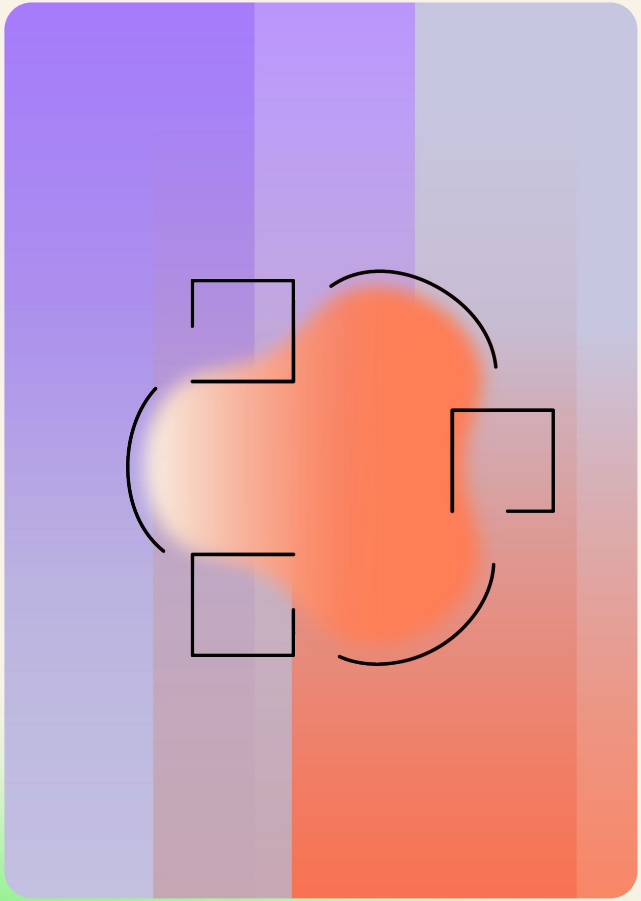
isbe Infraestructura de Servicios Blockchain de España

Confidential and Accountable: Privacy Requirements and Open Questions from Europe's First Qualified DLT



Miguel Calero
miguelcalero@alastria.io

I'm Miguel Calero

Executive Director ISBE @ Alastria



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

miguelcalero@alastria.io
@miguelcalero

isbe

ALASTRIA

Index

/01 Why we built ISBE

/02 This is ISBE

/03 Qualified Electronic Ledger (aka qDLT)

/04 Architecture

/05 Privacy Framework

/01

Why we built ISBE



11% of world GDP was locked out of blockchain. Until now.

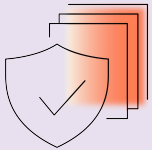
The institutional needs

20%	**PUBLIC SECTOR** 2,6B€/yr procurement
22%	**REGULATED INDUSTRY** 2B€/yr procurement
30%	**SUPPLIERS** 5B€/yr activity

That 72% GDP EU27, 11% globally, needs identifiable, auditable and contractible vendors.

Permissionless L1s structurally out

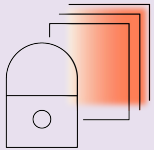
Cyber resilience, digital rights, and sovereignty in one architecture.
Not a market preference — a structural exclusion.



Cyber resilience

“They can’t contract anyone”

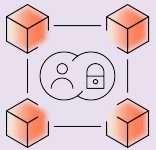
Ledger & EVM are the IT products. No legal entity means no audit, no contract, no exit strategy.
DORA · NIS2



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

This is our “checklist”

README Apache-2.0 license

Ref	Documento
T22	Informe de adecuación al marco legal y cumplimiento regulatorio v2.0
T22-1	Memoria Técnica 1 — Análisis de Interoperabilidad de Redes
T22-2	Memoria Técnica 2 — Análisis de Privacidad en Transacciones
T22-A1a	Anexo 1a — Política de servicio y requisitos de seguridad (QEL)
T22-A1b	Anexo 1b — Lista de conformidad servicio libro mayor
T22-A1c	Anexo 1c — Declaración de Prácticas de Certificación
T22-A2a	Anexo 2a — Directrices generales de cumplimiento
T22-A2b	Anexo 2b — Gestión de Incidentes de Seguridad con datos personales
T22-A2c	Anexo 2c — Cláusulas contrato de encargado
T22-A2d	Anexo 2d — Evaluación de Impacto en Protección de Datos (EIPD/PIA)
T22-A2e	Anexo 2e — Directrices Vinculantes RGPD
T22-A3	Anexo 3 — Análisis ENS (Esquema Nacional de Seguridad)
T22-A4	Anexo 4 — Análisis NIS2
T22-A5a	Anexo 5a — Variables red ISBE
T22-A5b	Anexo 5b — Article 9 (eIDAS2)
T22-A5c	Anexo 5c — Article 56 DORA
T22-A5d	Anexo 5d — Yellowpaper ISBE TKN
T22-A6	Anexo 6 — Análisis Criptoactivos y Tokenización
T22-A7	Anexo 7 — Términos y condiciones
T22-A8	Anexo 8 — RGPD: Evaluación de Impacto en Protección de Datos (EIPD/PIA) v2
T22-A9	Anexo 9 — QEL: Declaración de Prácticas de Certificación

/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 17 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

Backed by Institutions. Built for Institutions.

