

Identity Conversion Block (IDCB)

Business Requirements Document (BRD)

Version: 5.0

Date: Sep 20, 2026

Status: Final Review

Document Control

Version	Date	Author	Changes
5.0	Sep 20, 2026	Cross-Functional Team	Final Review

Table of Contents

1. Overview **5**
1.1 Purpose and Scope 5
1.1.1 Purpose 5
1.1.2 The Problem IDCB Solves 5
1.1.3 In Scope - Eight Core Capabilities 6
1.1.4 Out of Scope 7
1.2 Business Value 7
1.2.1 For Citizens 7
1.2.2 For Government Service Providers 8
1.2.3 For Government Leadership 8
1.3 Success Metrics 9
Only Availability, Performance, Privacy and Audit metrics form the contractual service levels; Adoption, Reliability and Compliance metrics are programme targets for RGoB **10**
2. Identity Conversion Block Overview **10**
2.1 IDCB Overview 10
2.1.1 Position in RGoB DPI Ecosystem 10
2.2 IDCB Roles and Responsibilities 10
2.3 Integration with Other Building Blocks 11
3. Usage Scenarios **13**
4. IDCB Capabilities and Requirements **13**
4.1 Capability 1: Identity Type and Domain Registry Management 13
4.1.1 Sub-Capabilities 14
4.1.2 Process Flow: Identity Type and Domain Registration 14
4.1.3 Functional Requirements - Identity Type and Domain Registry Management 16
4.2 Capability 2: Conversion Rule and Policy Engine 18
4.2.1 Sub-Capabilities 18
4.2.2 Process Flow: Conversion Rule Authoring and Activation 19
4.2.3 Functional Requirements - Conversion Rule and Policy Engine 20
4.3 Capability 3: Identity Resolution and Mapping Execution 22
4.3.1 Sub-Capabilities 23
4.3.2 Functional Requirements - Identity Resolution and Mapping Execution 24
4.4 Capability 4: Pseudonymisation and Privacy Protection 26
4.4.1 Sub-Capabilities 27
4.4.2 Functional Requirements — Pseudonymisation and Privacy Protection 27
4.5 Capability 5: Mapping Lifecycle Management 29
4.5.1 Sub-Capabilities 29

4.5.2 Functional Requirements - Mapping Lifecycle Management..... 29
4.6 Capability 6: Administrative Governance and Consumer Management..... 31
4.6.1 Sub-Capabilities..... 32
4.6.2 Functional Requirements - Administrative Governance and Consumer Management.. 32
4.7 Capability 7: Security and Key Management..... 34
4.7.1 Sub-Capabilities..... 34
4.7.2 Functional Requirements - Security and Key Management..... 35
4.8 Capability 8: Integration and API Management..... 37
4.8.1 Sub-Capabilities..... 37
4.8.2 Functional Requirements - Integration and API Management..... 38
4.9 Non-Functional Requirements..... 40
4.9.1 Performance Requirements..... 40
4.9.2 Availability and Scalability Requirements..... 41
4.9.3 Security Requirements..... 41
4.9.4 Privacy and Compliance Requirements..... 41
4.9.5 Environments, Standards and Operations..... 42
5. Solution and Integration Architecture..... 42
5.1 Logical Component Architecture..... 42
5.2 Integration Architecture..... 44
5.2.1 Key Integration Specifications..... 44
5.2.2 Failure Handling..... 44
6. Data, Security and Compliance..... 46
6.1 Data Model (Indicative)..... 46
6.1.1 Table: identity_domains..... 46
6.1.2 Table: identity_types..... 47
6.1.3 Table: trust_boundaries..... 48
Field..... 48
Type..... 48
Description..... 48
6.1.4 Table: conversion_rules..... 48
6.1.5 Table: identity_mappings..... 49
6.1.6 Table: conversion_audit_log..... 50
6.1.7 Table: registered_consumers..... 51
6.2 Data Security..... 52
6.3 Privacy and Compliance..... 52
7. Appendices..... 54
Appendix A: Glossary..... 54
Appendix B: Pseudonymisation Algorithms..... 55

Appendix C: API Reference Summary....55
Appendix D: Use Case Domain Reference....56
Appendix E: Key Performance Indicators....57
Appendix F: External References....58
Appendix G: Domain Integration Patterns....58
8. Usage Scenarios....59
8.1 Scenario 1: Vehicle Owner Identification Without CID Exposure....59
8.2 Scenario 2: Emergency Health Access Without CID Sharing....61
8.3 Scenario 3: Property Tax Assessment with Multi-Domain Resolution....62
8.4 Scenario 4: Applying for Vehicle Registration on My Bhutan Portal....63
8.5 Scenario 5: Passport Fine Check Without Linking Records....64

1. Overview

1.1 Purpose and Scope

1.1.1 Purpose

The Identity Conversion Block (IDCB) is a privacy-preserving identity mapping building block of the Bhutan DPI Blueprint, designed following GovStack building block principles. It enables secure, contextual translation of identities between heterogeneous government domains without exposing sensitive primary identifiers to requesting systems.

In traditional digital government architectures, identity domains are siloed and tightly coupled to specific sectoral systems — personal identifiers in the Civil Registry, vehicle registration numbers in RSTA, property parcel numbers in the Land Cadastre, taxpayer IDs in the Revenue Authority, and patient IDs in health systems. This fragmentation poses significant operational and privacy challenges when cross-domain services are required. Government systems struggle to perform cross-context operations such as identifying the legal owner of a vehicle, mapping delegation responsibilities from a company to its director, or resolving a property holder's tax obligations — without either exposing sensitive base identifiers or requiring costly manual reconciliation.

IDCB closes this gap by acting as a dedicated identity-translation layer between domains: it resolves an identity in one domain to its equivalent in another, under rules scoped to a specific purpose and trust boundary, and returns only a privacy-safe pseudonym — never the underlying identifier. (See Section 5 for the technical architecture.)

1.1.2 The Problem IDCB Solves

Problem	Impact Without IDCB	IDCB Solution
Identity silos across government domains	Cross-domain services require manual reconciliation; officers access more data than needed	IDCB resolves relationships across domains without exposing base identifiers
Privacy risks from direct identifier sharing	Personal identifiers (CIDs) exposed to all systems in a workflow, violating data minimisation principles	Pseudonymised opaque references returned; requesting system never receives raw identity
No mechanism for contextual identity conversion	Same conversion rule applied regardless of purpose, creating over-disclosure	Policy-aware engine returns different results for same identity depending on operational context
Inability to support indirect notifications	Notification systems must hold personal data to deliver alerts to asset owners	IDCB converts asset ID to pseudonymised owner reference; NTFB notifies without knowing the underlying identity

Lack of audit trail for cross-domain identity use	No traceable record of when and why identities were resolved across domains	Tamper-evident, cryptographically signed audit log of every conversion with purpose and context
Fragmented regulatory compliance	Each agency manages identity sharing ad hoc; compliance with Bhutanese data protection law is hard to demonstrate systematically	Centralised policy engine with legal basis tagging and compliance reporting across all domains

1.1.3 In Scope - Eight Core Capabilities

IDCB encompasses eight core capabilities covering the complete identity conversion lifecycle:

No.	Capability	Description
1	**Identity Type and Domain Registry Management**	Register and govern identity types, domains, identity relationships, trust boundaries, registry health and pseudonym prefixes.
2	**Conversion Rule and Policy Engine**	Author, version, simulate, and publish conversion rules per domain pair and context; enforce purpose and legal basis.
3	**Identity Resolution and Mapping Execution**	Execute real-time, bulk, one-to-many and recursive identity conversions, with trace support and reverse resolution for asset identifiers.
4	**Pseudonymisation and Privacy Protection**	Generate privacy-preserving pseudonyms, enforce domain isolation, enforce data minimisation, and detect scope violations.
5	**Mapping Lifecycle Management**	Create mappings automatically, expire them, revoke them with cascade, detect out-of-date links, and revoke in bulk.
6	**Administrative Governance and Consumer Management**	Admin UI with rule editor, consumer registration and credentials, consumer dashboard, expiry notices, roles,roles and governance dashboard.
7	**Security and Key Management**	AES-256 encryption, certified HSM key management with dual control, mutual TLS with NDI or SSO tokens, signed audit trail, and secrets and certificate management.

8	**Integration and API Management**	Serves My Bhutan Portal, government service systems, and service-provider and back-office systems through a versioned REST API with NDI or SSO tokens; registry access through INTP; events to EVTB and audit records to JLB; notification support for NTFB; rate limiting and health endpoints.

