CASHNET Application Architecture — Beginner to Pro Study Guide

A simple, complete learning path with diagrams, checklists, and quizzes

Generated on: 05 Sep 2025, 20:55

Table of Contents (What you'll learn)

Roadmap & How to Use This Guide

Level 0 (1 hour): Read Module 1 & 2 (the big picture + who does what).
Level 1 (2 hours): Do Module 3, 4, and 6 (flows, data, observability). Take the mini quizzes.
Level 2 (2 hours): Do Module 5 and 7 (security + EOD). Try one Practice Lab.
Level 3 (2–3 hours): Do Module 8 & 9 (resilience + runbooks). Take the Final Exam.
Keep the Glossary handy. Use the Checklists whenever you touch real systems.

Companion assets: the architecture diagram (Figure A) and optional video “A_Transaction_s_Secret_Journey.mp4”.

Module 1: Big Picture — What is CASHNET?

CASHNET is a payment processing setup. Its core, Renaissance Online (REN), is a real-time switch/router. It receives a payment request from an Acquirer (like HSBC or CITI), checks/securely translates secrets using the HSM, routes the request to the right Issuer Bank, and sends the decision back. Think of REN as a traffic cop with great memory and a safe (HSM).

```
[ Merchants / ATMs / E■com ]
        |
        v
[ ACQUIRERS ]  -->  [ RENAISSANCE ONLINE (REN) ]
                          |        |        |
                          |        |        +--> [ HSM ]  (crypto safe)
                          |        +--> [ ITM ] (EOD jobs)
                          +--> [ Issuer Adapters ] --> [ Issuer Banks ]
Outputs: REN --> WS Feed --> Offline RT/Clearing ; REN --> SFTP (files) ; REN --> DMS (reports)
Ops: Graylog (logs), Grafana (metrics), REN UI (console)
```

Plain words: REN = router + translator + recorder; HSM = lockbox for PIN/EMV; ITM = alarm clock for batches.

Module 2: Cast of Characters (People & Systems)

- **Acquirers**: Receive transactions from stores/ATMs/websites; forward to REN.
- **REN (Renaissance Online)**: Normalizes → routes → records; calls HSM; talks to Issuer Adapters.
- **Issuer Adapters**: Per■bank translators (each bank speaks a dialect).
- **Issuer Banks**: Approve/decline; own the customer's account.
- **HSM**: Hardware box for PIN/EMV and keys. Like a bank vault for secrets.
- **ITM/Scheduler**: Starts evening jobs: build files, send files, publish reports.
- **Endpoint WS Feed**: The "live stream" of transactions to the back■office.
- **Offline RT/Clearing**: Reconciliation, disputes, GL posting.
- **SFTP & DMS**: Files for machines (SFTP) and reports for people (DMS).
- **Observability**: Graylog (logs), Grafana (metrics), REN UI (operator console).

Module 3: Real-time Authorization — From Tap to Decision

```
1) ACQUIRER --> REN : Request (amount, card BIN, EMV data/PIN, merchant/terminal)
2) REN --> HSM --> REN : Check/compute cryptograms, PIN translation, MAC
3) REN --> Issuer Adapter --> Issuer Bank : Route by BIN/rules; speak bank’s dialect
4) Issuer Bank --> REN --> ACQUIRER : Approve/Decline (with code/reason)
5) REN --> WS Feed : Push facts for back■office to see quickly
6) REN --> Logs/Metrics : So ops can watch health in real time
```

Targets: p95 < 1s, p99 < 1.5s; issuer timeouts < 0.5%.

Mini Quiz (Module 3)

1 Q1: What does the HSM do during an authorization?

2 Q2: Who finally says “Approve” or “Decline”?

3 Q3: Why do we push a WS feed after authorization?

Module 4: Data Basics — ISO■8583 without the Scare

ISO■8583 is just a way to format messages. Think of it as labeled boxes. You don’t need to know every field — just the important ones.

```
Common fields (examples):
F2  PAN         -> the card number (mask in logs: first 6 + last 4)
F3  Proc Code   -> what we’re doing (purchase, refund, etc.)
F4  Amount      -> how much (minor units; e.g., paisa/cents)
F11 STAN        -> a local trace number
F37 RRN         -> a global reference for matching
F41 Terminal ID -> who swiped/tapped (terminal)
F42 Merchant ID -> which merchant
F52 PIN Data    -> encrypted PIN (never in clear)
F55 EMV Data    -> chip data blob (TLVs)
F64/128 MAC     -> proof message isn’t tampered
```

Tip: Keep a simple mapping sheet per bank adapter. Variants differ.

