

Government Integration Layer

Architecture & Interface Guide

How VisaChief.com connects to a department's visa processing system: the reference architecture, trust boundaries, data flows, integration patterns, interconnect options and the assurance path from sandbox to production cutover.

FRONT MATTER

Document Control & Contents

Field	Detail
Document title	Government Integration Layer — Architecture & Interface Guide
Companion document	VisaChief.com — Security & Data Protection Dossier (Government Edition)
Revision	1.0
Issue date	25 July 2026
Owner	Chief Technology Officer, VisaChief.com
Status	Reference architecture — the binding design is the integration schedule agreed with the department
Classification	OFFICIAL — Sensitive (Commercial-in-Confidence)
Audience	Departmental solution architects, integration and API teams, design authority, security assessors, project and procurement officers

Contents

§	Section	Purpose
1	Purpose & Design Principles	Why the layer exists and the rules it is built to
2	Reference Architecture	End-to-end component view and trust boundaries
3	Component Specification	What each element of the layer does
4	Network Topology & Zones	Deployment view and egress control
5	Lodgement Data Flow	Step-by-step sequence across the boundary
6	Integration Patterns & Protocols	Supported interfaces and when each applies
7	Interconnect Options	Three connectivity models the department may elect
8	Security Controls at the Boundary	Authentication, integrity, replay and rate control
9	Schema & Reference Data Governance	Versioning and backward compatibility
10	Environments & Conformance Testing	Sandbox to production, and how it is proven
11	Error Handling & Reconciliation	Failure taxonomy, retry policy, settlement
12	Observability, Audit & Evidence	What the department can see and retain
13	Performance & Availability Targets	Throughput, latency and service commitments
14	Responsibilities at the Boundary	Who owns what, unambiguously
15	Onboarding & Assurance Path	Gated route to production cutover
16	Assumptions, Dependencies & Open Items	What must be confirmed by the department
A	Appendix A — Indicative Interface Surface	Representative endpoints and payloads
B	Appendix B — Glossary	Terms used in this document

SECTION 1

Purpose & Design Principles

VisaChief.com prepares and manages visa applications. At the point of lodgement, and thereafter for status and requests for further information, the platform must exchange data with a department's visa processing system. The **Government Integration Layer** is the single component that performs that exchange.

It exists so that the department integrates with one hardened, contract-bound, independently assessable interface — never with the platform's internal services, and never with an AI component directly.

1.1 Design principles

- **One door.** All departmental traffic passes through the integration layer. No other VisaChief component may open a connection to a departmental endpoint.
- **The department controls its own ingress.** We connect on the department's terms — its gateway, its allow-list, its throttles, its certificate policy. We hold no credential capable of writing directly to a departmental data store.
- **Deterministic boundary.** Everything crossing the boundary is produced by deterministic code against a validated schema. AI-assisted output is reviewed by a registered migration agent before it can be packaged for lodgement.
- **Signed, versioned, idempotent.** Every payload carries a schema version, a signature and an idempotency key, so a retry can never create a duplicate case.
- **Evidence by default.** Every exchange writes an immutable audit record that the department can read, export and reconcile against its own logs.
- **Sovereign by construction.** The layer runs only in Australian regions; region pinning is enforced by policy-as-code, so a deployment elsewhere fails at the control plane.
- **Degrade safely.** If the department is unavailable, work queues durably and replays in order. Nothing is silently dropped and nothing is lodged twice.

