CASHNET Application Setup — Complete Learning Handbook

From Fresher to Team Lead / Tech Architect

Generated: 05 Sep 2025, 19:43

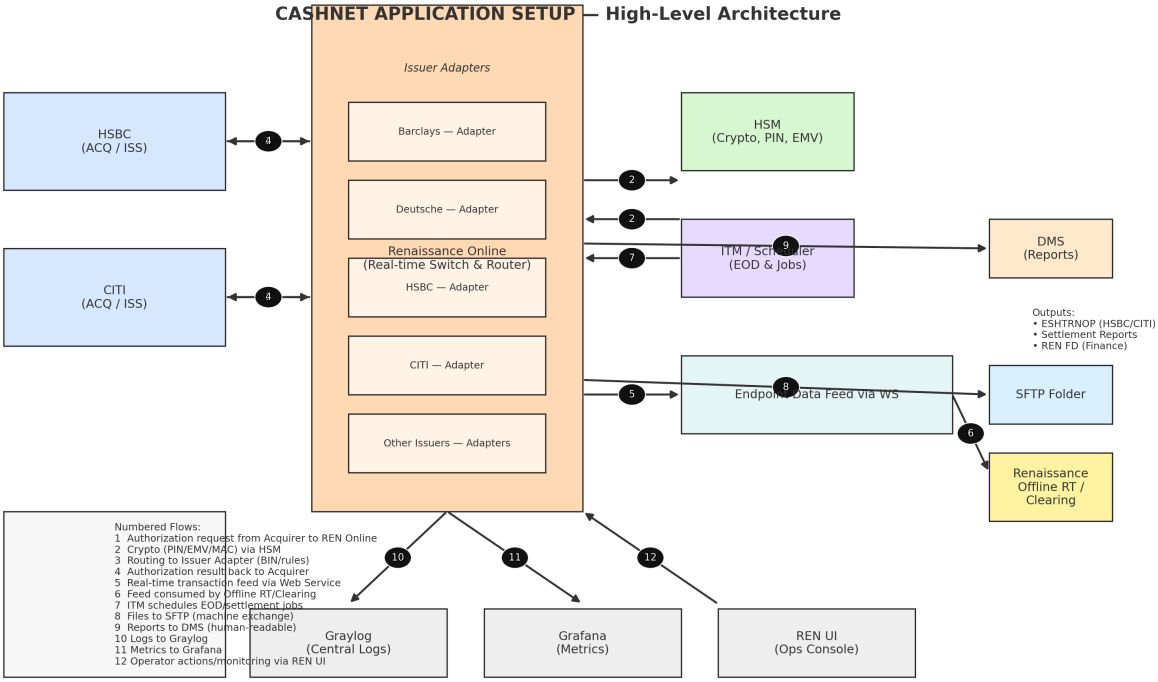

Figure 1: High-Level Architecture with Numbered Flows

0) How to Use This Handbook

This handbook is layered for different audiences. Read Sections 1–6 for a complete end-to-end picture; Sections 7–12 for operations and observability; Sections 10–20 for team leads and architects. Use the labs to practice offline.

1) One-Screen Mental Model (Text Map)

```
[ Merchants / ATMs / E■com ]
        |
        v
[ ACQUIRERS: HSBC, CITI ]  -->  [ RENAISSANCE ONLINE (REN) — real■time switch/router ]
                                        |         |             |             |
                                        |         |             |             +--> [ HSM ]  (Cryp
                                        |         |             |
                                        |         |             +--> [ ITM / Scheduler ] (EOD/Bat
                                        |         |
                                        |         +--> [ Issuer Adapters ] --> [ Issuer Banks (Ba
                                        |
                                        +--> [ Endpoint WS Feed ] --> [ Renaissance Offline RT/Cl

[ Outputs ]: REN --> SFTP Folder (machine files), REN --> DMS (reports)
[ Ops ]: REN --> Graylog (logs), REN --> Grafana (metrics), Ops <--> REN UI (console)
```

2) Components — What Each Block Does

Acquirers (HSBC ACQ/ISS, CITI ACQ/ISS)

Receive transactions from merchants/ATMs/e■com; forward to REN for authorization. Use ISO■8583 or JSON/XML over TLS. KPIs: TPS, timeout %, p95/p99 latency.