Mini Quiz (Module 4)

1. Q1: Which field should always be masked in logs (hint: PAN)?
2. Q2: What are STAN and RRN used for?
3. Q3: What is F55 used for in EMV transactions?

Module 5: Security — HSM & Keys in Plain English

The HSM is a locked box that holds sensitive keys and does secret math. You never take the secrets out; you send the question inside, and it returns the safe answer.

```
Key words (pun intended):
LMK — Local Master Key (master key inside HSM)
ZMK — Zone Master Key (for exchanging keys between orgs)
ZPK — Zone PIN Key (protects PIN blocks between orgs)
BDK — Base Derivation Key (for creating unique keys per txn/device)
PIN block formats: ISO■0/1/3 (know which partner uses which)
EMV: ARQC (request cryptogram) / ARPC (response cryptogram)
```

Golden Rules: dual control, split knowledge, audit trails, no clear PIN/CVV anywhere, rotate keys/certs early.

Mini Quiz (Module 5)

1 Q1: What is the job of the HSM in one sentence?

2 Q2: What does “dual control” mean and why?

3 Q3: Name one reason to rotate certificates early.

Module 6: Observability — Logs, Metrics, and the Ops Console

We can’t fix what we can’t see. Observability is how we see problems early.

Graylog (logs): Log JSON like this (never log CVV/PIN/keys).

```
{
  "ts": "...",
  "level": "INFO",
  "txn_id": "...", "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"
}
```

```
Grafana metrics to watch:
ren_tps, ren_latency_ms_p95/p99, 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
Alerts: p95 > 1000ms, p99 > 1500ms, issuer timeouts > 0.5%, HSM avail < 99.9%, EOD SFTP lag > 1
```

REN UI: Operator console with RBAC and audit. Use for safe actions (pause routes, drain queues).

Mini Quiz (Module 6)

1. Q1: Which tool do you search when tracing a single transaction?
2. Q2: Give one metric and threshold that should alert.
3. Q3: What kinds of actions belong in the REN UI?

Module 7: End-of-Day (EOD), Clearing & Settlement

```
A) ITM opens a cutover window (e.g., 23:30–23:59).
B) REN aggregates the day’s transactions by acquirer/issuer/merchant.
C) Build 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.
```

```
SFTP Handshake (safe pattern):
1) Write as .part (incomplete)
2) Rename to final when done (atomic)
3) Write .sha256 checksum (+ optional PGP .asc)
4) Wait for ACK_<filename>.txt from downstream
5) Mark job success only after ACK (or retry policy)
```

Mini Quiz (Module 7)

1. Q1: Why do we write files as .part first?
2. Q2: What is the purpose of the ACK file?
3. Q3: Name one EOD file type and its destination.

Module 8: Resilience — High Availability, DR & Capacity

High Availability (HA): duplicate components (REN, HSM, adapters) — active/active or active/sta
Queues: at■least■once delivery; dedupe by txn_id + stan + rrn to avoid double posting.
Disaster Recovery (DR): target RTO ~ 1 hour; RPO near■zero for auth; replicate configs, routing
Capacity: plan for peak TPS × 2; keep HSM util < 60% at peak; watch queue depth & CPU.

Mini Quiz (Module 8)

1. Q1: What is the difference between RTO and RPO?
2. Q2: Why do we dedupe by txn_id + stan + rrn?
3. Q3: What’s a safe headroom target for capacity?

Module 9: Runbooks & Checklists

Start■of■Shift:
[] TPS/latency okay? queues low?
[] Issuer adapters green?
[] HSM HA green; key versions correct
[] ITM calendar right for today
[] SFTP free space > 20%; last ACKs in
[] DMS reports published
[] WS consumer lag < 60s

Incident: Issuer Down
1) Confirm issue (Grafana p95/p99 + Graylog ISS■001 spikes)
2) Contain impact: pause/slow route in REN UI; inform stakeholders
3) Coordinate with issuer’s NOC; get ticket/status
4) Recover: warm■up traffic gradually; watch p95/p99
5) Post■incident: notes + draft RCA

Module 10: Do’s & Don’ts (Guardrails)

Do:
- Mask PAN (6+4). Hash txn_id. Redact secrets.
- Use atomic file writes + unique run■ids.
- Alert on latency/lag before customers notice.
- Keep test BINs + golden transactions.