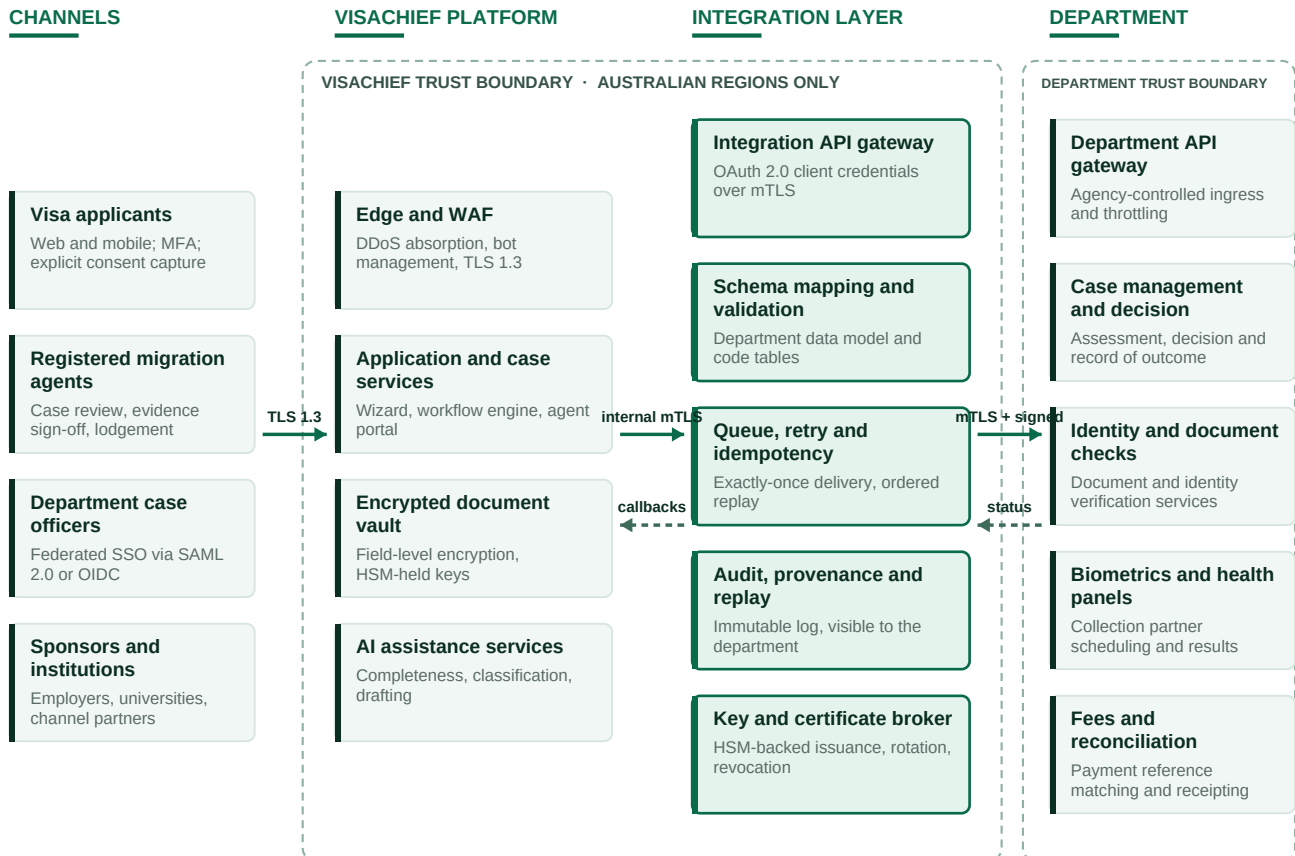
What this document is, and is not

This is a reference architecture. It shows a complete, implementable design and the options a department may choose between. It is not a claim of an existing connection to any particular departmental system. The binding design — endpoints, schemas, volumes and cutover — is agreed during design authority review and recorded in the integration schedule to the contract.

SECTION 2

Reference Architecture

Figure 1 shows the end-to-end view. Reading left to right: the people and systems that originate work, the VisaChief platform that prepares it, the integration layer that packages and transmits it, and the departmental environment that assesses and decides.



- Every cross-boundary call is mutually authenticated with certificate pinning; payloads are signed, versioned and idempotent.
- The department controls its own ingress. VisaChief holds no credential that can write directly to a departmental data store.
- Personal information never leaves Australian regions; the integration layer is the only component permitted to egress to the department.

Figure 1 — Reference architecture: VisaChief Government Integration Layer

SECTION 3

Component Specification

Each element of the integration layer has a single responsibility, so that a control can be tested in isolation and a failure has a bounded effect.

