DIGITAL COMMERCIAL BANK — INTEGRATION ACTIVATION REPORT

NVCT ↔ VUSD Bilateral Settlement · DAES 256 · ISO 20022 pacs.008 · INDA Rail · Ref: DCB-NP-21399964 · Rev. R3 (March 27, 2026)

Report Date: May 14, 2026 **API Ref:** DCB-NP-21399964 **Form Submitted:** April 14, 2026 **DCB Contact:** Felipe · Digital Commercial Bank
Prepared by: Frank O. Ekejija **Classification:** Confidential — Technical Team

1. EXECUTIVE SUMMARY

This report provides NVC Fund Bank's technical team with a focused, actionable account of the Digital Commercial Bank (DCB) integration engagement. DCB has confirmed readiness on their side. A USD 1.00 smoke test is standing by at DCB and can be executed within 15 minutes of credential exchange.

The integration objective is a live, bilateral NVCT ↔ VUSD 1:1 par-value settlement lane over ISO 20022 pacs.008.001.08 through the INDA Rail. Two connectivity paths are available and both are technically viable. The current pending setup (Path A — NVC as API host) follows from the April 14, 2026 API Configuration Form that NVC Fund Bank submitted to DCB. However, DCB operates a live DAES 256 API platform at `185.229.57.76 / luxliqdaes.cloud` and can equally provide credentials to NVC Fund Bank (Path B — DCB as API host), identical in structure to the KoreNet and DevMind integrations. The technical team should review both paths and confirm which to activate, since Path B can be executed significantly faster.

2. DCB READINESS CONFIRMATION

Inbound Confirmation — From Felipe · Digital Commercial Bank

> "DCB integration is ready. First USD 1.00 smoke test ready in 15 minutes once NVC credentials received."

Received: April 27, 2026 · Ref: DCB-NP-21399964 · DCB Egress IP confirmed: `94.207.76.109 : Port 443 : TLS 1.3`

Important context on Felipe's response: Felipe's message — "once NVC credentials received" — is a direct reply to the API Configuration Form submitted by NVC Fund Bank on April 14, 2026. That form declared NVC Fund Bank as the API host at `api.nvcfund.com` and stated that credentials (API keys, IPs, RSA public key) would be issued by NVC to DCB. Felipe confirmed he is ready to receive those credentials and connect inbound. This is **Path A**. It does not mean DCB cannot also operate as the API provider — DCB's DAES platform is already live. The choice of path was embedded in how the form was completed.

Status either way: DCB is technically ready for both paths. The USD 1.00 smoke test stands by. The decision NVC Fund Bank's technical team must make is which path to activate (see Section 3 below).

3. CONNECTIVITY ARCHITECTURE — TWO AVAILABLE PATHS

Both paths below are technically viable. The choice between them is a business and infrastructure decision for NVC Fund Bank's technical team to make before any further credentials are exchanged. Path B can be activated immediately using DCB's live DAES platform without any new infrastructure on NVC's side.

PARAMETER	PATH A — NVC AS API HOST (CURRENT FORM)	PATH B — DCB AS API HOST (DAES MODEL)
API Host	`api.nvcfund.com` — hosted by NVC Fund Bank	`185.229.57.76 / luxliqdaes.cloud` — hosted by DCB (already live)
Who provides credentials	NVC Fund Bank generates and sends to DCB	DCB generates and sends to NVC Fund Bank
NVC Fund Bank role	API Provider — DCB calls inbound to NVC	API Consumer — NVC calls outbound to DCB (same as KoreNet / DevMind)