1.1.4 Out of Scope

Out-of-Scope Item	Handled By
Primary identity creation and management	National Digital Identity (NDI)
User authentication and credential verification	National Digital Identity (NDI)/SSO
Master data management for domain registries	Respective sectoral domain systems (RSTA, Civil Registry, etc.)
Consent lifecycle management	Embedded in NDI SSI model per Blueprint decision
Storage of domain-specific application data	Respective service databases
Notification delivery to end users	Notification Block (NTFB)
User interface for citizens, businesses and service-provider officers	My Bhutan Portal
Changes to agency systems to store and use pseudonyms instead of CIDs/ Source Identifier	Each domain agency (IDCB vendor provides APIs, documentation and integration support)
NDE platform (APIG, INTP, EVTB) build and operation	NDE platform team
Business data held by agencies (e.g., fines, tax due)	Respective agency systems; IDCB only converts identities
Agency-side registry APIs that IDCB queries	Each domain agency, exposed through INTP

1.2 Business Value

1.2.1 For Citizens

Value Dimension	Description

Privacy Protection	Personal identifiers (CIDs) are never shared across government systems; citizens transact in digital services without their primary identity being broadcast to all participating systems
Seamless Cross-Domain Services	Government services that span multiple domains (tax, property, transport) operate without requiring citizens to repeatedly verify their identity for each domain
Reduced Data Exposure Risk	Pseudonymisation minimises the impact of data breaches in individual domain systems; compromise of one domain's pseudonym table cannot be used to re-identify citizens in other domains

1.2.2 For Government Service Providers

Value Dimension	Description
Secure Cross-Domain Interoperability	Agencies can request identity resolution across domain boundaries without building bespoke point-to-point integrations or holding copies of other agencies' identifier databases
Compliance by Design	Built-in pseudonymisation, purpose limitation, and data minimisation enforcement reduces per-agency compliance burden; legal basis tagging creates an auditable compliance record
Automation of Manual Reconciliation	Identity resolution that currently requires officers to manually look up records across multiple systems is automated, reducing processing time and error rates
Audit Readiness	Complete tamper-evident conversion logs with cryptographic signatures satisfy regulatory audit requirements without additional implementation effort per agency
Indirect Notification Support	NTFB can notify vehicle owners, property holders, and asset custodians without ever receiving or storing their personal identifiers

1.2.3 For Government Leadership

Value Dimension	Description
Systemic Privacy Risk Reduction	Centralised pseudonymisation eliminates the need for each agency to implement its own identity de-identification logic, reducing systemic risk
Regulatory Compliance	Supports compliance with Bhutanese law, including the Information, Communications and Media Act and the National Digital Identity Act 2023,

	and follows internationally recognised principles such as data minimisation and privacy by design (as in GDPR Articles 5 and 25).
Foundation for Digital Services Innovation	IDCB enables new categories of cross-domain government services that are currently impossible due to privacy constraints on direct identifier sharing
Citizen Trust and Transparency	Demonstrates Royal Government commitment to privacy-preserving digital governance, reinforcing citizen trust in the digital public infrastructure
Cost Efficiency	Eliminates redundant per-agency identity reconciliation infrastructure; expected reduction in identity reconciliation overhead across participating agencies, to be measured against a baseline taken before go-live

1.3 Success Metrics

Category	Metric	Target
Availability	IDCB service uptime, measured monthly, excluding outages of NDE, NDI and agency registries	**≥ 99.9% monthly**
Performance	Conversion time from IDCB store or cache (95th percentile)	**≤ 50ms**
Performance	Conversion time with live registry query (95th percentile)	**≤ 150ms**
Performance	Bulk throughput, sustained for 10 minutes with a registry simulator	**≥ 5,000 requests per second**
Privacy	Base identifiers (CID) exposed to any calling system	**0**
Privacy	Scope Violation Rate (attempted conversions outside policy)	**0 undetected violations**
Audit	Conversion Operations Logged	**100%**
Adoption	Government domains using IDCB ≥ 10 within 24 months of go-live	**≥ 10 major domains**
Adoption	Cross-domain queries per month ≥ 1,000,000 within 24 months of go-live	**≥ 10" and "≥ 1,000,000**
Reliability	Mapping accuracy: share of sample checks where the result matched the registry	**≥ 99%**
Compliance	Privacy Audit Findings (Critical)	**0**

Compliance	Conversion Operations with Legal Basis Reference	**100% of active contexts**
Performance	Real-time throughput, sustained peak	**≥ 1,000 requests per second**

Only Availability, Performance, Privacy and Audit metrics form the contractual service levels; Adoption, Reliability and Compliance metrics are programme targets for RGoB.

2. Identity Conversion Block Overview

2.1 IDCB Overview

2.1.1 Position in RGoB DPI Ecosystem

Building Block Group	Digital Identity
GovStack BB Layer	Digital Identity — Privacy-Preserving Identity Mapping
Function	Cross-domain identity resolution and pseudonymisation
Scope	Cross-cutting service for all government domains requiring identity translation
Role in RGoB DPI	Identity translation and pseudonymisation bridge enabling secure cross-domain digital government services

2.2 IDCB Roles and Responsibilities

Primary Responsibility: Privacy-preserving identity conversion platform enabling secure cross-domain identity resolution without exposing sensitive primary identifiers to any requesting system.

Direction	Detail
IDCB Receives	Identity conversion requests from authorised domain systems; source identifiers and target domain specifications; mapping policy configurations from administrators; mapping lifecycle events (expiration, revocation); purpose and context declarations for each conversion request; conversion requests made by My Bhutan Portal on behalf of an agency
IDCB Provides	Domain-specific surrogate pseudonymised identifiers; identity resolution between domains; privacy-preserving pseudonyms; mapping validation and enforcement; conversion audit trails; mapping lifecycle management APIs; event notifications for mapping changes; trace records; mediated yes/no checks between domains
IDCB Manages	Identity mappings between domains; conversion rules and policies; mapping scopes and contexts; pseudonymisation algorithms and key material (via

	HSM); mapping expiration and revocation; tamper-evident conversion audit logs; access control for mappings per consumer and context
Critical Boundary	IDCB converts and maps identities but does not create, authenticate, or authorise them. IDCB also does not hold or interpret business data. In a Mediated Check (Capability 3), it only carries a pre-registered yes/no question to the agency that owns the data, and returns that agency's answer. It assumes identities are already established in authoritative domain systems and provides translation services while enforcing privacy constraints. Identity creation is NDI's responsibility; IDCB decides whether a conversion request is allowed (by checking rules, trust boundaries and caller scope). Deciding whether a user may use a service remains the responsibility of that service. Re-identification is never available on demand - a real identity can only be recovered through the strictly governed Authorised Retrace capability (Capability 4), not through ordinary conversion or routine admin access.
Governance Model	IDCB is a shared platform used by many ministries, departments, and agencies, each acting as an independent domain owner (e.g., RSTA for vehicles, Civil Registry for citizens, Revenue for tax). Day-to-day rule authoring and domain administration is delegated to each agency's own Data Steward and Domain Architect, scoped strictly to their own domain(s) (see FR-6.7). The IDCB platform itself is owned and operated by GovTech Agency, which is responsible for hosting, operations, onboarding of agencies, and the contract with the vendor.

2.3 Integration with Other Building Blocks

Note: INTP, APIG, and EVTB are delivered as sub-components of the single National Digital Exchange (NDE) platform (built on WSO2 - API Manager, Enterprise Integrator/ESB, and Streaming Integrator respectively). They are listed as separate rows below because each serves a functionally distinct purpose for IDCB, but they share the same underlying platform and availability profile — an NDE outage affects all three simultaneously.

Code	Block Name	Integration Purpose	Pattern (indicative)	Dependency Strength
INTP	**Interoperability Platform (NDE and ESB)**	Mediated gateway for all real-time outbound queries from IDCB to authoritative domain registries (all Pattern A registries)	REST API (Sync)	Required (3)

NDI / SSO	**National Digital Identity / Single Sign-On**	Issue and verify the tokens of calling systems; sign in IDCB admin users through OIDC. SSO is the backup when NDI is unavailable. IDCB applies its own conversion policies.	OIDC / REST	Required (2)
JLB	**Journaling Block**	Store tamper-evident, cryptographically signed logs of all identity transformation operations	Event Bus (Async)	Required (2)
EVTB	**Event Bus**	Publish mapping lifecycle events (created, revoked, expired, scope violation) for downstream consumers	Event Bus (Async)	Required (1)
NTFB	**Notification Block**	Consume IDCB pseudonymised identity references to trigger notifications without holding base identifiers	REST API / Event Bus	Required (2)
APIG	**API Gateway**	Secures inbound access - the entry point other systems use to reach IDCB's own REST endpoints; enforces rate limiting and TLS termination	API Gateway	Infrastructure
	My Bhutan Portal	Single government portal for citizens, businesses and service-provider officers (replaces PSP and CBP). For IDCB it: (1) converts the applicant's identifier to the agency's pseudonym when an application is submitted; (2) acts for an agency when officers work in the portal.	REST API (Sync)	Required
GSS	**Government service systems**	Agency systems that deliver services (e.g., passport, vehicle registration, tax). They call IDCB to convert identifiers into their own domain's pseudonyms and to run checks. They also call IDCB when users register with the service (to create the mapping) and at every sign-in (to look up the user's pseudonym).	**REST API (Sync), EVTB (bulk)**	**Consumer**
SP / BO	**Service provider and back-office systems**	Systems where officers process applications, and approved non-government service providers. They call IDCB only under rules that	REST API (Sync)	Consumer

		name them, and receive pseudonyms only.		