Component	Responsibility	Key controls
Integration API gateway	Terminates the connection to and from the department; the only network path across the boundary	Mutual TLS with certificate pinning, OAuth 2.0 client credentials, per-client rate limits, full request and response logging
Schema mapping and validation	Translates the internal case model to the department's data model and validates every field before transmission	Strict schema validation, code-table lookup, rejection of unmapped or out-of-range values, no silent coercion
Package builder and signer	Assembles the lodgement package — structured data plus documents — and signs it	Deterministic assembly, manifest checksums, detached signature, schema version stamped into the payload
Queue, retry and idempotency	Guarantees ordered, exactly-once delivery under failure	Durable queue, idempotency keys, exponential backoff with jitter, poison-message quarantine, operator-visible dead-letter handling
Callback receiver	Accepts signed status events from the department, or polls where inbound connections are not permitted	Signature verification, replay window, nonce tracking, strict payload allow-list
Audit, provenance and replay	Records every exchange in an append-only store and can reproduce exactly what was sent	Immutable storage with independent retention, hash-chained entries, department-accessible export
Key and certificate broker	Manages the cryptographic material used at the boundary	HSM-held private keys, automated rotation, revocation and expiry alerting, no plaintext key export
Reference data service	Holds department code tables, fee schedules and checklists	Version pinning, change notification, reproducible outputs tied to a stated version

SECTION 4

Network Topology & Zones

The deployment view matters as much as the logical view: it is what determines whether a compromise in one zone can reach applicant data or the departmental link.

