Prism — FAQ

Institutional Privacy Questions & Answers

VerifiedX

QUESTION 1

How do view keys work?

Prism supports **selective disclosure via view access**, allowing institutions or users to grant visibility into otherwise shielded transactions to authorized parties (e.g., auditors, regulators, or compliance teams).

- Each shielded account can generate a **view key / audit permission**
- This enables:
  - Transaction history visibility
  - Balance verification
  - Counterparty review (where permitted)
- Access can be:
  - **Time-bound**
  - **Scope-restricted**
  - **Revocable**

KEY POINT

Privacy is preserved by default, but **full transparency can be programmatically enabled when required**.

QUESTION 2

Can shielding be disabled at the protocol or institutional level?

Yes. Prism is **fully optional and policy-driven**, and institutions can enforce **transparent-only transaction policies** at the wallet, application, or counterparty level.

- Institutions can:
  - Disable shielded transactions entirely
  - Restrict shielding to approved counterparties
  - Require all flows to remain transparent
- Enforcement layers:
  - Wallet-level controls
  - Smart contract / application rules
  - Institutional policy frameworks

KEY POINT

Prism does **not force privacy** — it enables **controlled, compliant usage**.

QUESTION 3

How does AML / transaction monitoring work if amounts and parties are hidden?

Prism maintains AML compatibility through a combination of **observable system boundaries, policy controls, and optional disclosure mechanisms**, ensuring institutions retain full monitoring capability.

A. Observable Entry / Exit Points

- Fiat on/off ramps
- Custodial endpoints
- Institutional wallets

These remain **fully visible and traceable**.

B. Policy-Based Restrictions

- Limit or prohibit shielded flows
- Require counterparties to be known / whitelisted
- Enforce transaction rules

C. Selective Disclosure (View Keys)

- Full transaction visibility when required
- Regulatory reporting
- Internal compliance review

D. Analytics Integration

- Compatible with providers like **Merkle Science**
- Enables risk scoring, pattern detection, and behavioral analysis

KEY POINT

While transaction data can be shielded, **risk monitoring and compliance oversight remain fully achievable through controls and disclosures**.

QUESTION 4

How is this different from mixers or obfuscation tools?

Prism does **not**:

- Pool funds
- Mix assets
- Obfuscate transaction lineage through commingling

Instead, each transaction is:

- **Individually validated**
- **Cryptographically provable**

System integrity remains **deterministic** and **auditable**.

KEY POINT

Prism is a **privacy-preserving validation system**, not an obfuscation mechanism. Transactions can be confidential, but validity, control, and auditability are always enforceable.