PARAMETER	PATH A — NVC AS API HOST (CURRENT FORM)	PATH B — DCB AS API HOST (DAES MODEL)
Why we are here	NVC's April 14 form declared this model — Felipe confirmed readiness to receive NVC credentials	DCB's DAES API is live and has always been available as an alternative
Infrastructure needed	Build + deploy api.nvcfund.com (DNS, server, TLS, OAuth 2.0 layer, pacs.008 handler)	None — DCB's endpoint is live. NVC stores DCB credentials in Secrets vault and calls out
Credential package	NVC generates: OAuth2 client_id/secret, HMAC key, RSA-2048 public key, webhook secret, IPs	DCB generates: API key / token, HMAC signing key, DCB public key — transmitted to NVC
Webhook direction	NVC hosts `webhooks.nvcfund.com/dcb/notifications` (per submitted form)	DCB hosts `luxliqdaes.cloud/api/webhooks/receive` (already live)
Time to activation	Weeks — requires building and deploying api.nvcfund.com from scratch	Days — request DCB credential package, store in vault, point client at DAES endpoint
Comparable to	NVC Fund Bank hosting its own banking API — significant DevOps effort	KoreNet model · DevMind model — NVC as outbound API consumer (already proven pattern)
Recommended?	Long-term (when NVC public API is needed for multiple partners)	**Yes — fastest path to live smoke test**

Recommended action: Contact DCB operations (`operations@digcommbank.com`) referencing DCB-NP-21399964 and request that DCB provision an inbound credential package for NVC Fund Bank to connect to DAES (Path B). This does not cancel or conflict with Path A — the April 14 form remains on record and Path A can be completed in parallel as NVC's long-term public API build-out. But Path B can produce a live smoke test result in days, not weeks.

4. PARTNERSHIP OVERVIEW — DIGITAL COMMERCIAL BANK & VUSD

500+	50+	$10B+	25+	8%
TEAM MEMBERS	COUNTRIES	AUM	INDUSTRY AWARDS	APY DEPOSITS
Worldwide	Served	Under Management	Recognised	Digital Accounts

Digital Commercial Bank Ltd. (DCB)

Website: digcommbank.com · luxliqdaes.cloud
Settlement Platform: DAES 256 — Digital Asset & Electronic Services
LEI: `254900KLR17QIS1G6I63`
BIC: `GEEIGB22XXX`
IBAN: `GB49GEEI04276701099100`
Global Server IP: `185.229.57.76 : 443 (TLS 1.3)`
Operations Contact: operations@digcommbank.com
Integration Contact: Felipe · DCB Integration Team
Compliance: ISO 20022 · ISO 27001:2022 · PCI-DSS Level 1 · SOC 2 Type II · FATF AML/CFT · KYC/KYB Completed · GDPR · Basel III
AML Score: 100/100 — Low Risk (reviewed December 30, 2025)
API Ref: DCB-NP-21399964 · Submitted April 14, 2026
Status: DCB SIDE: READY

VUSD — Institutional Stablecoin (VERGY.WORLD)

Type: USD-pegged institutional-grade stablecoin
Network: VERGY.WORLD · DCB Settlement Rail
TVL: $100B+ Total Value Locked
Countries: 150+ supported
Parity: 1 VUSD = $1.00 USD · Uptime: 99.9%
Settlement Speed: <1 second per transaction
Pair to NVCT: 1:1 USD — ZERO FX RISK

5. INSTITUTIONAL DUE DILIGENCE — COMPLIANCE, CUSTODY & OPERATIONAL PROOF

The DAES Institutional Account Statement (Ref: DCB-20251230-490364, December 30, 2025) for an existing DCB institutional client provides independent evidence of DCB's live operational capacity, full compliance posture, and custody account structure. This section documents what that statement confirms for NVC Fund Bank's due diligence and risk management requirements.

Full Regulatory Compliance & Certifications (Confirmed)

ISO 27001:2022 — Information Security Management CERTIFIED

ISO 20022 — Financial Messaging Standard NATIVE

PCI-DSS Level 1 — Card Data Security COMPLIANT

SOC 2 Type II — Security & Availability Controls CERTIFIED

FATF AML/CFT — Anti-Money Laundering VERIFIED

KYC / KYB — Customer Due Diligence COMPLETED

GDPR — Personal Data Protection COMPLIANT

Basel III — Banking Capital Requirements ALIGNED

DAES Custody Account Structure (NVC Fund Bank Will Receive)

Account Format: `DAES-BK-USD-XXXXXXX` (unique assigned number)
Account Type: Custody Banking Account — Segregated
Safekeeping: Full Title Transfer
Insurance: FDIC-Equivalent Coverage
Jurisdiction: International Banking Standards
Fund Access: On-demand
Valuation: Real-time
Fund Classification: M2 (custody) — M1 execution at settlement layer
Currency: USD (ISO 4217: 840)
Custodian: Digital Commercial Bank Ltd.