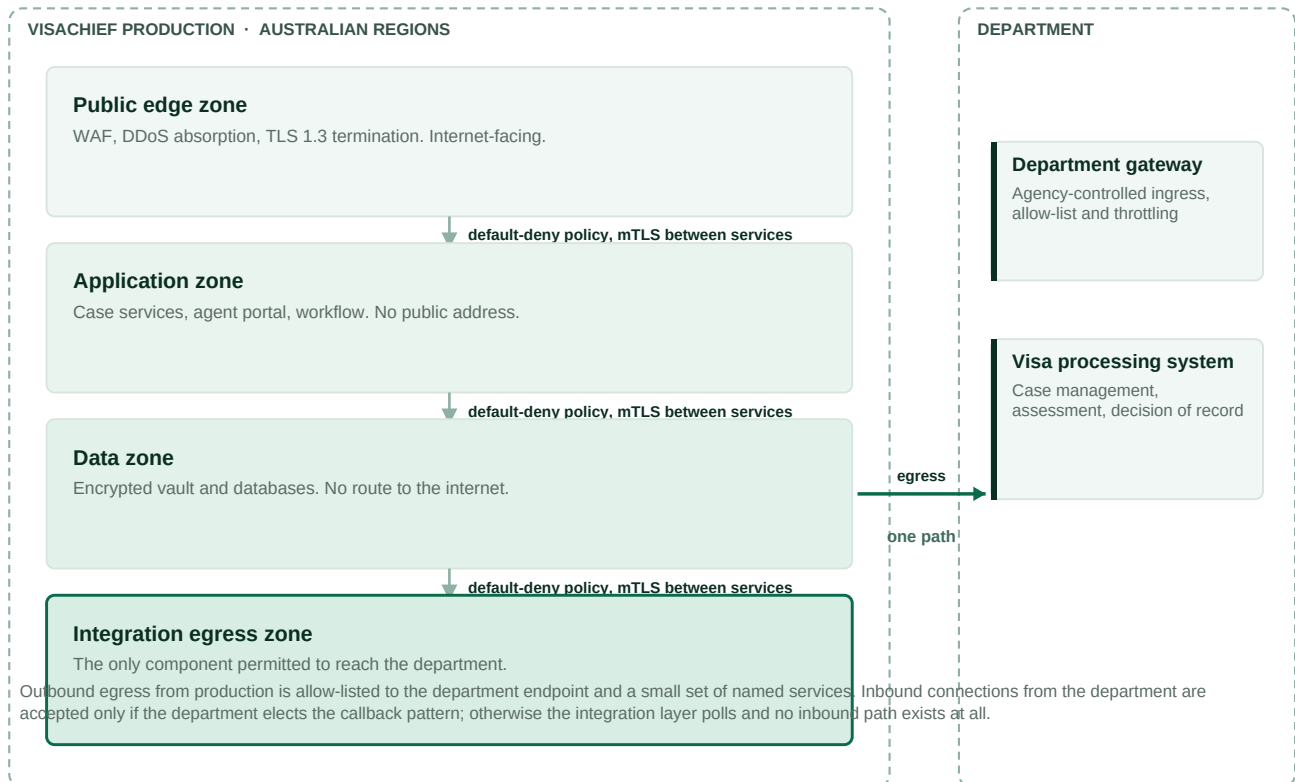


Figure 2 — Deployment zones and the single egress path

- Segmentation is default-deny: each zone may reach only its declared dependencies, enforced by network policy rather than convention.
- The data zone has no route to the internet. Document and case data can only be read through the application zone's authorisation checks.
- The integration egress zone holds the departmental certificates and is the only zone with an allow-listed route out. Compromise of the edge or application zone does not yield the ability to transmit to the department.
- Administrative access to any zone is just-in-time, peer-approved and session-recorded; there is no interactive shell in production.

SECTION 5

Lodgement Data Flow

The sequence below is the standard path for a prepared application. Each numbered step writes an immutable audit record that the department can read and process.

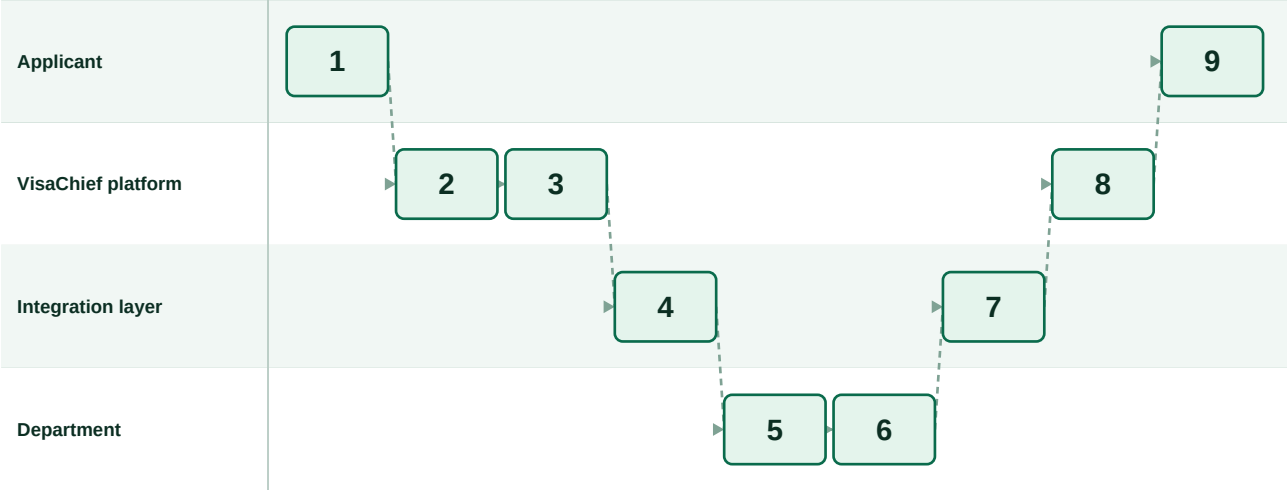


Figure 3 — Lodgement sequence across trust boundaries

Step	Action	Control applied
1	Applicant submits evidence and grants explicit consent	Consent recorded; upload type-verified, malware-scanned and quarantined
2	Vault stores documents; AI completeness check runs	Field-level encryption; identifiers minimised before inference
3	Registered migration agent reviews and signs off	Mandatory human decision point; agent identity bound to the case record
4	Integration layer builds and signs the lodgement package	Schema validation against the department model; manifest checksums; detached signature
5	Package transmitted to the department gateway	Mutual TLS, certificate pinning, idempotency key, backoff and ordered retry
6	Department acknowledges receipt and assigns a reference	Acknowledgement persisted to the immutable audit log
7	Status changes and requests for information returned	Signed callback or authenticated poll — the department elects which
8	Platform updates the case and notifies the agent	Tenancy-scoped authorisation on every read
9	Applicant notified; decision recorded against the case	Decision attributed to the department, never to VisaChief