Some of the companies and institutions behind ISBE

ALASTRIA

2017 Founded

400+ Members

7 yrs Network operations

FINANCIAL INSTITUTIONS

ABANCA · BBVA · CaixaBank · Iberpay · kutxabank · Santander · VISA · Unicaja

PUBLIC SECTOR & INSTITUTIONS

Comunidad de Madrid · Gobierno de Canarias · ICO · Principado de Asturias

CORPORATES, TELCO, UTILITIES...

Campofrío · Iberdrola · Indra · FUJITSU · GENERALI · metrovacesa · repsol · Telefónica

IT CONSULTING & PROFESSIONAL SERVICES

ALTIA · Deloitte. · Globant · gradiant · inetum. · izertis

WEB3 NATIVES

ADHARA · BRICKKEN · CALEA · ioBuilders · ONYZE · TOKEN CITY

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.

Architecture	Network of networks: Bare+Main
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/EUDI - 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

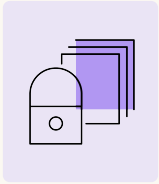
MiCA exempt utility token, Euro - denominated tiers, only served to identified accounts

09 MARKETPLACE & ECOSYSTEM

Network & Service Providers, Partners, Solutions & Infrastructure providers

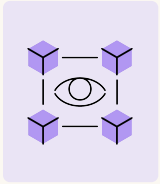
Strategic Pillars

ACTIVE



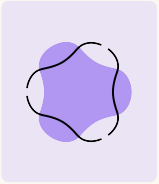
Evidence certification

ACTIVE



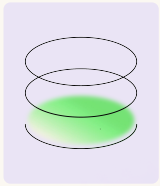
Verifiable business logic

ACTIVE



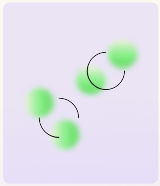
Trust services

EARLY STAGE



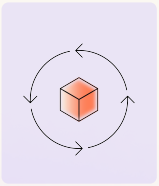
Digital Money

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
- ➔ Stablecoin Issuer
- ➔ Privacy Framework

/03

Qualified Electronic Ledger (aka qDLT)

Why Qualified Electronic Ledger is different

- ➔ **Approved cryptographic algorithms** (secp256r1 / P-256, ENISA list)
- ➔ **ETSI EN 319-compatible digital signature format**
- ➔ **HSM-backed key custody** (CC EAL4+ / FIPS 140-3 Level 3)
- ➔ Guaranteed integrity and uniqueness of **sequential chronological ordering**
- ➔ Delivery through a notified **Qualified Trust Service Provider**
- ➔ ENAC-accredited **conformity assessment** (CEN/TS 18264:2026)

→

- ➔ **Legal presumption** of accuracy and integrity — court-admissible records
- ➔ **Reversal of the burden of proof** — the challenger must disprove
- ➔ **EU-wide legal effect** across 27 member states, no additional agreements
- ➔ **Procurable** by public administrations
- ➔ **Reduced legal and counterparty risk** for regulated use cases

Reg. (EU) 2024/1183 · Impl. Reg. (EU) 2025/2531 · CEN/TS 18264:2026 · December 2025

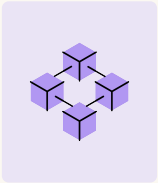
/04

Architecture

isbe

ALASTRIA

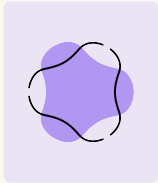
Dual network



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

Performance capabilities

2s
Block time

FIFO
Strict ordering

2/3+
Supermajority

0
Reorgs. Ever.

QBFT deterministic finality.

No probabilistic settlement.

No mempool games.