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

Glossary — Scary words made simple

Acquirer: The bank that gets the transaction from the shop/ATM/website.
Issuer: The bank that owns the customer’s card/account.
REN: The smart router/translator in the middle.
HSM: The locked box that does secret math (PIN/EMV) and guards keys.
ITM: The job alarm clock that starts evening/batch tasks.
BIN: First digits of a card that tell us which issuer it belongs to.
STAN/RRN: Numbers used to match the same txn across systems.
EMV: Chip card rules; ARQC/ARPC are proof messages.
SFTP/DMS: Files for machines / Reports for humans.
PCI DSS: Security rules we follow to keep card data safe.

Practice Labs — Learn by Doing (No prod needed)

- Lab A: Parse a mock request → normalize JSON → log with txn_id/stage (mask PAN).
- Lab B: BIN routing table: given PAN, pick issuer; test gaps and overlaps.
- Lab C: Safe SFTP drop: write .part → rename → checksum → wait for ACK.
- Lab D: Emit fake metrics (tps/latency/errors) → visualize in a dashboard.
- Lab E: Simulate issuer timeout → watch retries & circuit breaker; HSM down → fail closed.

Module Quizzes (Short form)

M1–2

1 What is REN in one sentence?

2 Name two differences between SFTP and DMS.

3 Who finally approves or declines a transaction?

M3

1 List the 4 main steps from ACQ to decision.

2 Why do we call the HSM in the middle of the flow?

M4

1 Name three important ISO fields and why they matter.

2 What should never appear in logs?

M5

1 Explain 'dual control' in one sentence.

2 What are ARQC/ARPC used for?

M6

1 Give one Graylog field you’d filter on to trace a txn.

2 Name a metric and an alert threshold.

M7

1 Why use .part then rename on SFTP?

2 What is the purpose of an ACK file?

M8

1 What’s RTO vs RPO?

2 Why dedupe by txn_id + stan + rrn?

M9–10

1 Write one line from the start■of■shift checklist.

2 Give one 'Do' and one 'Don’t'.

Final Exam (Open book)

1. 1) Draw (text) a full real■time flow from ACQ to decision including HSM and Issuer Adapter.
2. 2) Describe the EOD flow and explain how idempotency is preserved.
3. 3) Propose 3 alerts that would catch issues before customers notice.
4. 4) Explain the role of the HSM, keys, and certificate rotation in keeping data safe.
5. 5) You see many ISS■001 timeouts to one issuer. Walk through confirm→contain→coordinate→recover.

Answer Key (Short hints)

M3 Q1: HSM verifies MAC/EMV, translates PIN; Issuer decides approve/decline; WS feed for back■o
M4 Q1: PAN(F2 masked), Amount(F4), Proc Code(F3); never log CVV/PIN/keys.
M5 Q1: Two people required for key actions; M5 Q2: EMV proof messages.
M6: Graylog filter by txn_id/rrn/stan; Alert p95>1000ms 5m.
M7: .part avoids half■reads; ACK proves consumer received.
M8: RTO=time to recover; RPO=data you can afford to lose; dedupe prevents double posting.
M9–10: Start■of■shift bullet; Do mask PAN; Don’t change keys without ticket.
Final: Use the module diagrams and checklists as scaffolding.

Appendix — Error Catalog (Operator Facing)

Code	Category	Why it happens	What to do
VAL■001	VALIDATION_ERROR	Missing/invalid fields	Fix input; engage acquirer
CRY■001	CRYPTO_ERROR	EMV/PIN/crypto mismatch	Check EMV params; partner alignment
CRY■002	HSM_UNAVAILABLE	HSM down/link broken	Failover HSM; raise incident
RTG■001	ROUTING_ERROR	BIN table gap	Fix route in change window
ISS■001	TIMEOUT_ISSUER	Issuer outage/slow	Pause route; coordinate; warm■up later
FIL■001	FILE_TRANSFER_ERROR	SFTP issue	Retry; perms; manual drop if approved
FIL■002	DUPLICATE_FILE	Run■id clash	New run■id; keep idempotency
SEC■001	CERT_EXPIRED	Missed rotation	Emergency rotate; update trust stores

Appendix — File Naming & Sidecars

```
<FEED>_<COUNTERPARTY>_<YYYYMMDD>_<HHMM>_RUN<nn>.<ext>
Sidecars: .part (temp) -> rename ; .sha256 (checksum) ; .asc (PGP) ; ACK_<filename>.txt
```

Appendix — Sample Metrics Names

```
ren_tps, ren_latency_ms_p95, ren_latency_ms_p99, ren_error_rate, ren_queue_depth, hsm_availabil
```

Appendix — Inside REN (Text Diagram)

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