SECTION 6

Integration Patterns & Protocols

Pattern	Protocol	Typical use	Assurance
Synchronous API	REST/JSON over HTTPS, OAuth 2.0 client credentials, mutual TLS	Eligibility checks, status lookup, reference data	Per-call authentication, rate limits, full request logging
Asynchronous submission	Queued POST with idempotency key and signed payload	Lodgement packages and document bundles	Exactly-once delivery, ordered replay, acknowledgement receipts
Event callback	Signed webhook to a VisaChief endpoint, or authenticated poll	Status changes, requests for further information	Signature verification, replay window, poll fallback where inbound is prohibited
Bulk exchange	SFTP with PGP-encrypted payloads, or brokered object-store handoff	Batch reconciliation and periodic reporting	Key-pair authentication, manifest checksums, transfer receipts
Identity federation	SAML 2.0 or OIDC with SCIM provisioning	Department staff access to the case portal	The department's own directory and MFA policy govern access and revocation
Reference data sync	Versioned pull of code tables and legislative instruments	Visa subclasses, fees, document checklists	Version pinning and change notification so outputs stay reproducible

Pattern selection

Departments that cannot accept inbound connections use the poll variant of the callback pattern; nothing else in the design changes. Departments with an existing whole-of-government API gateway use the gateway-brokered interconnect in Section 7 and keep their standard onboarding process.

SECTION 7

Interconnect Options

The department elects the connectivity model. All three carry identical application-layer controls — mutual TLS, signed payloads, idempotency and full audit. They differ only in network exposure and lead time.

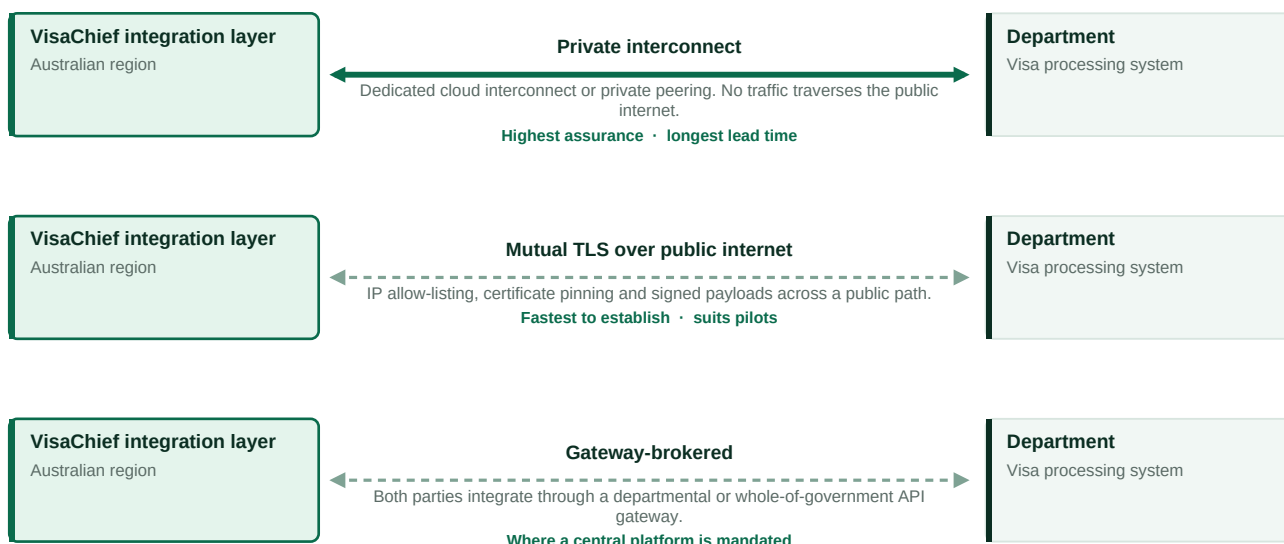


Figure 4 — Interconnect options; the department elects one

Option	Network exposure	Indicative lead time	Notes
Private interconnect	None — private path only	Longest; depends on the department's existing interconnect	Preferred where the department already operates cloud interconnect
Mutual TLS over public internet	Public path, allow-listed and pinned	Shortest	Suitable for pilots and lower-volume integrations; upgradeable later without redesign
Gateway-brokered	Determined by the central gateway	Governed by the gateway's own onboarding	The department's standard integration process applies unchanged

SECTION 8

Security Controls at the Boundary

The controls below apply to every exchange regardless of pattern or interconnect. Full platform security is documented in the companion Security & Data Protection Dossier.