Dependency Strength: Required (3) = IDCB cannot convert without it; Required (2) = IDCB runs but a core function stops (e.g., authentication, audit); Required (1) = IDCB runs with reduced function and buffers until it returns; Infrastructure = shared platform service.Consumer = a system that calls IDCB; IDCB does not depend on it.

3. Usage Scenarios

Usage scenarios showing IDCB in operation are in Section 8.

4. IDCB Capabilities and Requirements

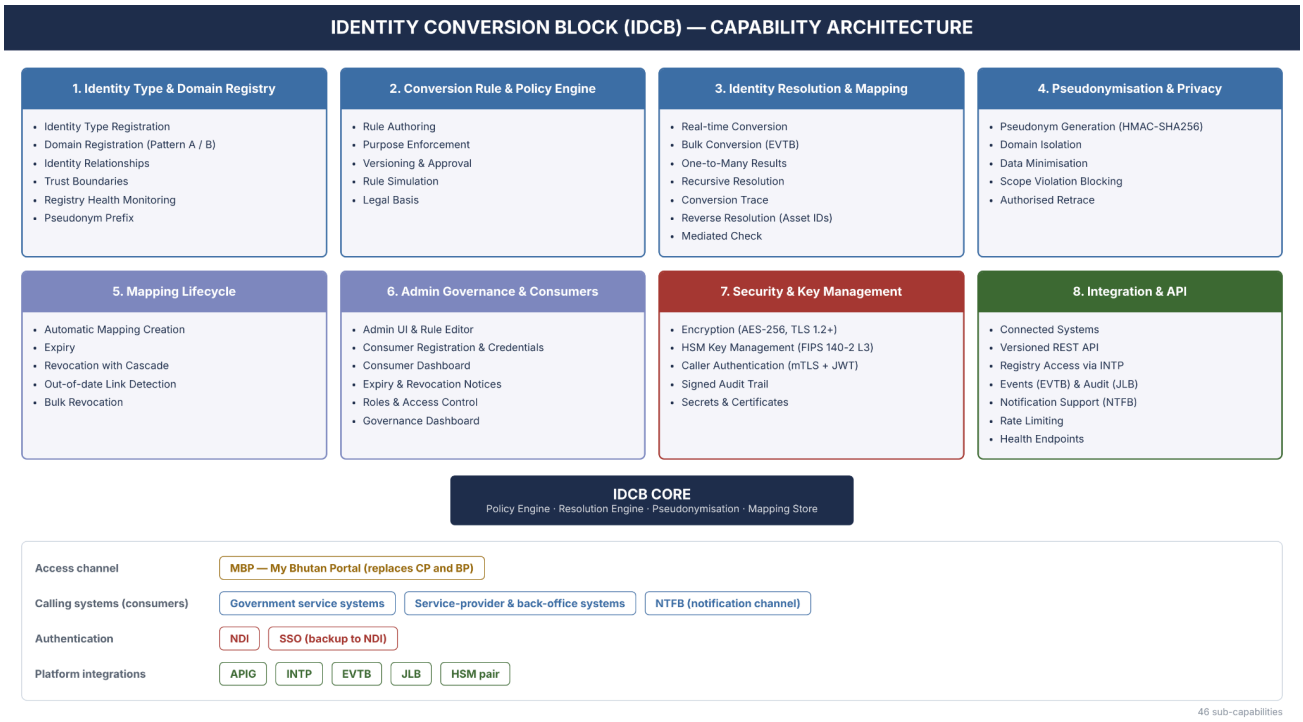


Figure 1: IDCB Capability Architecture - 8 Capability Groups, 46 Sub-Capabilities

4.1 Capability 1: Identity Type and Domain Registry Management

Identity Type and Domain Registry Management is IDCB's setup layer. Authorised Data Stewards use it to register the identity types and domains IDCB works with, the relationships between identity types, which domains may convert to which (trust boundaries), and each domain's pseudonym prefix. Every setup change is approved by a second person before it takes effect. Without this capability, IDCB cannot tell identity types apart, keep domains separate, or check requests against allowed domain pairs.

4.1.1 Sub-Capabilities

1. **Identity type registration:** Register identity types in ID_TYPE:IDENTIFIER format (e.g., CID, VRN, TIN, LPN, BRN, HID and work permit number for foreign workers). Each type belongs to one domain and has a validation pattern and a sensitivity class: base identifier (e.g., CID) or asset identifier (e.g., VRN).
2. **Domain registration:** Register domains (Civil Registry, RSTA, Tax Authority, Health System, Land Cadastre, Business Registry, Customs, Immigration) with their owning agency, integration pattern (Pattern A or B, see Appendix G), and, for Pattern A, the registry connection details.
3. **Identity relationships:** Define the allowed links between identity types (e.g., Company → Director → Land Parcel) that recursive resolution may follow, with a maximum chain depth.
4. **Trust boundaries:** Define which source domain may convert to which target domain, and for which purposes. Anything not allowed is denied.
5. **Registry health monitoring:** For Pattern A domains, check each registry regularly and alert the domain's Data Steward when it is down or out of date.
6. **Pseudonym prefix:** Let each domain set a short prefix (e.g., TRF for RSTA) so its pseudonyms are recognisable.

4.1.2 Process Flow: Identity Type and Domain Registration

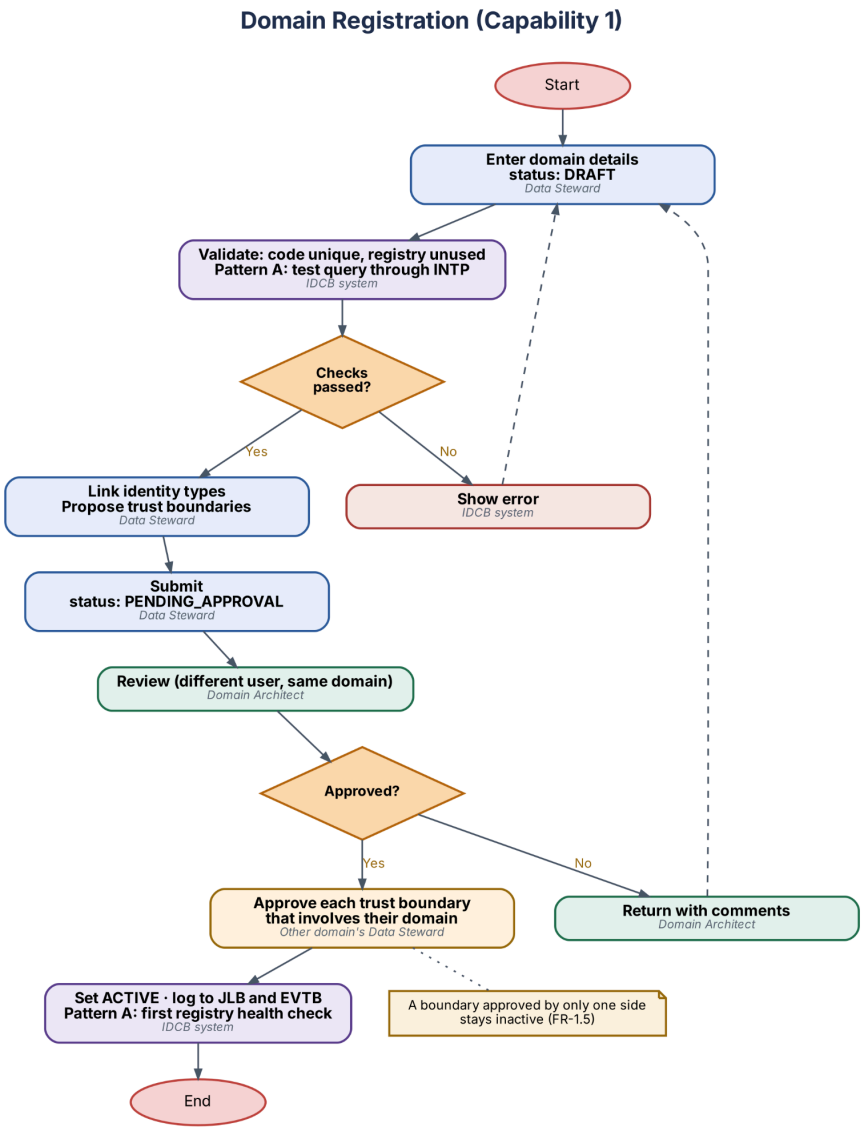


Figure 2: Identity Type and Domain Registration Process Flow

The Data Steward sets up the domain and its rules, the Domain Architect double-checks it, and IDCB confirms the connection actually works before going live.