AML / CFT Risk Assessment (Confirmed Active)

AML Score: 100 / 100
Risk Classification: LOW — Approved
KYC Status: Verified · Completed
Last Review: December 30, 2025
Next Review: December 30, 2026

NVC Fund Bank's AML/CFT compliance function can rely on DCB's own 100/100 AML score as a baseline for correspondent banking risk assessment. DCB's FATF AML/CFT verification is current and independently certified.

Operational Scale — Confirmed Live Institutional Activity

The December 30, 2025 DAES statement for an existing institutional client (account balance: $755B+ USD, active since December 12, 2017) shows DCB processing real-time transactions with the following counterparties:

Citigroup · Standard Chartered · Mitsubishi UFJ Financial
Industrial & Commercial Bank of China · China Construction Bank
Agricultural Bank of China · Credit Suisse
Postal Savings Bank of China · China Merchants Bank
Shanghai Pudong Development Bank

This confirms DCB is an active, live settlement institution — not a paper entity.

M1 vs M2 clarification for treasury: DCB's technical document describes M1 (immediate liquidity) as the fund type for direct settlement execution — this refers to the settlement mechanism, where funds move immediately with no intermediary hold. The custody accounts themselves are classified M2 (near money — savings deposits). NVC Fund Bank's account at DCB will carry M2 classification for the custody wrapper, with M1-speed execution at the INDA settlement layer.

6. SETTLEMENT ARCHITECTURE — NVCT ↔ VUSD BILATERAL SWAP LANE

The settlement architecture establishes a par-value bilateral swap lane between NVCT and VUSD. Both tokens maintain a strict 1:1 USD peg, eliminating foreign exchange conversion risk in the settlement layer. All transfers use NVCT's `transfer()` function — **mint() is never called on NVCT**; the full 30T supply is pre-minted. Message framing follows ISO 20022 pacs.008.001.08 and routes through the INDA Rail, with NVC Fund Bank hosting the API endpoint at `api.nvcfund.com`.

7. DCB DAES 256 SETTLEMENT ARCHITECTURE

DCB's settlement infrastructure is built on DAES 256 (Digital Asset & Electronic Services), a proprietary engine operating at `luxliqdaes.cloud`. This is a critical detail for NVC Fund Bank's technical team: DCB is not a simple REST API consumer — they operate a full settlement engine with five integrated modules and four connectivity channels.

DAES 256 Core Components

Transaction Orchestrator: Initiation, routing, lifecycle management
Validation Engine: JSON schema + ISO 20022 pacs.008.001.08 validation
Settlement Engine: INDA direct settlement — M1 immediate funds
Security Layer: HMAC-SHA256 (LAU) · RSA-2048 PKI · AES-256-GCM
Certification Module: Generates 6-document post-settlement package

Connectivity Channels Available

A2A — API to API: REST / Webhook · Real-time bidirectional
IP2IP / IP-ID: Direct network-level · Point-to-point
SSH / SFTP: Secure asynchronous file exchange
Webhook Direct: HTTP POST · HMAC signature · Instant delivery
DCB Webhook: `luxliqdaes.cloud/api/webhooks/receive`

Recommended channel for NVC Fund Bank: A2A (REST / Webhook) is the primary real-time channel for the initial integration. IP2IP can be added as a secondary high-assurance channel once A2A is confirmed working. mTLS is supported by DCB as optional mutual authentication and should be requested for production.