Control	Implementation
Transport	TLS 1.3 with mutual authentication. Client and server certificates are pinned. Deprecated protocol versions and cipher suites are refused.
Client authentication	OAuth 2.0 client credentials bound to the presented client certificate, so a stolen token cannot be replayed from another host.
Payload integrity	Detached signature over a canonical form of the payload, plus manifest checksums for every attached document. A modified payload fails verification.
Replay protection	Nonce and timestamp with a bounded acceptance window; previously seen identifiers are rejected.
Idempotency	Every submission carries a client-generated idempotency key. A retry returns the original result rather than creating a second case.
Authorisation	Scoped credentials per environment and per interface. A sandbox credential cannot address production.
Rate and volume control	Client-side throttling to the department's published limits, with circuit breaking and backpressure so the department is never flooded.
Certificate lifecycle	HSM-held private keys, automated rotation, expiry alerting at 90, 30 and 7 days, and a rehearsed emergency revocation path.
Content safety	Documents are type-verified, malware-scanned and, for office formats, disarmed and reconstructed before they can be packaged.
Data minimisation	Only fields required by the department's schema are transmitted. Internal identifiers, model outputs and working notes are not.

SECTION 9

Schema & Reference Data Governance

Immigration rules change frequently. The integration must absorb that change without silent divergence between what the department expects and what we send.

- **Explicit versioning.** Every payload states its schema version. The department's supported versions are configured, not inferred.
- **Additive change by default.** New optional fields do not break existing consumers. Breaking changes require a new major version and a negotiated migration window.
- **Contract testing.** Schema conformance runs in our build pipeline against the department's published contract; a violation fails the build rather than reaching production.
- **Code tables are pulled, not hard-coded.** Visa subclasses, document types, fee schedules and country codes are synchronised from the department's reference data with a stated version.
- **Reproducibility.** Because outputs are tied to a pinned reference-data version, any past submission can be reproduced exactly as it was assembled.
- **Change notification.** The department is notified before we adopt a new schema or reference-data version in production, and either party may pause adoption.

9.1 Compatibility policy

Change type	Handling	Notice
New optional field	Adopted additively; no consumer impact	Release note
New mandatory field	Treated as breaking; new minor version with a dual-run period	Agreed in advance
Field removal or type change	Breaking; new major version	Negotiated migration window
Code-table value added	Picked up automatically on reference-data sync	Change log
Code-table value retired	Existing in-flight cases continue on the pinned version	Change log plus impact list

SECTION 10

Environments & Conformance Testing

Environment	Purpose	Data	Connectivity
Sandbox	Initial connectivity, certificate exchange, contract familiarisation	Synthetic only	Department test endpoint or mock
Staging	Conformance testing and pre-release validation, production-like configuration	Synthetic or irreversibly de-identified	Department test endpoint
Production pilot	Limited live volume under agreed caps	Live, with volume caps	Production endpoint
Production	Full service	Live	Production endpoint

10.1 Conformance suite

- Happy-path lodgement across each visa product in scope, verified end to end against the department's acknowledgement.
- Negative cases: schema violation, oversized document, unsupported document type, missing mandatory evidence — each must be rejected cleanly with an actionable error.
- Failure injection: department endpoint unavailable, slow response, partial failure mid-batch, duplicate submission — verifying queueing, ordered replay and idempotency.
- Security tests: expired certificate, revoked certificate, invalid signature, replayed nonce, sandbox credential against production — all must fail closed.
- Reconciliation: a full day of traffic reconciled line-by-line between our audit log and the department's records, with a required zero-variance result before cutover.