Step	Actor	Action
1	**Data Steward**	Opens the admin UI and selects “Register New Domain”. Enters domain_code, domain_name, owning agency, integration pattern (A or B) and, for Pattern A, the registry connection details and staleness threshold. Saved as DRAFT.

2	**IDCB**	Checks that domain_code is unique and the registry isn't used by another domain. For Pattern A, sends a test query through INTP. If the test fails, the domain cannot be submitted.
3	**Data Steward**	Links the domain's identity types, proposes its trust boundaries, and submits. Status becomes PENDING_APPROVAL.
4	**Domain Architect**	A different user from the same domain reviews it, then approves it or returns it with comments.
5	**Other domain's Data Steward**	Approves or rejects each proposed trust boundary that involves their domain.
6	**IDCB**	Sets the domain to ACTIVE and records domain.activated in JLB and EVTB. For Pattern A, runs the first registry health check.

4.1.3 Functional Requirements - Identity Type and Domain Registry Management

ID	Requirement	Priority	Acceptance Criteria
FR-1.1	Register identity types with: type_code (unique, e.g., CID, VRN), owning domain (exactly one), validation pattern (regular expression), and sensitivity class (BASE_IDENTIFIER or ASSET_IDENTIFIER). Status is ACTIVE or INACTIVE.	MUST	Duplicate type_code rejected. A type cannot be saved without an owning domain. Identifiers that fail the validation pattern return HTTP 400. INACTIVE types cannot be used in new rules. JLB: identity_type.registered, identity_type.updated.
FR-1.2	Register domains with: domain_code (UPPER_SNAKE_CASE, unique), name, owning agency, integration pattern (A or B), and, for Pattern A only, registry adapter details and staleness threshold. Status: DRAFT, PENDING_APPROVAL, ACTIVE or SUSPENDED. For Pattern A, a connection test through INTP must pass before submission. For Pattern B, the owning agency's confirmation	MUST	A Pattern A domain cannot be submitted if the connection test fails. A Pattern B domain cannot be activated without the recorded confirmation. While a domain is SUSPENDED, conversions involving it return HTTP 403 DOMAIN_SUSPENDED and its mappings are kept but cannot be resolved. JLB: domain.activated, domain.suspended.

	that its system does not store CIDs must be recorded.		
FR-1.3	Define allowed links between identity types for recursive resolution (e.g., BRN → director CID → LPN). Maximum chain depth configurable from 1 to 10 (default 5).	MUST	Circular links rejected when saved. Links allowed only between ACTIVE types. Runtime resolution never exceeds the configured depth.
FR-1.4	For Pattern A domains, check each registry through INTP every 5 minutes. Record its status (UP, DEGRADED, DOWN) and the last check time. Alert the domain's Data Steward through NTFB when the registry is down or beyond its staleness threshold. Show registry status in the admin dashboard, limited to the viewer's own domains.	MUST	Alert received within 5 minutes of a failure. Conversions served from cache while the registry is down carry staleness_flag: true (FR-3.6). No checks or alerts for Pattern B domains.
FR-1.5	Configure trust boundaries per source domain, target domain and purpose (operational context). Deny everything not allowed: return HTTP 403 TRUST_BOUNDARY_VIOLATION and log the attempt. A boundary between two agencies' domains becomes active only when both domains' Data Stewards approve it. Suspending a boundary immediately suspends every rule that depends on it.	MUST	Out-of-boundary requests return 403 and are logged with full request details. A boundary approved by one side only stays inactive. Dependent rules are suspended within 60 seconds of suspending the boundary.
FR-1.6	Every creation or change of an identity type, domain, identity relationship, trust boundary or pseudonym prefix needs approval by a different user who holds the Domain Architect role for that domain; trust boundaries follow FR-1.5. Each change is logged in	MUST	Self-approval blocked and logged. Approver name and time recorded. Change active within 60 seconds of approval.

	JLB with before and after values, published to EVTB, and takes effect within 60 seconds of approval.		
FR-1.7	Let the Data Steward set a pseudonym prefix per domain (3–10 uppercase letters or digits, unique across domains). Pseudonym format: `<PREFIX>_<16 lowercase base32 characters>`. If no prefix is set, IDCB derives one from domain_code. Pseudonyms must be unique within a domain; on a collision, IDCB generates a new value and raises an alert.	MUST	Duplicate or invalid prefix rejected. Default applied when blank. A forced collision test produces two different pseudonyms and one alert. Changing the prefix affects only new pseudonyms; existing ones are never changed.

4.2 Capability 2: Conversion Rule and Policy Engine

The Conversion Rule and Policy Engine decides whether a conversion is allowed. Each rule covers one source domain, one target domain and one purpose. It states who may call it, what it may return, how long the resulting mappings last, and the legal basis that permits it. Every request is checked against an active rule before any lookup happens. Rules are tested, approved by a second person and versioned before they go live.

4.2.1 Sub-Capabilities

1. **Rule authoring:** Define a rule per source domain, target domain and purpose. The rule sets hop behaviour (direct or recursive), result cardinality (one-to-one or one-to-many), permitted callers, response fields, mapping validity period, rule end date, and whether Authorised Retrace is allowed.
2. **Purpose enforcement:** Every request must state its purpose (e.g., traffic_enforcement, emergency_care, tax_assessment). The same identity can be allowed for one purpose and refused for another. Refusals are logged.
3. **Versioning and approval:** Keep every version of every rule. A rule goes live only after approval by a second person, and only one version per domain pair and purpose can be active at a time.

4. **Rule simulation:** Test a rule with made-up identifiers before approval, without touching real registries or real keys.
5. **Legal basis:** Every rule must cite the law, directive or data-sharing agreement (MoU) that permits it.