Renaissance Online (REN — the switch)

Normalizes messages, routes by BIN/rules, calls HSM for crypto, talks to issuer adapters, logs/metrics everything, and streams to WS feed. KPIs: TPS, router hit ratios, queue depth, error rates, latency.

Issuer Adapters (per bank)

Translate REN’s internal model to the bank’s protocol (ISO variant/MQ/HTTPS). Handle retries/timeouts and map fields. KPIs: issuer timeouts, adapter errors, bank latency/approval rate.

HSM (Hardware Security Module)

Performs PIN translation, EMV ARQC/ARPC, message MAC/HMAC, and secure key storage/derivation. KPIs: availability, crypto op latency, key version drift.

ITM / Scheduler

Orchestrates EOD and batch jobs (file builds, transfers, retries). KPIs: job success %, start/finish times, reruns.

Endpoint WS Feed

Near■real■time stream of posted transactions to Offline RT/Clearing. Protocol: HTTPS + signed payloads. KPIs: delivery lag, consumer ACKs, backlog size.

Renaissance Offline RT/Clearing

Reconciliation, exceptions, disputes support, and GL integration. Inputs: WS feed + SFTP files. KPIs: match %, exception volume, time■to■close.

SFTP Folder

Machine■readable files: ESHTRNOP, Settlement reports, REN FD. Temp■write + atomic rename; checksums; PGP; ACKs. KPIs: on■time delivery, checksum pass rate, pickup lag.

DMS (Document Management)

Human■readable reports (PDF/CSV/HTML) with access control and retention.

Observability

Graylog (logs), Grafana (metrics/alerts), and REN UI (RBAC■controlled ops console).

Inside REN (Mental Picture)

```
[ACQ Listeners] -> [Normalizer] -> [Router/BIN Rules] -> [Per■Issuer Queues] -> [Issuer Adapt
                                  \-> [Crypto Service] -> [HSM]
                                  \-> [Event Bus] ----> [Logs/Metrics/WS feed]
```

3) End-to-End Flows

3.1 Real-Time Authorization

```
1) ACQUIRER --> REN : Auth request (PAN/BIN, amount, EMV data/PIN, merchant/terminal)
2) REN --> HSM --> REN : Crypto (MAC verify, ARQC validate, PIN translate)
3) REN --> Issuer Adapter --> Issuer Bank : Routed by BIN/rules
4) Issuer Bank --> REN --> ACQUIRER : Approve/Decline (auth code, reason)
5) REN --> WS Feed : push txn facts downstream (near real time)
6) REN --> Logs/Metrics ; Ops watch REN UI/Grafana; investigate via Graylog
```

Typical SLAs: p95 < 1000 ms, p99 < 1500 ms, timeout rate < 0.5%.

3.2 Reversal / Refund / Void — Quick Definitions

Reversal: Cancel an authorization when issuer didn't receive commit or customer aborted. **Refund**: Return funds after a completed sale. **Void**: Cancel an un■settled transaction in the same batch/day.

3.3 EOD / Clearing / Settlement

```
A) ITM cutover window opens (e.g., T+0 23:30–23:59)
B) REN aggregates by acquirer/issuer/merchant
C) Build & drop files:
   - ESHTRNOP (HSBC/CITI special)  --> SFTP
   - Settlement Reports (others)    --> SFTP
   - REN FD (finance/GL)            --> SFTP and/or DMS
D) DMS publishes human■readable reports
E) Offline RT/Clearing consumes WS + SFTP and completes reconciliation
```

File practices: atomic rename from .part, checksums (.sha256), optional PGP, and downstream ACKs.