No environment is promoted without documented exit criteria signed by both parties. Non-production environments never contain live personal information.

SECTION 11

Error Handling & Reconciliation

The design principle is simple: fail loudly, never silently, and never twice.

Failure	Behaviour	Visibility
Transient network or 5xx from the department	Exponential backoff with jitter, ordered retry within the agreed window	Retry count and outcome in the audit log; alert on threshold breach
Department endpoint unavailable	Work queues durably; nothing is dropped; replay resumes in submission order	Operational alert; agent-visible case status
Schema validation failure	Rejected before transmission; the case is returned to the agent with a specific field-level error	Agent notification; never silently corrected
Signature or certificate failure	Fail closed; no fallback to an unauthenticated path	Immediate security alert and escalation
Duplicate submission	Idempotency key returns the original result	Recorded as a duplicate attempt, not a new case
Poison message	Quarantined to a dead-letter queue after the retry budget; the queue is not blocked for other work	Operator review with a documented remediation path
Partial batch failure	Successful items are committed; failed items are isolated and replayed individually	Per-item outcome in the reconciliation report

A daily reconciliation compares our audit log against the department's acknowledgements and flags any variance for investigation within one business day. The reconciliation report is available to the department.

SECTION 12

Observability, Audit & Evidence

- **Immutable exchange log.** Every request, response, retry and acknowledgement is written to append-only storage with independent retention. Production credentials cannot alter or delete it.
- **Department access.** The department may subscribe to, or export, the audit records relating to its own integration — so it can reconcile against its records without relying on our assertion.
- **Provenance.** Each submission records the case, the agent who signed off, the schema and reference-data versions used, and the exact payload hash, so any past submission can be reproduced.
- **Metrics.** Volume, latency, error rate, retry rate and queue depth are reported against the targets in Section 13.
- **Alerting.** Certificate expiry, signature failure, authorisation failure, queue-depth growth and reconciliation variance all raise operational alerts with defined escalation.
- **Incident notification.** Any security incident affecting the integration is notified to the department within 24 hours of confirmation, with updates at agreed intervals.

SECTION 13

Performance & Availability Targets

Targets are set at design authority review against the department's expected volumes; the figures below are the standard commitments in the absence of agreed alternatives.

Measure	Target
Integration layer availability	99.9% monthly, excluding agreed maintenance windows
Synchronous API response (95th percentile)	Under 800 ms, excluding department-side time
Lodgement package submission	Transmitted within 60 seconds of agent sign-off under normal operation
Status propagation to the case	Within 5 minutes of receipt of a callback, or one polling interval
Recovery point objective	15 minutes or better for integration state
Recovery time objective	4 hours or better for the integration layer
Queue drain after an outage	Full backlog replayed in submission order within the agreed window
Planned maintenance notice	Minimum 5 business days

SECTION 14

Responsibilities at the Boundary

Clear demarcation prevents the gaps where incidents happen.

Item	VisaChief.com	Department
Integration layer build and operation	Owns	Reviews and approves the design
Interface specification and data model	Implements to specification	Owns the specification and code tables
Certificates and key rotation	Issues and rotates its own; supports pinning	Issues and rotates its own
Ingress control, throttling and quotas	Respects published limits	Owns
Payload content and completeness	Validates against schema and completeness rules	Owns assessment and the decision
Audit log of exchanges	Produces the immutable log and provides access	Retains per its own records authority
Reconciliation	Produces the daily report and investigates variance	Confirms against its own records
Incident notification across the boundary	Within 24 hours of confirmation	Per its own policy
Environment provisioning	Sandbox, staging and production on our side	Test endpoints and test data on its side
Change and release notice	Notifies before adopting a new schema version	Notifies of interface or reference-data change

SECTION 15

Onboarding & Assurance Path

Each gate has documented exit criteria signed by both parties. No gate is skipped, and volume is capped until the final gate closes.

