundle fee
Network Access Provider	Execution, Archive & Validator node Committed capacity with distribution rights
qDLT / QTSP	Bare Network QTSPs / TSPs HSM required

Thanks for your attention!

https://redisbe.com/

isbe

ALASTRIA

Thanks for your attention!

https://redisbe.com/

Linkedin
@redisbe

Facebook
red ISBE

Instagram
@red.isbe

X
@REDISBE

isbe

ALASTRIA