mUSD Technical Architecture

Canton-Native Institutional Cash and Securities Minting Protocol | April 2026 | v4.0

1. Protocol Overview

mUSD is a Canton-native stable settlement token built on Digital Asset's DAML smart contract language and the Canton Network's Global Synchronizer. The protocol is designed exclusively for institutional use — securities-backed minting, treasury settlement, and deployment into Canton-native yield vehicles through a structurally separate Institutional Yield Vault.

The architecture is Canton-exclusive by design. There is no Ethereum bridge, no public-chain DeFi dependency in the core product, and no blended retail and institutional reserve pools. Every component — collateral validation, minting, yield routing, and payout — operates within Canton's privacy-preserving, formally-verified DAML environment.

2. DAML and Canton Foundation

Why DAML

DAML (Digital Asset Modelling Language) is an open-source, purpose-built smart contract language for regulated financial workflows. Unlike EVM-compatible contracts, DAML enforces explicit party authorization at the contract level — no transaction can execute without all required signatories present. This eliminates the single-key-drain attack surface that has caused billions in EVM losses.

- Formally verified execution — deterministic outcomes, no partial execution
- Sub-transaction privacy — counterparties see only the data they are entitled to
- Granular authorization — each contract action requires explicit multi-party consent
- No open mempool — no front-running, no MEV, no eavesdropping on contract state
- Atomic interoperability via Global Synchronizer — cross-application settlement without bridges

Canton Network Infrastructure

Canton is the Global Synchronizer infrastructure connecting sovereign ledgers operated by institutions including Goldman Sachs, BNY, BNP Paribas, DTCC, Euroclear, and HSBC. It processes over $350 billion in repo daily and $6T+ in tokenized asset volume monthly. Minted operates as a Featured Application on Canton, earning Canton Coin rewards based on transaction activity — creating a native revenue stream that scales with network usage.

3. Securities Minting Architecture

Securities Minting is the primary institutional entry point. Institutions holding approved Canton-native tokenized securities mint mUSD against that collateral without liquidating their position. The workflow is entirely bilateral and off-chain on the yield side — no open DeFi strategy, no smart contract risk on the yield leg.

Minting Flow

Step	Action	Party
1	Institution pledges eligible Canton-native securities	Institution → Minted
2	Minted validates collateral eligibility and applies haircut	Minted (DAML contract)
3	mUSD minted to institution at approved advance rate (60–85% LTV)	Canton Global Synchronizer
4	Collateral ring-fenced or routed to Institutional Yield Vault	Custody / Asset Control Partner
5	Institution holds mUSD as liquid settlement instrument	Institution

Eligible Collateral (Initial)

Asset	Example	Advance Rate
Tokenized US Treasuries	USYC on Canton (Hashnote / DRW)	80–85%
Tokenized money market funds	Franklin Benji / FOBXX on Canton	80–85%
Tokenized sovereign bonds	USDM1 and comparable instruments	70–80%
Canton-native structured debt	T-RIZE digital bond programme	60–75%
Other approved RWAs	Governance-approved on a case-by-case basis	Case-by-case

4. Token Design

mUSD — Base Settlement Token

mUSD is a non-yield-bearing Canton-native stable settlement token. It is the neutral cash leg — designed to be stable, liquid, and institutionally legible. mUSD does not carry yield exposure. It is the instrument that connects collateral, settlement workflows, and yield access.

Implemented as a CIP-56 compliant DAML contract on the Canton Global Synchronizer. Sub-transaction privacy ensures counterparties see only their own positions.

smUSD Vaults — Institutional Yield Vault

Yield is accessed exclusively through a structurally separate smUSD Vault architecture. Institutions opt in explicitly. The vault receives economic exposure to approved Canton-native yield vehicles — tokenized private credit, structured digital bonds, trade finance instruments — while the base mUSD product remains clean, redemption-oriented, and peg-stable.

Layer	Instrument	Yield-Bearing	Economic Role

Settlement layer	mUSD	No	Neutral cash leg — treasury, settlement, collateral
Yield access layer	smUSD Vault	Yes	Controlled exposure to Canton-native yield vehicles

5. Security and Audit Status

Control	Implementation
Multi-party authorization	No mint executes without all required DAML signatories
Sub-transaction privacy	Contract state invisible to non-parties — no front-running
Atomic settlement	DAML atomic commit — no partial execution possible
Collateralization enforcement	120% enforced on-chain before any mint
Replay protection	Per-attestation address and chain ID binding
Rate limiting	Net mint/burn capped on 24-hour rolling window
Emergency controls	Multi-sig admin with 48-hour timelock
Key management	HSM-backed custody with attested enclave signing
Audit status	Softstack audit complete (Canton Protocol + DeFi Lending). Tier 1 in progress.
Test coverage	244 test cases, 14/14 Canton audit checks, audit readiness 9.8/10
Sandbox validation	18-phase sandbox validation via 5North — all phases passed

6. Compliance Infrastructure

Minted operates with a full institutional compliance stack established prior to launch. This was a deliberate pre-condition — not a post-launch addition.

Compliance Element	Status
Broker-Dealer oversight	In place
Transfer Agent registration	**In place**
ATS oversight	**In place**
PPSI charter (Payment/Issuance)	**In place**
Issuer of Record	**Established**
KYC / KYB / Sanctions screening	**Required for all institutional participants**
Legal counsel (General Counsel)	**Wallace Glausi — Securities law, Reg D, BD/TA/ATS**