AccreDeFi
Self-Serve Compliant Tokenization

Data Security Protocol

AccreDeFi secures all data accessed via the Plaid API through a comprehensive defense-in-depth strategy that adheres to data minimization, strict access controls, and cryptographic protection, ensuring regulatory compliance and auditability.

1 - Data Minimization and Purpose Limitation

AccreDeFi operates on the principle of **Need-to-Know** data retention.
We only extract and retain the minimum necessary data required for on-chain compliance enforcement and XDC Ordinal inscription.
Plaid Data Used: We utilize Plaid's verified data (account numbers, routing information, verified addresses, name, etc.) primarily to:
Verify Identity: Confirm the Issuer's real-world identity matches the Secure GIRN Anchor.
Ordinal Inscription: Collect international financial identifiers (BIC/IBAN/Routing) for immutable inclusion in the XDC Ordinal records (as mandated by the protocol).
Data NOT Stored: We do not retain raw user credentials, Plaid Access Tokens long-term, or store excessive transaction history beyond what is required for the specific Ordinal record.

2. Encryption and Storage Security

All sensitive data obtained via Plaid is subject to strong encryption both in transit and at rest:

Encryption In Transit: All communication between the AccreDeFi backend service and the Plaid API is secured using HTTPS/TLS 1.2+, as mandated by Plaid and industry standards.
Encryption At Rest (Cloud SQL): Data stored in our Cloud SQL database (TokenBook off-chain data) is encrypted using AES-256 and leverages Google Cloud's built-in managed encryption keys.
Tokenization: Sensitive financial identifiers necessary for TGE are tokenized or hashed where possible before permanent storage, reducing the risk profile of our database.

3. Access Control and Authentication

Access to Plaid data and our backend database is strictly limited via role-based access control (RBAC):

Service Accounts: Access to Plaid APIs and our database is restricted to dedicated, non-human service accounts using secure, short-lived credentials.

Environment Variables: All Plaid credentials (PLAID_CLIENT_ID, PLAID_SECRET) are stored securely as environment variables and managed via a secure vault system (e.g., Google Secret Manager or HashiCorp Vault), preventing them from being hardcoded or accessed directly by unauthorized personnel.

Dedicated Systems: The ComplianceStatusGenerator is deployed on a dedicated Compute Engine instance with hardened security policies, isolating it from public-facing services.

4. Auditability and Regulatory Compliance

AccreDeFi's architecture enforces an immutable audit trail, a core requirement for compliant finance:

Immutable On-Chain Record: The final, verified Plaid data elements used for the TGE are cryptographically included in the XDC Ordinal Inscription. This provides an unchangeable, verifiable record for regulators (FINRA, SEC, etc.).

Data Logging: All interactions with the Plaid API are logged internally with unique request_id values, ensuring complete traceability and facilitating rapid response to support requests or regulatory inquiries.

Compliance with Plaid Terms: We explicitly agree to adhere to all Plaid Developer terms and conditions regarding the handling and storage of consumer data, including data retention and deletion policies.

Contact Details

RegulatedTokens.com


Contact@AccreDefi.Net

AccreDefi