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

→

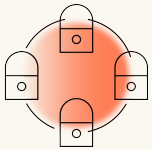
FastAPI Middleware
Rule application

→

On-Chain Smart Contract
Auditable filters

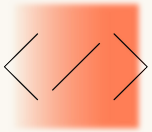
→

Hyperledger Besu
Unmodified node



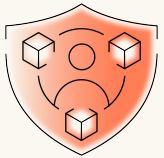
Logical Deletion

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

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
}
```

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

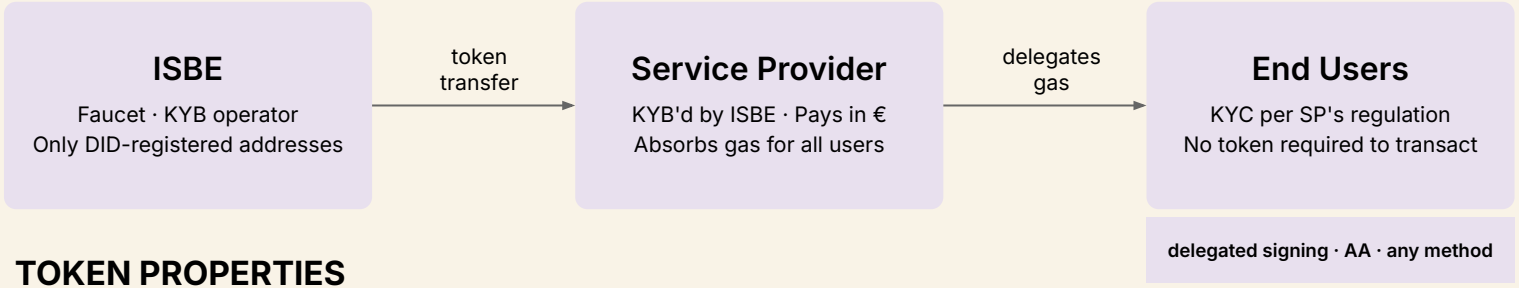
EUDI Wallet	Business Wallet (LEAR)	EBSI-compatible

isbe

ALASTRIA

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.

/05

Privacy Framework

isbe

ALASTRIA

Different threat model, different requirements

	Permissionless	ISBE
Adversary	Anonymous, potentially malicious	Known, identified, legally bound
What to hide	Everything, from everyone	Business data, between specific participants
Regulator	Outside the system	Inside, with controlled visibility
Privacy goal	Anonymity	Inter-participant confidentiality

Collecting requirements

Current requirements

- ➔ Regulated tokens can’t be redesign or redeployed
- ➔ Token holders must not see each other's balances or transaction flows
- ➔ Validators may see transaction data — trusted by governance design
- ➔ Regulator retains full audit capability at all times
- ➔ Confidentiality must not compromise the kill switch or GDPR erasure
- ➔ Must not require modifications to the Hyperledger Besu client

Aspirational

- ➔ Confidentiality as a service capability — not a token or contract design choice.
- ➔ Any transaction, any contract, any time. Opt-in. No redesign required.
- ➔ Beyond tokens: evidence, trust registries, business logic — all eligible.

Solutions under evaluation beyond status quo

PALADIN
Programmable Privacy

Notary + ZKP

- → Native Besu
- → Apache 2.0
- → LF DT ecosystem
- → Designed for regulated institutional tokens

- → Node per participant required in current architecture
- → Waiting for multi-tenant Privacy Groups (Pente)

ZAMA

FHE

- → Strongest cryptographic guarantee
- → ERC-7984 as emerging token standard
- → Relevant for EMT confidentiality layer

- → On-prem coprocessor deployment needs evaluation
- → Application beyond tokens unclear
- → External dependency even in on-prem mode

iExec

TEE (Intel TDX/SDX)

- → Full control over on-chain and off-chain data confidentiality
- → Directly applicable to EMT and RWA token confidentiality
- → Selective disclosure model aligns with ISBE's requirement

- → RLC token dependency
- → Besu permissioned deployment needs evaluation
- → On-prem deployment model needs validation for ISBE context

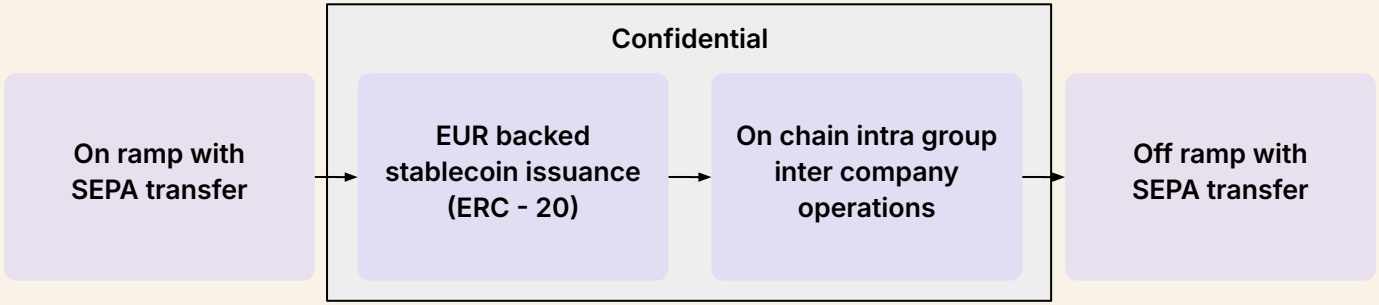
DOXA

ZKP batch settlement

- → Institutional policy model maps directly to ISBE SP structure
- → Kill switch via approval key revocation

- → Public chain-first design
- → Privacy pools model not clearly applicable inside ISBE

Ongoing pilot: On-chain treasury



- ➔ Smart contract under regulatory supervision — cannot be redesigned or redeployed
- ➔ MiCA freeze and forced transfer obligations must remain fully operational
- ➔ Regulator retains full audit capability at all times — confidentiality does not apply to the supervisor
- ➔ Multiple legal entities, multiple jurisdictions — confidentiality between subsidiaries, full traceability for group consolidation and per-jurisdiction regulators
- ➔ Confidentiality perimeter starts and ends at the smart contract — SEPA transfers remain visible to the banking system

Questions?



isbe

ALASTRIA

Let's continue the conversation

Miguel Calero, Executive Director
miguelcalero@alastria.io

Web
redisbe.com

Linkedin
@redisbe

Instagram
@red.isbe

X
@REDISBE

isbe

ALASTRIA