Introduction

Copy

S.I.G.N. is sovereign-grade digital infrastructure for national systems of money, identity, and capital. Sign Protocol provides the shared evidence layer used across deployments.

S.I.G.N. is a sovereign-grade architecture for building and operating national digital infrastructure across three foundational systems:

- **New Money System**: CBDC and regulated stablecoins operating across public and private rails with policy-grade controls and supervisory visibility
- **New ID System**: verifiable credentials and national identity primitives enabling privacy-preserving verification at scale
- **New Capital System**: programmatic allocation and distribution for grants, benefits, incentives, and compliant capital programs

S.I.G.N. is not a product container. It is a system-level blueprint for deployments that must remain governable, auditable, and operable under national concurrency.

Across these systems, one requirement repeats: **inspection-ready evidence**. In many deployments, that evidence layer is implemented using **Sign Protocol**, an omni-chain attestation protocol for creating, retrieving, and verifying structured records.

This documentation includes:

- system architecture and deployment guidance for S.I.G.N.
- use case blueprints for Money, ID, and Capital
- documentation for Sign products, including Sign Protocol, TokenTable, and EthSign
- full developer documentation for Sign Protocol (smart contracts, SDKs, APIs, advanced topics)

Archived copy · cryp2nova.com

If you came here for Sign Protocol developer docs, you are in the right place. The framing has expanded: S.I.G.N. describes the sovereign system architecture, and Sign Protocol is the evidence layer used across sovereign and institutional workloads. TokenTable and EthSign are standalone products that use the same core primitives and can be integrated into S.I.G.N. deployments when appropriate.

Trust, but verify at sovereign scale

Every day, systems depend on claims:

- a person claims eligibility for a program
- a business claims compliance
- an institution claims approval
- a system claims a payment was executed
- a registry claims an asset record is accurate

Historically, these claims were accepted based on relationships and institutional trust. In digital systems that operate across agencies, vendors, and networks, trust assumptions become fragile. Verification must be repeatable, attributable, and compatible with oversight.

S.I.G.N. exists to make verification reliable, repeatable, and operable at national scale.

Attestations as a modern solution to authenticity

Attestations are portable, verifiable proofs that can travel across systems and time. They encode a statement, bind it to an issuer, and make it verifiable later.

Archived copy · cryp2nova.com

In consumer life, a person might need a notarized document to prove a claim. In a sovereign context, the same pattern scales to system-critical actions:

- eligibility for benefits and public programs
- compliance gates for regulated services
- approvals for high-impact actions (distributions, conversions, registry updates)
- proof that a distribution occurred under an approved ruleset version
- proof that a registry update was authorized and traceable

S.I.G.N. treats attestations as operational infrastructure, not as an abstract primitive.

What is S.I.G.N.?

S.I.G.N. is a layered stack that unifies:

- **execution**: money movement and program logic
- **identity**: credentials and verification
- **evidence**: cryptographic records of what happened, when, and under which authority

Sovereign deployments must satisfy constraints that typical consumer systems do not:

- privacy by default for sensitive payloads
- lawful auditability and inspection readiness
- strict operational control (keys, upgrades, emergency actions)
- interoperability across agencies, vendors, and networks
- performance and availability under national concurrency

S.I.G.N. is designed so that policy and oversight remain under sovereign governance while the technical substrate stays verifiable.

Archived copy · cryp2nova.com

Start here:

- S.I.G.N. Overview
- Reference Architecture
- Security & Privacy
- Governance & Operations

The three systems

New Money System

A sovereign digital money rail supporting CBDC and regulated stablecoins across public and private rails.

Common requirements:

- real-time settlement and deterministic finality targets
- policy controls (limits, approvals, emergency controls)
- supervisory visibility and reporting
- optional confidentiality for retail flows
- interoperability across rails and networks

Read: New Money System

New ID System

A national identity and credential layer supporting reusable verification without central "query my identity" APIs.

Common requirements:

- W3C Verifiable Credentials (VC) and Decentralized Identifiers (DID)
- selective disclosure and privacy-preserving proofs

Archived copy · cryp2nova.com

- trust registry and issuer accreditation
- revocation and status checks
- offline presentation patterns where required (QR, NFC)

Read: New ID System

New Capital System

A programmatic capital and distribution layer for benefits, grants, incentives, and compliant capital programs.

