lokblok

SALES INFORMATION SHEET

Lokblok Business Wallet Demonstrator

Institutional-Grade Digital Asset Infrastructure
for Enterprise Governance & Compliance

0
Keys stored

8+
Blockchains supported

1–4w
New chain integration

Overview

The Lokblok Business Wallet Demonstrator is a sample with source code institutional wallet infrastructure designed for organisations managing digital assets.

Unlike conventional institutional wallets, it delivers a fundamentally different security architecture, one that combines ephemeral keys that are calculated and exist only at the point of use, hardware-rooted key management with enterprise governance, compliance enforcement, and operational flexibility.

Reference Implementation

This is not an institutional wallet product. It is a reference implementation demonstrating how Lokblok's Phantom Secrets and MPC hardware architecture and SDK can enable financial institutions, security vendors, or device manufacturers to build the next generation of wallet infrastructure.

Use Case

The Business Wallet Demonstrator is designed to showcase Lokblok features and SDKs for organisations that need secure digital asset management at scale with zero-custody cryptography . These organisations must handle large transaction volumes, multi-user approval workflows, regulatory compliance, and security audits. Requirements that existing wallet systems struggle to support without introducing security risks or operational friction.

- Banks
- Exchanges
- Asset Managers
- Fintech Platforms
- Corporate Treasury
- Tokenisation Platforms

The Institutional Wallet Problem

Most enterprise wallet solutions rely on standard MPC or multisig systems, introducing four key challenges:

Key fragments still exist
Even MPC systems store shares somewhere in software infrastructure, creating a persistent attack surface.

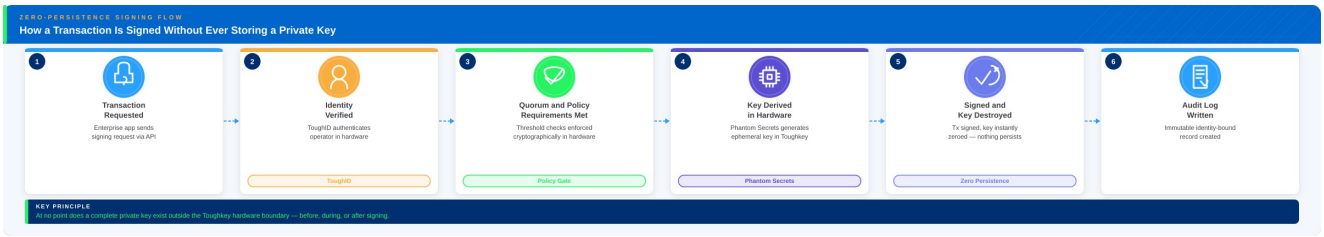
Limited business logic
Typical systems support only simple rules such as 2-of-3 signatures - insufficient for real corporate governance.

Operational complexity
Compliance workflows, address controls, and KYC verification are usually bolted on externally.

Vendor lock-in
Adding new blockchain support can require costly development, some providers charge hundreds of thousands.

How the Lokblok Business Wallet Demonstrator Works

The Business Wallet Demonstrator is built using Lokblok's Phantom Secrets SDK architecture, enabling secure wallet functions to be integrated directly into enterprise platforms. It combines multiple core components that together deliver hardware-rooted security, enterprise governance, and regulatory compliance - without exposing private key material.



CORE COMPONENTS

Phantom Secrets

Ephemeral keys generated on-demand, signed, immediately destroyed

Secure Terminal

Hardened compute environment for all high-risk signing operations

ToughID

Hardware-bound identity with biometric liveness checks and workflows verified

Phantom Gate

Mutual recognition between the endpoint and application server and attestation for phishing-proof secure connections

Core Capabilities

1 Zero-Cryptographic Custody by end user, business services, or institutions.

Transactions are signed using Phantom Secrets MPC and threshold cryptography executed inside FIPS 140-3 Level 3 hardware modules. This eliminates exposure of key material to software infrastructure.

2 Hierarchical Signature Policies

Unlike traditional MPC wallets that use flat signing rules, the Business Wallet supports hierarchical authorization. For instance:

— Transactions under £10k — manager approval
— Transactions over £100k — CFO approval required
— International transfers — compliance sign-off required

3 Segregation of Duties

Institutional governance requires separation of responsibilities. Organisations can mirror real corporate governance structures in their wallet architecture.