4.2.2 Process Flow: Conversion Rule Authoring and Activation

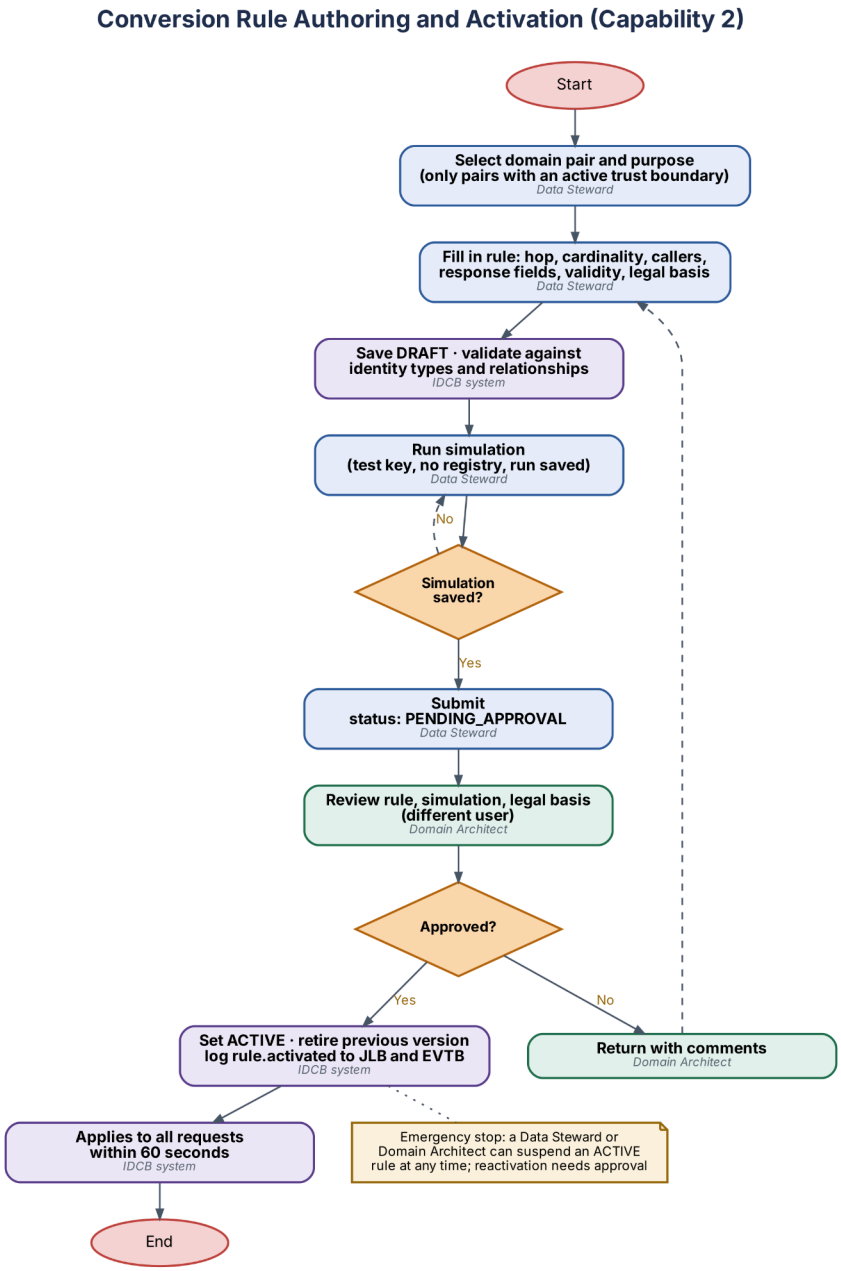


Figure 3: Process Flow: Conversion Rule Authoring and Activation

Step	Actor	Action
1	**Data Steward**	Opens “Conversion Rules” in the admin UI and selects source domain, target domain and purpose. IDCB shows only pairs that have an active trust boundary (FR-1.5).
2	**Data Steward**	Fills in the rule: hop behaviour, result cardinality, permitted callers, response fields, mapping validity period, rule end date, legal basis and retrace eligibility. Saved as DRAFT.
3	**IDCB**	Validates the rule against registered identity types and relationships. A DRAFT rule has no effect on live traffic.
4	**Data Steward**	Runs a simulation with made-up identifiers and checks the output. Then submits the rule. Status becomes PENDING_APPROVAL.
5	**Domain Architect**	A different user from the same domain reviews the rule, the simulation result and the legal basis, then approves it or returns it with comments.
6	**IDCB**	On approval, sets the rule to ACTIVE and archives the previous version. Records rule.activated in JLB and EVTB. The new rule applies to all requests within 60 seconds.

4.2.3 Functional Requirements - Conversion Rule and Policy Engine

ID	Requirements	Priority	Acceptance Criteria
FR-2.1	Each rule covers one source domain, one target domain and one purpose (operational context). Each rule records: hop behaviour (direct or recursive); result cardinality (one-to-one or one-to-many), set separately from hop behaviour; permitted callers (registered consumer systems); response fields allowed	MUST	All fields present and saved with each version. Hop behaviour and cardinality can be combined (e.g., recursive and one-to-many). A rule cannot be saved for a pair without an active trust boundary. A rule stops working automatically after its end date.

	(FR-4.3); mapping validity period (FR-5.1); optional rule end date; whether reverse resolution is allowed (FR-3.7), and Authorised Retrace eligibility (Capability 4).		
FR-2.2	Check every conversion request in this order: (1) caller authenticated (FR-8.1); (2) purpose stated; (3) trust boundary exists (FR-1.5); (4) an active rule exists for the source domain, target domain and purpose; (5) caller is permitted by that rule. Stop at the first failure. No registry lookup happens before all checks pass.	MUST	Missing purpose returns HTTP 400 CONTEXT_REQUIRED. No active rule returns HTTP 403 CONTEXT_NOT_AUTHORISED. Caller not permitted returns HTTP 403 CALLER_NOT_PERMITTED. Every refusal is logged in JLB with caller, domain pair, purpose and time. Tests confirm no registry call happens on any refusal.
FR-2.3	Rule statuses: DRAFT → PENDING_APPROVAL → ACTIVE → SUSPENDED or RETIRED. The approver must be a different user from the author. Only one ACTIVE version is allowed per source domain, target domain and purpose; activating a new version retires the old one. Keep every version and allow rollback, which creates a new DRAFT from an earlier version. A Data Steward or Domain Architect can suspend an ACTIVE rule immediately, with no approval needed (emergency stop). Reactivating it needs approval.	MUST	Self-approval blocked. Two ACTIVE versions for the same pair and purpose are impossible. A suspended rule refuses requests within 60 seconds. Every status change is recorded in JLB with actor and time. Full version history visible in the admin UI.
FR-2.4	Provide rule simulation. The Data Steward enters made-up identifiers and sees the result the rule would produce. Simulation uses no live registry and a separate test key, never production keys. Each simulation run is saved against the rule version. A rule cannot be submitted for approval without at least one saved simulation run.	MUST	No registry call during simulation. Simulation results never appear in the conversion audit log. Saved runs are visible to the approver. Submitting without a run is blocked.

FR-2.5	Every rule must have a legal_basis_ref: a law or regulation section, a Cabinet or ministerial directive, or an inter-agency data-sharing agreement (MoU). An optional link to the document may be added. The approver confirms the legal basis at approval. The legal_basis_ref is copied into every audit log record created under the rule. Provide a report of active rules by legal basis type.	MUST	A rule without a legal_basis_ref cannot be submitted. 100% of conversion audit records carry a legal_basis_ref. The report lists every active rule with its legal basis.
FR-2.1	Each rule covers one source domain, one target domain and one purpose (operational context). Each rule records: hop behaviour (direct or recursive); result cardinality (one-to-one, one-to-many), set separately from hop behaviour; permitted callers (registered consumer systems); response fields allowed; mapping validity period (FR-5.1); optional rule end date; and Authorised Retrace eligibility (Capability 4).	MUST	All fields present and saved with each version. Hop behaviour and cardinality can be combined (e.g., recursive and one-to-many). A rule cannot be saved for a pair without an active trust boundary. A rule stops working automatically after its end date.

4.3 Capability 3: Identity Resolution and Mapping Execution

Identity Resolution and Mapping Execution is the engine that performs conversions. It handles single real-time requests, large batches, requests that return several results, and requests that follow a chain of links across domains. For Pattern A domains it looks up the authoritative registry through INTP. For Pattern B domains it uses IDCB's own mapping store. It always returns pseudonyms, never the underlying identifier.