7A. DCB TRANSACTION LIFECYCLE

STAGE	ACTION	DCB SYSTEM
1. Initiation	Counterparty sends JSON or ISO 20022 XML via API, IP, or SFTP	Transaction Orchestrator
2. Validation	JSON schema validation + ISO 20022 pacs.008 validation + HMAC-SHA256 signature check	Validation Engine
3. Authorization	INDA instruction validated · Settlement conditions confirmed	Settlement Engine
4. Execution	Direct debit/credit via DAES — no intermediary routing · M1 immediate funds	Settlement Engine
5. Confirmation	Status returned via API/Webhook · `real_transaction: true`	Transaction Orchestrator
6. Certification	6-document post-settlement package generated (PIN-secured + SFTP delivery available)	Certification Module

7B. POST-SETTLEMENT CERTIFICATION PACKAGE

Every completed transaction through DAES 256 produces a 6-document cryptographic certification package. NVC Fund Bank's compliance and treasury teams should expect and archive all six documents for each settlement.

Settlement Certification Documents (per transaction)

1. ISO 20022 Transfer Statement (PDF)
2. pacs.008.001.08 Settlement Certificate
3. HMAC-SHA256 LAU Integrity Proof

JSON Payload Key Fields (DCB Standard)

transfer_id: Maps to ISO 20022 MsgId / EndToEndId / InstrId
real_transaction: Must be `true` for live execution
settlement_type: e.g. `FIAT_DEPOSIT`

4. SwiftNet PKI Digital Signature Certificate (RSA-2048)
5. Interbank Settlement Confirmation
6. Bilateral MAC Verification Certificate

Delivery: PIN-secured access · Optional SFTP/SSH transmission

sender.bic: Maps to DbtrAgt > FinInstnId > BICFI
signature.method: `HMAC-SHA256`
signature.value: HMAC result in header: `X-Signature`
hash: SHA-256 body hash included in payload

8. FULL TECHNICAL SPECIFICATION

PARAMETER	VALUE
NVC API Host (to provision)	`api.nvcfund.com/v1` — DNS not yet active
DCB Global Server	`185.229.57.76 : 443 (TLS 1.3)` — luxliqdaes.cloud
DCB Outbound / Egress IP	`94.207.76.109 : 443 (TLS 1.3)` — whitelist on NVC firewall
DCB Webhook Receive	`luxliqdaes.cloud/api/webhooks/receive`
NVC API Role	Path A: API Provider — DCB calls inbound to `api.nvcfund.com` (form as submitted) | Path B: API Consumer — NVC calls outbound to DCB DAES (recommended, same as KoreNet/DevMind)
Message Format (Primary)	ISO 20022 pacs.008.001.08 · Namespace: urn:iso:std:iso:20022:tech:xsd:pacs.008.001.08
Message Format (API)	JSON (`application/json; charset=UTF-8`) with ISO 20022 field mapping
Authentication	API Keys / Tokens (per-endpoint) · HMAC-SHA256 (LAU) · IP Whitelisting
HMAC Signing Header	`X-Signature` (HMAC-SHA256 value) + `body_hash` (SHA-256 body)
PKI / Asymmetric Encryption	RSA-2048 / SHA-256 (confirmed in DCB technical document Rev. R3)
Symmetric Encryption	AES-256-GCM (PIN-locked fund packages)
Mutual TLS (mTLS)	Optional — supported by DCB, recommended for production
Transport Security	TLS 1.2 / TLS 1.3 (TLS 1.3 preferred)
Settlement Model	INDA — Instructed by Direct Agent · No SWIFT · No IBAN routing · No correspondent banks
Fund Type	M1 — Immediate Liquidity (Direct Funds)
Settlement Speed	Real-time or near real-time
NVCT Contract	`0x36785Bb0396d3717aE3ddec61a4F562b7FcD9A37` · Base Mainnet
NVCT Transfer Method	`transfer()` only — **mint() is never called**
Settlement Parity	1 NVCT = 1 VUSD = $1.00 USD — zero FX conversion risk
Post-Settlement Docs	6-document certification package per transaction (PIN-secured)
Compliance Standards (DCB)	ISO 20022 · ISO 27001 · PCI-DSS Level 1 · FATF AML/CFT
First Smoke Test	USD 1.00 · Standing by at DCB · Executes within 15 min of credential receipt
Compliance Contact (NVC)	`compliance@nvcfund.com`

9. CREDENTIAL PACKAGE — PATH A: ITEMS NVC FUND BANK MUST DELIVER TO DCB

All five items below must be generated from the live `api.nvcfund.com` system using hardware-backed key management (HSM or equivalent). Transmission to DCB must occur through a verified, mutually authenticated secure channel — not email, chat, or any web admin interface. Coordinate through `compliance@nvcfund.com`.