4) Data You Must Understand

4.1 ISO■8583 Common Fields (subset)

```
F2  PAN (masked in logs: 6+4)          F37 RRN                    F52 PIN Data (encrypted)
F3  Processing Code                     F38 Auth Code              F55 ICC Data (EMV TLVs)
F4  Amount, Transaction                 F41 Terminal ID            F60..63 Private data
```

```
F7  Transmission Date/Time              F42 Merchant ID             F64/128 MAC
F11 STAN                                F43 Merchant Name/Location
F49 Currency                            F22 POS Entry Mode
```

Keep a mapping sheet per issuer adapter; variants differ.

4.2 Transaction State Model (simplified)

```
RECEIVED -> NORMALIZED -> CRYPTO_OK -> ROUTED -> ISSUER_RESP {APPROVED|DECLINED|TIMEOUT}
        -> (if TIMEOUT) RETRY/CIRCUIT_BREAK
        -> (if APPROVED) CAPTURED? -> INCLUDED_IN_EOD? -> SETTLED
        -> (if REVERSAL/VOID/REFUND) state flows accordingly
```

4.3 Reconciliation Model (what must match)

Match counts and amounts by acquirer/merchant and by issuer; ensure one■and■only■once posting in Finance (REN FD vs GL).

5) Security You Cannot Skip

5.1 HSM & Keys — Core Vocabulary

LMK (Local Master Key): wraps other keys in HSM. **ZMK**: zone master key for inter■org exchanges. **ZPK**: zone PIN key for PIN blocks. **BDK**: base derivation key (DUKPT). PIN block formats ISO■0/1/3; EMV ARQC/ARPC. Use dual control and auditable ceremonies.

5.2 TLS/Certificates & Data Protection

Use mutual TLS where possible; rotate certs early; FIPS■approved ciphers. Mask PAN (6+4); never log CVV/PIN/keys. Apply PCI DSS scope, network segmentation, and PGP for files at rest.

6) Naming, Files & Conventions

```
<FEED>_<COUNTERPARTY>_<YYYYMMDD>_<HHMM>_RUN<nn>.<ext>
Examples:
ESHTRNOP_HSBC_20251005_2335_RUN01.csv
SETTLEMENT_GEN_OTHERS_20251005_2345_RUN01.csv
RENFD_FIN_20251005_2350_RUN02.csv

Sidecars:
*.part (temp)  -> final rename
*.sha256 (checksum)
*.asc (PGP signature/encryption)
ACK_<filename>.txt (downstream acknowledgment)
```

7) Observability (Logs, Metrics, Alerts)

7.1 Log Schema (JSON)

```
{
  "ts": "2025-10-05T12:34:56.789Z",
  "level": "INFO",
  "txn_id": "8f1b0f7b-90f1-4b6e-b6a3-28c0c9",
  "stage": "ROUTED_TO_ISSUER",
  "acquirer": "HSBC",
  "issuer": "BARCLAYS",
  "pan_masked": "512345******6789",
  "amount_minor": 12345,
```

```
  "currency": "INR",
  "latency_ms": 212,
  "decision": "APPROVED",
  "stan": "123456",
  "rrn": "052312345678",
  "bin": "512345",
  "mti": "0100",
  "processing_code": "000000"
}
```

Never log CVV, full PAN, clear PIN, or keys.

7.2 Metrics to Publish (Prometheus names)

```
ren_tps{route="hsbc"}
ren_latency_ms_p95{stage="issuer_call"}
ren_latency_ms_p99{stage="issuer_call"}
ren_error_rate{type="issuer_timeout"}
ren_queue_depth{name="barclays_out"}
hsm_availability_percent
sftp_delivery_lag_seconds{feed="ESHTRNOP"}
ws_feed_backlog_count
```

Alert starters: p95 > 1000ms (5m), p99 > 1500ms (5m), issuer_timeout > 0.5% (10m), HSM availability < 99.9% daily, SFTP lag > 900s during EOD.