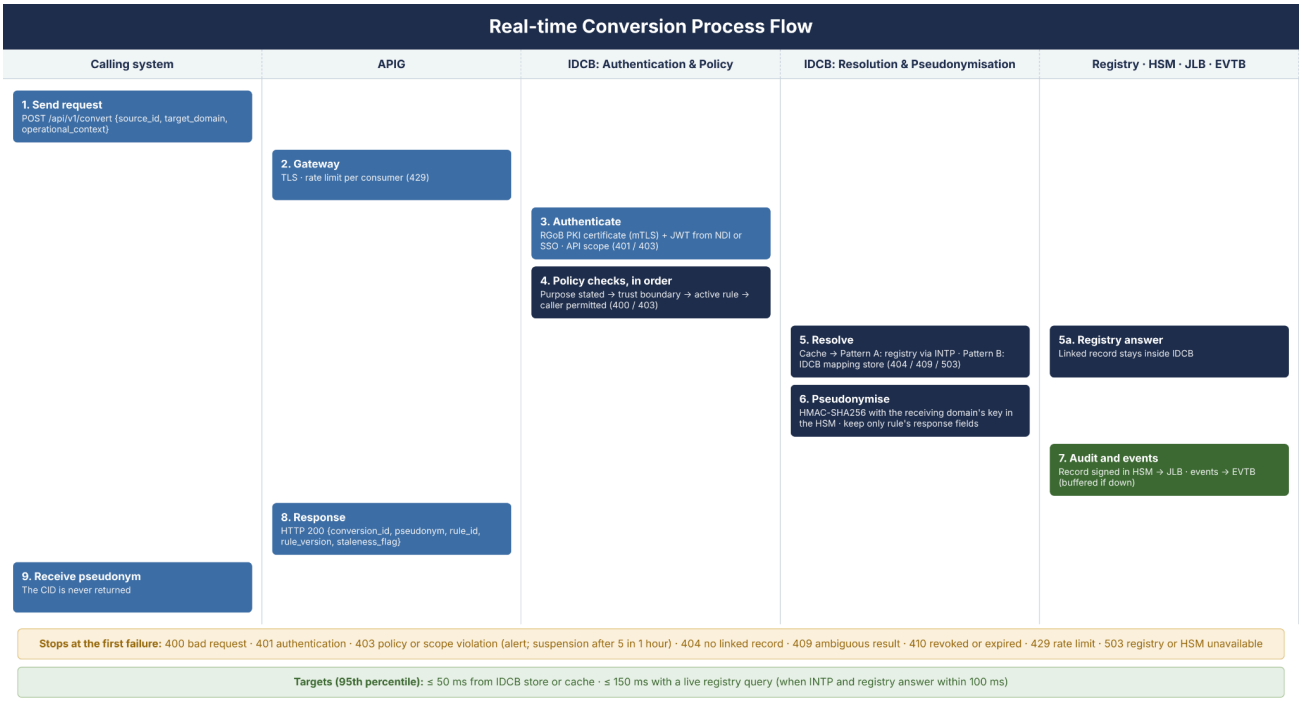


Figure 4: Real-time Conversion Process Flow

4.3.1 Sub-Capabilities

1. **Real-time conversion:** Convert one identifier per request through the REST API, within the times in Section 4.9.1. If a registry is down, return a cached result marked as possibly out of date, or refuse with HTTP 503.
2. **Bulk conversion:** Accept batches of up to 1,000 conversions through EVTB for high-volume work such as bulk notices or annual tax assessments, returning a result for each item.
3. **One-to-many results:** Return several pseudonyms for one identifier (e.g., one CID → all vehicles owned), with paging for large results.
4. **Recursive resolution:** Follow a chain of allowed links (e.g., Business → Director → Land Parcels, as defined in FR-1.3), checking policy at every step and stopping if any step is not allowed.
5. **Conversion trace:** Let Data Stewards and Compliance Auditors see how a past conversion was produced, for audits and investigations.

6. **Reverse resolution for asset identifiers:** Let an authorised caller turn a pseudonym it received back into the asset identifier it stands for (e.g., a land parcel number), when the rule allows it. Never returns a CID or other personal identifier.
7. **Mediated check:** Answer a pre-registered yes/no question about a person using another agency's data, without either agency learning the other's pseudonym. Only the answer is returned.

4.3.2 Functional Requirements - Identity Resolution and Mapping Execution

ID	Requirement	Priority	Acceptance Criteria
FR-3.1	Provide real-time conversion via POST /api/v1/convert with source_id (ID_TYPE:IDENTIFIER), target_domain and operational_context. Apply the checks in FR-2.2 first. Pattern A domains are resolved through INTP; Pattern B domains are resolved from IDCB's mapping store. Every request gets a unique conversion_id, used in the response, trace and audit log. Response fields: conversion_id, pseudonym (or pseudonyms), rule_id, rule_version, staleness_flag.	MUST	Meets 4.9.1 timings (≤ 50ms from store or cache, ≤ 150ms with a registry query, 95th percentile). Malformed source_id returns HTTP 400. No linked record returns HTTP 404 NO_LINKED_RECORD. More than one result under a one-to-one rule returns HTTP 409 AMBIGUOUS_RESULT. Registry down with no cache returns HTTP 503 with retry_after. The source identifier never appears in the response.
FR-3.2	Provide bulk conversion through EVTB. A batch holds up to 1,000 requests and carries a batch_id. Each item gets its own result (success or error code) on a reply topic. Resending the same batch_id does not repeat the conversions or the audit records. Items that cannot be processed go to a dead-letter queue.	MUST	A batch of 1,000 is processed with no lost items. One failed item does not stop the batch. A resent batch_id returns the original results with no new audit records. Throughput meets 4.9.1 (≥ 5,000 per second sustained).
FR-3.3	Support one-to-many results when the rule allows it: return an ordered array of pseudonyms, paged with a cursor above 100 items.	MUST	Every array item is a pseudonym for the caller's domain. Paging returns all items with no duplicates. The source identifier never appears.

FR-3.4	Support recursive resolution along links defined in FR-1.3, up to the configured maximum depth. At every step, check that the link is allowed for the rule and purpose. If any step fails, stop and return HTTP 403 with no partial results. Stop circular chains. Identifiers found at intermediate steps (e.g., a director's CID) are never returned.	MUST	Depth limit enforced. Circular chain stopped and logged. A failed step returns 403 with nothing disclosed. Only final-step pseudonyms are returned. Each step is recorded in the trace.
FR-3.5	Provide GET /api/v1/convert/{conversion_id}/trace, returning how the conversion was produced: rule and version, registries or store used, steps followed, and time. Available only to Data Stewards of the domains involved and to Compliance Auditors.	MUST	Other roles receive HTTP 403. Every trace access is logged in JLB. The trace never shows a CID in plain text.
FR-3.6	Cache conversion results for performance and registry outages. The cache time is configurable per domain (default 12 hours). Cached results carry their creation and expiry times. Results served from cache while the registry is down carry staleness_flag: true. Revoked mappings are removed from the cache immediately (FR-4.5).	MUST	Expired entries are never served. A revoked mapping is never served from cache. staleness_flag is correct in tests with the registry up and down.
FR-3.7	Provide reverse resolution via POST /api/v1/resolve: turn a pseudonym issued to the calling system back into the identifier it stands for, only when (a) the rule has reverse resolution allowed, (b) the caller has the idcb.resolve API scope, and (c) the identifier is an ASSET_IDENTIFIER (FR-1.1). Personal identifiers (BASE_IDENTIFIER, e.g., CID) are never returned; recovering a person's	MUST	A pseudonym issued to another caller returns HTTP 403. A missing rule permission or scope returns HTTP 403. A request that would return a BASE_IDENTIFIER returns HTTP 403. Every request is logged in JLB.

	identity is only possible through Authorised Retrace (FR-4.6).		
FR-3.8	Provide mediated checks via POST /api/v1/check. The caller sends its own pseudonym, the check_code, the target domain and the operational context. IDCB checks the rule and trust boundary, converts the pseudonym internally, asks the target domain's registered check endpoint through INTP, and returns only the answer. Checks are registered by the target domain's Data Steward, with a fixed answer type (yes/no or a short fixed list) and a legal basis.	SHOULD	Caller never receives the target pseudonym or CID; target agency never receives the caller's pseudonym; free-text answers rejected; unregistered check_code returns HTTP 403; every check logged in JLB.

4.4 Capability 4: Pseudonymisation and Privacy Protection

Pseudonymisation and Privacy Protection ensures that a calling system only ever receives pseudonyms, never the real identifier. Each pseudonym is made with the secret key of the domain that receives it, so the same person has a different pseudonym in every domain and agencies cannot match their records without IDCB. The capability also limits responses to what the rule allows, blocks out-of-policy requests, and provides a tightly controlled way to recover a real identity when the law requires it.

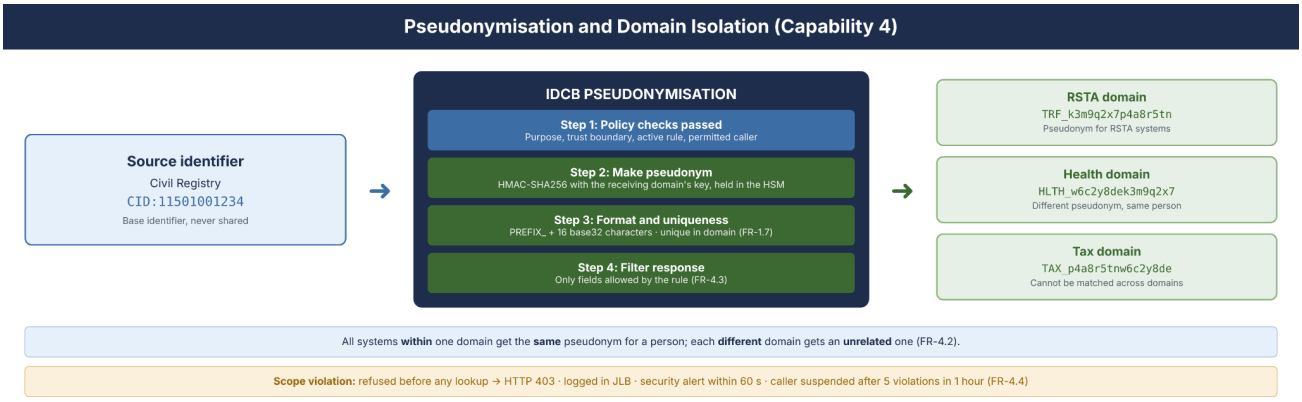


Figure 5: Pseudonymisation and Domain Isolation

4.4.1 Sub-Capabilities

1. **Pseudonym generation:** Return every result as a pseudonym made with HMAC-SHA256 and the receiving domain's secret key held in the HSM. The receiving system cannot reverse it.
2. **Domain isolation:** The same person gets a different pseudonym in each domain. Systems in the same domain get the same pseudonym, so an agency's own systems stay consistent.
3. **Data minimisation:** Return only the response fields the rule allows (FR-2.1). Nothing else is ever added.
4. **Scope violation blocking:** Block and log every out-of-policy request, alert the security team, and suspend a calling system automatically after repeated violations.
5. **Authorised Retrace:** Recover the real identity behind a pseudonym only for a recorded legal case, with approval by a second, senior person. Never available through the API to calling systems.