1. **api.nvcfund.com — Primary + Secondary IP Addresses**
   DNS for api.nvcfund.com is not currently active. Infrastructure must provision the production API host and expose primary and secondary IPs. DCB requires both to configure their firewall and set up failover routing. This is a prerequisite for every other item on this list.

2. **OAuth2 client_id / client_secret + API Key**
   Generated from the live NVC API credential management system. Must be scoped to DCB's settlement and swap operations only, with defined rate limits. Include the token endpoint URL and rotation schedule at issuance.

3. **HMAC-SHA256 Payload Signing Key**
   Used by DCB to cryptographically sign every outbound API request body. NVC Fund Bank verifies the signature on receipt before processing. Key must be generated in an HSM or equivalent hardware-backed key store. Define the signing header name and algorithm version in the credential package.

4. **RSA-2048 Public Key / PKI Certificate (PEM format)**
   DCB's PKI layer uses RSA-2048 / SHA-256 (confirmed in DCB technical document Rev. R3, March 27, 2026). NVC Fund Bank must generate an RSA-2048 key pair; the public key is delivered to DCB in PEM format. The corresponding private key must never leave NVC Fund Bank's infrastructure. Include the key fingerprint for verification. Compatible with DCB's SwiftNet PKI signature certificate format.

5. **Webhook Endpoint Secret + TLS Certificate Pin**
   Required for DCB to authenticate inbound event notifications sent from NVC Fund Bank. The shared webhook secret is used to validate HMAC signatures on delivery payloads. The TLS certificate pin prevents man-in-the-middle attacks on the notification delivery path.

Security Protocol: No credential in this package should transit through email, chat applications, or web-based administrative interfaces. All items must be packaged, encrypted, and delivered through a verified secure channel with a complete audit trail. Contact: **compliance@nvcfund.com**.

NVC Fund Bank Infrastructure — Two-Way IP Configuration Required:
(a) **Inbound allowlist:** Add DCB's outbound/egress IP `94.207.76.109 : 443` to the NVC api.nvcfund.com firewall — this is the IP DCB will use when connecting inbound to NVC's API.
(b) **Outbound route:** NVC Fund Bank should also record DCB's global DAES server `185.229.57.76 : 443 (TLS 1.3)` for any NVC-initiated outbound calls to DCB (e.g. posting to DCB's webhook at luxliqdaes.cloud/api/webhooks/receive).

10. ACTIVATION PLANS — PATH A (WEEKS) & PATH B (DAYS)

PATH B — DCB as API Host (Recommended — Days to Live)

B1

Contact DCB — Request Inbound Credential Package

Email `operations@digcommbank.com` referencing DCB-NP-21399964. Advise DCB that NVC Fund Bank wishes to connect outbound to the DAES platform (`185.229.57.76 / luxliqdaes.cloud`) as an API consumer, and request that DCB issue NVC Fund Bank an inbound credential package: API key/token, HMAC signing key, DCB public key (RSA-2048), and webhook secret.

Owner: Compliance / Frank O. Ekejija · No infrastructure prerequisite — can start today

B2

Store Credentials and Configure Outbound Client

Upon receipt of DCB's credential package, store all items in NVC Fund Bank's Secrets vault. Configure the NVC API client to call `luxliqdaes.cloud/api` using DCB's API key, signing each request with HMAC-SHA256 in the `X-Signature` header. Set the webhook receive endpoint to DCB's live address (`luxliqdaes.cloud/api/webhooks/receive`). No server hosting required.

Owner: Infrastructure / DevOps · Blocked by B1 only

B3

Smoke Test + Agreement Countersignature

Send the USD 1.00 pacs.008 test transaction outbound to DCB's DAES endpoint. DCB's Certification Module issues the 6-document settlement package. NVC Fund Bank archives all six. Route the Bilateral Swap Agreement (NVCT ↔ VUSD) and the Correspondent Banking MOU to Felipe at DCB for countersignature within the same session.