8) Error Catalog (Operator-Facing)

Code	Category	Example Message	Typical Cause	Operator Action
VAL■001	VALIDATION_ERROR	Missing/invalid field (F4/F49)	Bad request from acquirer	Inspect sample; engage acquirer
CRY■001	CRYPTO_ERROR	ARQC validation failed	EMV data mismatch	Check EMV parameters; align with issu
CRY■002	HSM_UNAVAILABLE	Crypto service down	HSM link/HA issue	Failover; open incident
RTG■001	ROUTING_ERROR	BIN not routable	BIN table gap	Fix route in change window
ISS■001	TIMEOUT_ISSUER	No response from issuer	Bank outage/latency	Pause route; coordinate with bank
FIL■001	FILE_TRANSFER_ERROR	SFTP write/pickup failure	Network/perm	Retry; validate perms; manual drop if a
FIL■002	DUPLICATE_FILE	Run■id already processed	Re■emit w/o bump	Use new run■id; maintain idempotenc
SCH■001	SCHEDULER_JOB_ERROR	EMOD failed	Dependency/timeout	Check predecessor; rerun with logs
SEC■001	CERT_EXPIRED	TLS/PGP cert expired	Rotation missed	Emergency rotate; update trust stores

9) Operations Runbooks

9.1 Start-of-Shift Health Checks

```
[] Grafana: TPS/latency nominal? queues below thresholds?
[] Issuer adapters green? (Barclays/Deutsche/HSBC/CITI/Others)
[] HSM HA green; key versions as expected
[] ITM calendar correct for today (holidays? early cutover?)
[] SFTP free space > 20%; last night’s ACKs received
[] DMS publishing worked; reports reachable
[] Endpoint WS consumer lag < 60s
```

9.2 EOD Monitoring Checklist

```
[] Pre■cutover: inflight ≈ 0; queues drained
[] Job chain start times OK (ITM)
```

```
[] ESHTRNOP/Settlement/REN FD built with expected counts
[] SFTP .part -> final -> checksum -> ACK observed
[] DMS posts done; retention tags applied
[] Reco summary tallies with acquirer/issuer provisional totals
```

9.3 Incident Quick-Play (Issuer Down)

```
1) Confirm: spike in issuer timeouts (Grafana) + errors (Graylog ISS■001)
2) Contain: Reduce/stop route to failing issuer (REN UI) — communicate ETA
3) Coordinate: Call issuer NOC; get incident ticket & status
4) Recover: When green, warm■up with % traffic; monitor p95/p99
5) Post■incident: Notes + RCA draft + timeline
```

10) Testing & UAT Matrix

Functional

Approve, Decline, Partial Approve, Reversal, Void, Refund; EMV online/offline; PIN online; realtime feed idempotency; reconciliation totals match.

Negative / Failure Drills

Issuer timeout & retries; HSM failover; SFTP failure & idempotent rerun; BIN table mistake & fix.

Performance

Sustained target TPS with p95/p99 within SLA; burst 2× for 5 minutes; queue depth stays below watermarks.

Batch/EOD

Files generated with correct schema/counts; `.part`→final rename verified; checksum/PGP verify; ACKs written/consumed.

11) Change Management — Safe Patterns

BIN/Routing changes: test with test BINs in lower env, peer review, change window, snapshot + rollback plan.

New issuer onboarding: protocol agreement, adapter build/SIT, HSM keys & certs, observability, UAT, gradual prod cutover.

Key/Cert rotation: calendar dashboards, rotate early, dual control, auditable steps.

Scheduler updates: change via ticket; dry-run; watch predecessor/timeout chains.

12) High Availability, DR & Capacity

HA: REN/HSM/adapters in active-active or active-standby; queues with at-least-once semantics; dedupe by txn_id+stan+rrn.