4.4.2 Functional Requirements — Pseudonymisation and Privacy Protection

ID	Requirement	Priority	Acceptance Criteria
FR-4.1	Return every conversion result as a pseudonym made with HMAC-SHA256, using the secret key of the domain of the receiving system, in the format set by FR-1.7. Base identifiers must never appear in any API response, log or error message returned to calling systems.	MUST	Automated scans of responses, errors and consumer-visible logs find zero CID patterns. Any exposure is treated as a critical security incident. No other pseudonym algorithm is accepted.
FR-4.2	Each domain has its own HMAC key, held in the HSM. The same identifier produces different pseudonyms in different domains, and the same pseudonym for all systems within one domain. No calling system can link pseudonyms across domains without going through IDCB.	MUST	Tests show the same source_id gives different pseudonyms for two domains, and the same pseudonym for two systems in one domain. Separate keys per domain confirmed in the HSM.
FR-4.3	Return only the response fields allowed by the rule (FR-2.1). No extra identity details may be added.	MUST	Every response is checked against the rule's response fields. Any extra field blocks

			the response with HTTP 500 and raises a critical alert.
FR-4.4	Treat as a scope violation: any request refused for having no trust boundary, no active rule, a caller not permitted by the rule, or a missing scope. Malformed requests (HTTP 400) are not violations. For each violation: block before any lookup; log caller, purpose, source identifier type, target domain and time in JLB; publish scope.violation.detected to EVTB; and alert the security team through NTFB within 60 seconds. After 5 violations by the same calling system within 1 hour (configurable), suspend that system automatically and notify its consumer admin. Only the IDCB platform security team can lift a suspension, after review.	MUST	100% of violations blocked before lookup and logged. Alert received within 60 seconds. Suspension at the threshold, after which the system receives HTTP 403 SUSPENDED. The lift action is recorded in JLB with reviewer and reason.
FR-4.5	Once a mapping is revoked (FR-5.3), its pseudonym can never be resolved again, including from cache (FR-3.6) and during registry outages.	MUST	Revoked pseudonyms return HTTP 410 GONE in every test, including with the cache warm and the registry down.
FR-4.6	Provide Authorised Retrace, used only through the admin UI, never through the consumer API. (1) A Data Steward of the domain holding the pseudonym submits a request with a case reference and justification. (2) A Retrace Approver (a senior officer named by the owning agency and provisioned through NDI) approves or rejects it; the requester cannot approve their own request. (3) Approved results are shown to the requester only, for 24 hours. (4) Only rules marked retrace-eligible allow retrace. Every request, approval, rejection and view is logged in JLB under a separate event type. Compliance Auditors receive a monthly retrace report.	MUST	Retrace impossible without an approved request. Self-approval blocked. Rules not marked eligible refuse retrace. The result cannot be viewed after 24 hours. All retrace events separately identifiable in JLB. Monthly report produced.

4.5 Capability 5: Mapping Lifecycle Management

A mapping is IDCB's stored link between a person or asset and the pseudonym issued for it in one domain under one rule. Mapping Lifecycle Management creates mappings automatically on the first successful conversion, expires them when the rule's validity period ends, revokes them when needed, and detects links that have gone out of date. Without it, IDCB would keep serving old or wrong links.

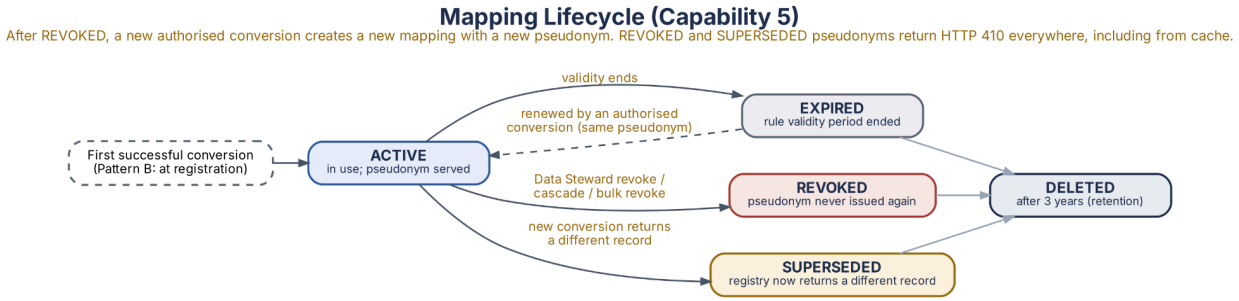


Figure 6: Mapping Lifecycle

4.5.1 Sub-Capabilities

1. **Automatic mapping creation:** The first successful conversion for a person or asset, in a domain, under a rule creates a mapping (for Pattern B, the registration conversion). Later conversions reuse it.
2. **Expiry:** Mappings expire when the rule's validity period ends. Systems that received the pseudonym are notified. A later authorised conversion renews the mapping.
3. **Revocation with cascade:** A Data Steward can revoke a mapping immediately. Mappings derived from it are revoked too. A revoked pseudonym is never issued again.
4. **Out-of-date link detection:** When a new conversion returns a different result than the stored mapping (e.g., a vehicle now has a new owner), the old mapping is marked superseded and the systems that hold it are told.
5. **Bulk revocation:** Revoke many mappings at once (e.g., when a domain is retired or a rule is withdrawn), with approval by a second person.

4.5.2 Functional Requirements - Mapping Lifecycle Management

ID	Requirement	Priority	Acceptance Criteria

FR-5.1	Create a mapping automatically on the first successful conversion of a person or asset, in a domain, under a rule (for Pattern B, at the registration conversion). Store: mapping_id, rule_id and version, a keyed lookup value and an encrypted copy of the source identifier (Section 6.2), the pseudonym, key version, status and expiry. The expiry comes from the rule's mapping validity period (FR-2.1) and cannot be overridden per mapping. Later conversions for the same person or asset, domain and rule reuse the mapping. Record which calling systems have received its pseudonym. Mappings cannot be created manually.	MUST	Only one ACTIVE mapping per person or asset, domain and rule (enforced by the database). Repeat conversions return the same pseudonym. No admin screen or API can create a mapping directly. Creation logged in JLB with rule_id and version.
FR-5.2	Set a mapping to EXPIRED automatically at its expiry time and publish mapping.expired to EVTB within 60 seconds. Notify the systems that received its pseudonym (FR-6.6). Requests that present an expired pseudonym (e.g., reverse resolution) return HTTP 410 PSEUDONYM_EXPIRED. A later authorised conversion renews the mapping with the same pseudonym.	MUST	Expiry applied at the correct time. Event published within 60 seconds. 410 returned for expired pseudonyms. Renewal after expiry returns the original pseudonym.
FR-5.3	Allow a Data Steward of the owning domain to revoke a mapping immediately, via the admin UI or DELETE /api/v1/mappings/{mapping_id}, with a mandatory reason. Calling systems cannot revoke. Cascade: also revoke every mapping that was created through this mapping in a recursive resolution (FR-3.4).	MUST	Revocation takes effect immediately. Cascade complete within 5 seconds. A revoked pseudonym returns HTTP 410 GONE everywhere, including from cache (FR-4.5). A new conversion after revocation returns a different pseudonym. Reason, actor and time logged in JLB.

	Remove revoked mappings from the cache immediately. Publish mapping.revoked to EVTB for each revoked mapping and notify the systems that held them. After revocation, a new authorised conversion for the same person or asset creates a new mapping with a new pseudonym; a revoked pseudonym is never issued again.		
FR-5.4	Detect out-of-date links for Pattern A domains. When a conversion returns a different linked record than an ACTIVE mapping for the same source and rule (e.g., a new vehicle owner), mark the old mapping SUPERSEDED, create the new one, notify the systems that received the old pseudonym, and flag it to the domain's Data Steward. Out-of-date links reported by an agency are handled the same way.	MUST	The old mapping is marked SUPERSEDED in the same transaction as the new conversion. A superseded pseudonym returns HTTP 410 GONE. Notices sent through NTFB. The flag appears in the admin dashboard within 15 minutes.
FR-5.5	Support bulk revocation of up to 10,000 mappings at once, selected by rule, domain or a list of mapping_ids, through the admin UI. Needs approval by a second Data Steward or Domain Architect of the same domain. Cascade, cache removal and events apply as in FR-5.3.	SHOULD	Self-approval blocked. 1,000 mappings revoked in 30 seconds or less. Downloadable result report. One bulk event plus per-mapping events recorded in JLB.