Owner: Treasury Operations + Legal/Compliance · Blocked by B2

PATH A — NVC as API Host (Current Form — Weeks to Live)

A1

Infrastructure — Provision api.nvcfund.com

Allocate DNS and IP addresses (primary + failover) for `api.nvcfund.com`. Deploy the NVC Fund Bank production API service with OAuth 2.0, HMAC-SHA256 signing verification, and ISO 20022 pacs.008.001.08 message handling. Configure TLS 1.3 termination. Token endpoint at `auth.nvcfund.com/oauth/token`. Webhook receiver at `webhooks.nvcfund.com/dcb/notifications`. Add DCB egress IP `94.207.76.109 : 443` to the firewall allowlist.

Owner: Infrastructure / DevOps · PREREQUISITE — all A-steps blocked until complete

A2

Generate and Securely Transmit Credential Package to DCB

Security team generates all five credential items (Section 9) from the live `api.nvcfund.com` system: OAuth2 client_id/secret, HMAC-SHA256 key, RSA-2048 public key (PEM), webhook secret, primary + secondary IPs. Transmit to Felipe at DCB via verified encrypted secure channel. Coordinate through `compliance@nvcfund.com`.

Owner: Information Security / Compliance · Blocked by A1

A3

Smoke Test Execution + Agreement Countersignature

Upon DCB confirming credential receipt (estimated 15 minutes), DCB connects inbound to `api.nvcfund.com` and executes the USD 1.00 pacs.008 test transaction. NVC Fund Bank monitors inbound logs, confirms ledger booking, and verifies NVCT `transfer()` execution. Route Swap Agreement and Correspondent MOU to DCB for countersignature.

Owner: Treasury Operations + Legal/Compliance · Blocked by A2

11. PENDING LEGAL AGREEMENTS

DOCUMENT	STATUS	ACTION REQUIRED
NVCT ↔ VUSD Bilateral Swap Agreement	AWAITING DCB COUNTERSIGNATURE	Route to Felipe at DCB following smoke test confirmation
NVC Fund Bank — DCB Correspondent Banking MOU	AWAITING DCB COUNTERSIGNATURE	Route to Felipe at DCB in same session as swap agreement
NVC Fund Bank API Configuration Form (DCB-NP-21399964)	SUBMITTED APRIL 14, 2026	No further action — on record at DCB

12. TIMELINE

DATE / PERIOD	EVENT	STATUS
April 14, 2026	NVC Fund Bank submits API Configuration Form to DCB (Ref: DCB-NP-21399964) — 14 configuration points, OAuth 2.0, TLS 1.3, ISO 20022 pacs.008	COMPLETE
April 27, 2026	Felipe / DCB confirms integration readiness inbound — egress IP 94.207.76.109 supplied — USD 1.00 smoke test standing by	COMPLETE
Pending	NVC Fund Bank provisions api.nvcfund.com DNS + deploys production API	NOT STARTED
Pending	NVC Fund Bank generates and transmits credential package (5 items) to DCB via secure channel	NOT STARTED
T+15 min after creds	DCB executes USD 1.00 smoke test · NVC verifies inbound pacs.008 + ledger booking	STANDING BY (DCB)
Same session as smoke	Swap Agreement + Correspondent MOU routed to DCB for countersignature	PENDING

13. AUTHORIZATION

This report was prepared by Frank O. Ekejija for distribution to the NVC Fund Bank technical team as the primary reference document for the Digital Commercial Bank integration activation. Technical specifications in Section 7 incorporate DCB's own technical document (Direct Settlement Infrastructure, Rev. R3, March 27, 2026). Compliance and custody details in Section 4 are drawn from the DCB DAES Institutional Account Statement (Ref: DCB-20251230-490364, December 30, 2025). All technical team actions should be coordinated with the Infrastructure, Information Security, Treasury Operations, and Legal/Compliance functions in the sequence specified in Section 9.

AUTHORIZED BY: FRANK O. EKEJIJA · DATE: MAY 14, 2026

TECHNICAL LEAD — NVC FUND BANK · DATE: _____