DR: Target RTO ~1h; RPO near-zero for auth; replicate routing tables, keys (HSM backups), configs; quarterly drills.

Capacity: Plan for peak TPS × 2; watch queue depth & CPU; keep HSM utilization < 60% on peak.

13) Compliance & Audit Pointers (PCI-aware)

Scope: Card data, HSM, REN, logs with PAN fragments. Controls: RBAC, dual control for keys, secrets vault, encrypted disks, secure backups. Retention: raw logs 90 days hot/1 year cold; reports 7 years (example). Evidence: change tickets, key ceremonies, access reviews, incident records.

14) Do & Don’t

```
Do:
- Mask PAN (6+4), hash txn_id, redact secrets.
- Use atomic file writes and unique run■ids.
- Alert on lag/latency before customers call.
- Keep test BINs and golden transactions.

Don’t:
- Change routing/keys without ticket + peer review.
- Retry blindly on crypto errors.
- Re■emit batch with the same run■id.
- Store CVV or clear PIN anywhere.
```

15) Glossary

```
ACQ/ISS — Acquirer / Issuer
REN — Renaissance Online switch
HSM — Hardware Security Module (crypto)
ITM — Workload scheduler for batch/EOD
DMS — Document Management (reports)
BIN — Bank Identification Number (first 6–8 of PAN)
ARQC/ARPC — EMV request/response cryptograms
STAN / RRN — Trace numbers used for matching
DUKPT — Key derivation method at terminals
EOD — End of day cutover batch
```

16) Practical Labs (Do-It-Yourself)

Lab A — Build a mini normalizer & logger; Lab B — Routing engine; Lab C — Idempotent SFTP drop; Lab D — Observability dashboard; Lab E — Failure simulation.

17) Sample Artifacts You Can Reuse

Generic settlement CSV header:

```
run_id,file_type,org,batch_date,merchant_id,terminal_id,txn_id,stan,rrn,card_bin,amount_minor,
```

DMS report should include: summary by acquirer/issuer; exceptions list; reconciliation tie■outs.

Adapter retry policy (YAML):

```
issuer_adapter:
  timeout_ms: 1200
  retries: 2
  backoff_ms: 200
  circuit_breaker:
    failure_rate_threshold_percent: 5
    rolling_window_sec: 60
    open_state_cooldown_sec: 30
```

18) Security Playbooks (Short Form)

Key ceremony (rotation): schedule window, custodians A/B, validate HSM backups, load new keys (KCV), update references, rotate, monitor, archive evidence.

Cert renewal: CSR, CA-signed, stage & test, install in prod, monitor handshakes, rollback plan.

19) TL/TA Release Checklist

Release notes reviewed; backward compatibility; feature flags/canary routes; dashboards/alerts updated; runbooks amended; rollback plan tested.

20) Quick Reference Card

```
Latency guardrails: p95 < 1s, p99 < 1.5s, issuer timeout < 0.5%.
Files: .part -> final -> .sha256 -> ACK_*. Unique run■id.
Logs: JSON; mask PAN (6+4); include txn_id, stan, rrn, error_code.
Security: Dual control for keys; strong TLS; PGP for files; no CVV/PIN in logs.
Ops: Watch queues & latency; Graylog first, Grafana next; REN UI for controlled actions.
Changes: Ticket + peer review + lower■env tests + rollback plan.
```

Appendix: Numbered Flows (from Figure 1)

1 Authorization request from Acquirer to REN Online
2 Crypto (PIN/EMV/MAC) via HSM
3 Routing to Issuer Adapter (BIN/rules)
4 Authorization result back to Acquirer
5 Real-time transaction feed via Web Service
6 Feed consumed by Offline RT/Clearing
7 ITM schedules EOD/settlement jobs
8 Files to SFTP (machine exchange)
9 Reports to DMS (human-readable)
10 Logs to Graylog
11 Metrics to Grafana
12 Operator actions/monitoring via REN UI