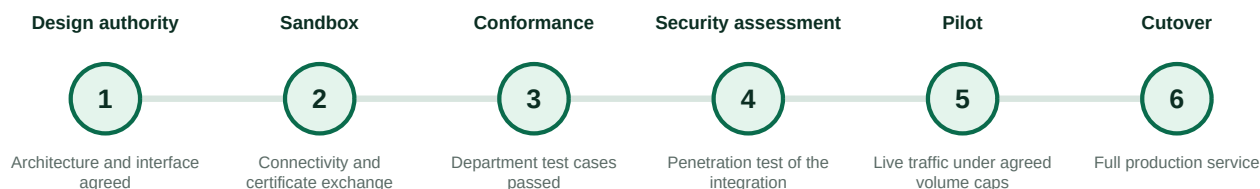


Figure 5 — Gated onboarding path to production cutover

Gate	Exit criteria	Owner
1 Design authority	Interface specification, data model, interconnect option and volumes agreed and recorded in the integration schedule	Joint
2 Sandbox	Mutual TLS established, certificates exchanged and pinned, first authenticated call succeeds	Joint
3 Conformance	Full conformance suite passed, including negative and failure-injection cases; results signed off	Department
4 Security assessment	Independent penetration test of the integration completed; critical and high findings remediated and retested	VisaChief, evidence to the department
5 Pilot	Agreed pilot volume processed with zero reconciliation variance over a continuous agreed period	Joint
6 Cutover	Volume caps lifted, runbooks and escalation matrix published, support model live	Joint

SECTION 16

Assumptions, Dependencies & Open Items

Stated plainly, so that design authority review starts from an accurate position rather than an optimistic one.

Item	Position	To be confirmed by the department
Departmental interface availability	This design assumes the department exposes, or will expose, a machine interface for lodgement and status	Whether such an interface exists today, and its specification
Lodgement authority	Final review and lodgement is performed by a registered migration agency in our partner network	Any additional accreditation the department requires
Inbound connections	Design supports both callback and poll	Whether inbound connections to VisaChief are permitted
Interconnect	Three options offered	Which option, and the department's lead time
Identity and document verification	Referenced generically	Which verification services are in scope and on whose credentials they are invoked
Volumes	Targets in Section 13 assume volumes agreed at design authority	Expected peak and average volumes
Retention	Configurable to the department's schedule	Applicable records authority and disposal schedule
Assurance requirement	IRAP assessment available, scoped to the engagement	Whether IRAP, and at what classification

APPENDIX A

Indicative Interface Surface

Representative only. The binding surface is the department's published specification; where none exists, we propose the following as a starting point for design authority review.

Operation	Method	Purpose	Idempotent
Reference data — code tables	GET	Retrieve visa subclasses, document types, fee schedule with version	Yes
Case — submit lodgement package	POST	Transmit structured application data and document manifest	Yes, via idempotency key
Document — upload	PUT	Transfer an individual document referenced in the manifest	Yes, via content hash
Case — acknowledge	GET	Retrieve the department reference assigned to a submission	Yes
Case — status	GET	Poll current status where callbacks are not used	Yes
Event — callback receiver	POST	Receive signed status and request-for-information events	Yes, via event identifier
Case — respond to request	POST	Submit further evidence against a departmental request	Yes, via idempotency key
Reconciliation — daily manifest	GET	Retrieve the day's submissions and outcomes for variance checking	Yes

APPENDIX B

Glossary

Term	Meaning
Integration layer	The VisaChief component that performs all exchange with the department
Idempotency key	A client-generated identifier ensuring a retried submission cannot create a duplicate case
mTLS	Mutual Transport Layer Security — both client and server present and verify certificates
Certificate pinning	Accepting only a specific, expected certificate rather than any certificate a public authority has signed
Detached signature	A cryptographic signature stored alongside, rather than inside, the payload it authenticates
Dead-letter queue	A holding queue for messages that cannot be processed, so they do not block other work
Conformance suite	The agreed set of tests a department requires before an integration may carry live traffic
Reconciliation variance	Any difference between our record of exchanges and the department's record

This document describes a reference architecture for connecting VisaChief.com to a departmental visa processing system. It is commercial-in-confidence, provided for evaluation and design authority review, and does not itself form a contractual warranty; binding obligations are those set out in the executed agreement and its integration schedule. VisaChief.com prepares and manages applications; visa decisions are made solely by the relevant government authority.