— Different key holder roles with distinct permissions
— Policy-based signing requirements
— Independent approval authorities

4 Address Whitelisting

Organisations can restrict transfers to approved addresses only, reducing the risk of funds being sent to malicious addresses.

- Whitelist governance approvals
- Separate authorisation wallet for whitelist changes
- Smart contract or policy-based enforcement

5 KYC-Verified Addresses

The system integrates with ToughID identity verification. Only verified addresses can be added to the whitelist, allowing the wallet to enforce compliance requirements automatically.

6 Risk Scoring & Compliance Checks

Before addresses are approved, the system can perform automated checks, embedding compliance into the wallet infrastructure itself.

- Risk scoring and sanctions screening
- Compliance verification
- Transaction policy enforcement

Blockchain Support

The Business Wallet Demonstrator supports multiple blockchains. New integrations can typically be completed within 1–2 weeks - significantly faster than many competing institutional platforms. ERC-20 and ERC-1155 tokens are also supported across several chains.

Bitcoin	**Ethereum**	**Avalanche**	**Solana**
Polkadot	**Polygon**	**Tron**	**XRP**

Advanced Capabilities near Deployment

Off-Chain Private Transfers
Assets transferred privately without broadcasting to the blockchain.

Key Delegation
Cryptographic delegation allows controlled transfer of signing authority.

Transfer-on-Sale / Death
Supports asset inheritance or delegated ownership scenarios.

Batch Recovery
Recovery of multiple wallets through a single identity verification.

Why Phantom Secrets Outperforms Standard MPC/TSS

Standard Threshold Signature Schemes (TSS) and Multi-Party Computation (MPC) represent the current market standard for institutional wallets. Phantom Secrets is a fundamentally different architecture — and it outperforms on every axis that matters for enterprise deployment.

	Standard MPC / TSS	lokblok Phantom Secrets
Asynchronous Signing	✗ Signers must be online simultaneously - co-ordinated sessions required every time	✓ Signers authorise independently at any time - no co-ordination needed
Attack Surface (Nothing to Steal)	✗ Key shares exist at rest in software or HSMs - a persistent, stealable target	✓ Keys materialise only during signing, then vanish - zero at-rest attack surface
Performance at Large Thresholds	✗ Computation scales poorly above 2-of-3 or 3-of-5 - high thresholds are impractical	✓ Efficient at any quorum size - 5-of-9 or 7-of-12 run without performance penalty
Keys per Toughkey Device	◷ Typically, one key identity per device - scaling to many accounts requires more devices	✓ One Toughkey covers unlimited accounts and wallets - no per-account hardware needed
Computational Scalability	✗ Offline/async TSS signing doesn't scale above small thresholds computationally	✓ Hardware-bound computation scales linearly – high thresholds remain fast

Async
Sign without co-ordination

1 Key
Unlimited accounts

Any K-of-N
No threshold penalty

Key Features Summary

Capability	Benefit
Hardware-based MPC and Phantom Secrets Threshold Secret Sharing	Removes software attack vectors
Hierarchical signatures	Enables real corporate governance
Segregation of duties	Prevents insider misuse
Address whitelisting	Prevents unauthorised transfers
KYC address verification	Supports regulatory compliance
Risk scoring	Embedded compliance checks
Fast blockchain integration	Lower operational cost
SDK architecture and source code samples	Easy integration into existing platforms

WHY IT'S BETTER

Five advantages that separate Lokblok from traditional institutional wallet approaches

lokblok.co

No keys stored

Reduces exposure from endpoint and infrastructure attacks.

Business logic enforced cryptographically

Approval workflows cannot be bypassed. Agile enough to mimic offline approvals.

Enterprise-ready governance

Supports real-world corporate approval structures natively.

Faster blockchain integration

New chains in 1–2 weeks vs months for competing solutions.

Built for compliance

Identity verification and policy enforcement are native features.

What This Demonstrator Shows

The Lokblok Business Wallet Demonstrator proves that organisations can operate digital asset infrastructure without the traditional risks of key custody.

Secure

Compliant

Operationally Flexible

Future-Ready

> *"It demonstrates how institutions can offer digital asset services without exposing themselves to the traditional risks of key custody."*

lokblok

Ready to see the Demonstrator in action?

Contact us to arrange a live walkthrough of the Business Wallet platform.

lokblok.co | info@lokblok.co