Common requirements:

- identity-linked targeting and duplicate prevention
- schedule-based distributions (one-time, recurring, vesting)
- deterministic reconciliation and budget traceability
- evidence manifests for audits and disputes

Read: New Capital System

The evidence layer

All three systems rely on a shared trust and evidence layer to answer questions like:

- who approved what
- under which authority
- when the action occurred
- what ruleset version applied
- what evidence supports eligibility and compliance
- what settlement references prove execution

In the Sign ecosystem, this evidence layer is implemented by **Sign Protocol** using two primitives:

Archived copy · cryp2nova.com

- **Schemas**: templates defining how structured data is represented
- **Attestations**: signed, verifiable records conforming to schemas

Sign Protocol supports multiple data placement models:

- fully on-chain attestations
- fully off-chain payloads with verifiable anchors (for large or sensitive data)
- hybrid models combining on-chain references and off-chain payloads
- privacy-enhanced modes including private and ZK attestations where applicable

SignScan provides unified querying across supported chains and storage:

- REST and GraphQL APIs
- SDK-based access patterns
- explorer and dataset visibility for non-programmers

Product overview: Sign Protocol
Developer entrypoint: Getting Started

Sign products and how they relate to S.I.G.N.

CRYP2NOVA

S.I.G.N. is the sovereign system architecture. Sign products are deployable offerings that can be used independently and are often combined in sovereign and regulated deployments.

- **Sign Protocol**: schemas, attestations, privacy modes, indexing and querying
- **TokenTable**: allocation, vesting, and large-scale distribution for capital programs
- **EthSign**: agreement and signature workflows producing verifiable proof of execution

Archived copy · cryp2nova.com

These products share core primitives, but they are not defined as "subsystems of S.I.G.N.". They are components that can support S.I.G.N. deployments when the program requires their specific capabilities.

Products overview: Products Overview

Technical snapshot (standards and interfaces)

This is a reference snapshot of standards commonly used in S.I.G.N. deployments.

Identity:

- W3C Verifiable Credentials (VC) and W3C DIDs
- issuance via OpenID for Verifiable Credential Issuance (OIDC4VCI)
- presentation via OpenID for Verifiable Presentations (OIDC4VP)
- revocation via W3C Bitstring Status List
- offline presentation patterns (QR, NFC) where required
- compatibility targets for mobile drivers license patterns (ISO/IEC 18013-5/7) when relevant

CRYP2NOVA

Evidence:

- schema-driven structured data models
- cryptographic signatures (ECDSA, EdDSA, RSA depending on deployment)
- privacy-preserving proofs (selective disclosure, ZK systems where applicable)
- indexing and query layers for operational reporting and audits

Money rails (deployment-dependent):

- public mode via L1 smart contracts or sovereign L2 deployments

Archived copy · cryp2nova.com

- private mode via permissioned CBDC rails for confidentiality-first requirements
- controlled interoperability via bridging or messaging gateways

---

Deployment modes (public, private, hybrid)

S.I.G.N. is designed for deployment realities, not ideology.

Public mode:

- optimized for transparency-first programs, public verification, and broad accessibility
- governance is expressed via chain parameters (L2) or contract governance (L1)

Private mode:

- optimized for confidentiality-first programs and regulated domestic payment flows
- governance is enforced through permissioning, membership controls, and audit access policy

Hybrid mode:

- combines public verification and private execution where required
- interoperability must be treated as critical infrastructure with explicit trust assumptions

---

CRYP2NOVA

Archived copy · cryp2nova.com

How to read these docs

If you are exploring S.I.G.N. (systems, architecture, governance)

Start with:

- S.I.G.N. Overview
- Reference Architecture
- Security & Privacy
- Governance & Operations

Then:

- New Money System
- New ID System
- New Capital System

If you are building (developers, integrators)

Start with:

- Getting Started

Then go deeper:

- writing data: Writing Data
- querying data: Querying Data
- advanced topics: Advanced Topics
- supported networks: Supported Networks

CRYP2NOVA

Archived copy · cryp2nova.com

If you are evaluating products

Start with:

- Products Overview

Tenets that guide S.I.G.N. (and Sign)

Keep it simple, Signer.

Sovereign systems are already complex (policy, compliance, privacy, interoperability). Infrastructure should reduce complexity, not add it. The goal is to make verifiable systems intuitive to integrate and difficult to misuse.

Improvise. Adapt. Excel.

The path to real infrastructure is never linear. Deployments evolve with policy, adoption, interoperability constraints, and emerging threats while remaining governable and auditable.

CRYP2NOVA

An open stack

Verification is most valuable when it is portable. S.I.G.N. embraces open standards and interoperable primitives so systems can evolve without locking policy into one vendor or one network.

Evidence maketh governance

Identity primitives establish representation. Evidence establishes history. Attestations are the bedrock of accountability: who approved what, under which authority, when, and according to which rules.

Archived copy · cryp2nova.com

Where to go next

- Start with S.I.G.N.: S.I.G.N. Overview
- Explore national systems:
  - New Money System
  - New ID System
  - New Capital System
- Build with Sign Protocol:
  - Getting Started
- Evaluate products:
  - Products Overview

Next
FAQ

Last updated 6 months ago

Was this helpful?

CRYP2NOVA
Copyright Sign 2021-2024

Archived copy · cryp2nova.com