4.6 Capability 6: Administrative Governance and Consumer Management

Administrative Governance and Consumer Management gives people control over IDCB. It provides the admin screens, registers and manages the systems that call IDCB, defines who may do what and sends notices

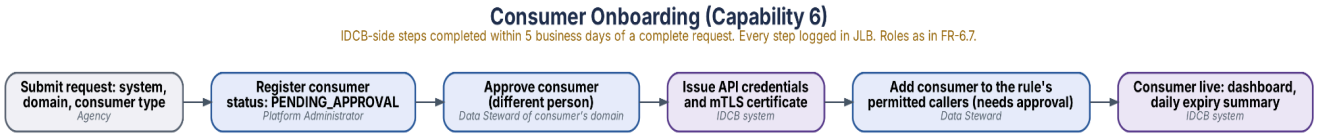


Figure 7: Consumer Onboarding Process Flow

4.6.1 Sub-Capabilities

1. **Admin UI:** Web screens, with NDI sign-in (or SSO when NDI is unavailable), for all setup in Capabilities 1, 2 and 5, including a form-based rule editor with JSON import and export. No engineering work is needed for setup changes.
2. **Consumer registration and credentials:** Register each calling system with its agency, domain, rate limit and credentials; approve it before use; rotate, suspend or revoke its credentials.
3. **Consumer dashboard:** Each calling system's administrators see their own usage, limits and violations, and nothing about other systems.
4. **Expiry and revocation notices:** Daily summaries of mappings about to expire, and notices when mappings are revoked or superseded.
5. **Roles and access control:** Defined roles, each limited to its own domain where applicable, with maker and checker always being different people.
6. **Governance dashboard:** One view of pending approvals, expiring mappings, violations and conversion volume by domain pair.

4.6.2 Functional Requirements - Administrative Governance and Consumer Management

ID	Requirement	Priority	Acceptance Criteria
FR-6.1	Provide a web admin UI with NDI sign-in (or SSO when NDI is unavailable), or SSO when NDI is unavailable (OIDC) for all setup in Capabilities 1, 2 and 5, with no code changes needed. Every UI action is also available through an admin API. Sessions time out after 30 minutes of inactivity.	MUST	All setup possible through the UI. No direct database access needed. Meets WCAG 2.1 AA. Every action logged in JLB.

FR-6.2	Provide a form-based rule editor for all rule fields in FR-2.1, with one-click simulation (FR-2.4). Support JSON export and import of rules; imported rules arrive as DRAFT and go through normal approval.	MUST	Every FR-2.1 field editable in the form. Invalid JSON rejected with the line number shown. An imported rule never becomes ACTIVE without approval.
FR-6.3	Register calling systems (consumers) with: agency, system name (must match the certificate CN), domain (whose key is used for its pseudonyms, FR-4.1), consumer type (PORTAL, GOVERNMENT_SYSTEM or SERVICE_PROVIDER), rate limit, and, for PORTAL only, the agencies it may act for. A Platform Administrator registers the system; a Data Steward of the consumer's domain approves it. On approval, IDCB issues the API credentials and the mTLS certificate. A PORTAL (e.g., My Bhutan Portal) acting for an agency must send the agency and the signed-in user with every request; IDCB applies only that agency's permissions. IDCB-side steps must be completed within 5 business days of receiving a complete request.	MUST	A consumer cannot be used before approval. Self-approval blocked. A portal request without an agency, or naming an agency it may not act for, returns HTTP 403. The agency and acting user are recorded in the audit log. All steps logged in JLB.
FR-6.4	Support rotation, suspension and revocation of each consumer's credentials and certificates through the admin UI.	MUST	Rotation causes no service interruption. Revoked credentials are refused immediately. All events logged in JLB.
FR-6.5	Provide a dashboard for each consumer's administrators: number of active mappings, API calls (last 30 days), rate limit status, and recorded violations with time and purpose.	MUST	A consumer sees only its own data. Rate limit status is shown live. No data from other consumers is visible.
FR-6.6	Send a daily summary through NTFB to each consumer's administrators and to the rule's Data Steward: the number of mappings expiring within 30 days, within 7 days and today, per rule. Send a notice when mappings are revoked or superseded	MUST	The summary is sent daily when there is something to report. Revocation and superseded notices are sent within 5 minutes. No

	(FR-5.3, FR-5.4). Because expiry comes from the rule, the summary links to the rule; extending expiry means updating the rule.		per-mapping expiry setting exists.
FR-6.7	Enforce these roles, provisioned through NDI. **Data Steward** (per domain): setup, rules, revocation, retrace requests. **Domain Architect** (per domain): review and approve changes, run simulations, emergency-suspend rules. **Retrace Approver** (per domain): approve or reject retrace requests (FR-4.6). **Compliance Auditor** (all domains, read-only): audit logs, traces, reports. **Platform Administrator**: register consumers and manage credentials. **Platform Security Officer**: handle security alerts and lift suspensions (FR-4.4). **Consumer Administrator** (per consumer): view their own dashboard and receive notices. One person cannot hold both the Data Steward and Domain Architect roles in the same domain.	MUST	Every action outside a user's role is blocked and logged. Assigning conflicting roles to one person is refused. 100% of admin actions recorded in JLB with role, user, action and time.
FR-6.8	Provide a governance dashboard showing pending approvals, expiring mappings, violations and conversion volume by domain pair and purpose, limited to the viewer's domains. It is a view only, using data already in JLB and IDCB.	SHOULD	Updates at least hourly. Drill-down to the underlying records. Loads in 3 seconds or less.

4.7 Capability 7: Security and Key Management

Security and Key Management protects IDCB's data, keys and connections against outside attackers and insiders. All data is encrypted, all keys live in a certified HSM under dual control, every calling system must prove its identity twice (certificate and token), and every audit record is signed so that tampering can be detected.

4.7.1 Sub-Capabilities

1. **Encryption:** AES-256 for everything IDCB stores, including the cache. TLS 1.2 minimum (1.3 preferred) for all connections. No plaintext identifiers in any store, log or message.

2. **HSM key management:** All keys are held in a certified HSM pair. Signing and encryption keys are rotated regularly. Pseudonym keys are not rotated on a schedule, so pseudonyms stay stable. No single person can generate, export or restore keys.
3. **Caller authentication:** Every calling system presents both an RGoB PKI certificate (mTLS) and a token (JWT) issued by NDI or SSO. Both must be valid.
4. **Signed audit trail:** Every audit record is signed in the HSM before it is sent to JLB, so any change can be detected.
5. **Secrets and certificates:** Passwords, keys and certificates are kept only in an approved secret store, and expiry is alerted well in advance.

4.7.2 Functional Requirements - Security and Key Management

ID	Requirement	Priority	Acceptance Criteria
FR-7.1	Encrypt all data stored by IDCB (mappings, rules, configuration, cache and audit records before sending) with AES-256. Use TLS 1.2 minimum (TLS 1.3 preferred) with HSTS on all endpoints. Validate NDI and other partner certificates against the RGoB trust store. No plaintext identifiers in any database field, log, error or dashboard.	MUST	Database scan finds zero plaintext identifier fields. TLS scan confirms TLS 1.2 or higher on every endpoint. HSTS header present. Log and error scans find zero CID patterns.
FR-7.2	Hold all keys in an HSM pair certified FIPS 140-2 Level 3 or higher (or FIPS 140-3 Level 3), in an RGoB-approved location, with automatic failover. Key types: one pseudonymisation key per domain (FR-4.2); one lookup key; one retrace encryption key (FR-4.6); data encryption keys; one audit signing key; one simulation test key (FR-2.4). Signing and encryption keys are rotated every 90 days (configurable), using envelope encryption so stored data does not need re-encrypting. Pseudonymisation and lookup keys are **not** rotated on a schedule, so issued pseudonyms never change; they are replaced only under FR-7.5. Key generation, backup, restore and export need at least two authorised officers (dual control).	MUST	HSM certificate provided. Failover tested with no conversion failures. Rotation of signing and encryption keys causes no interruption, and old records stay readable and verifiable. Pseudonyms identical before and after a scheduled rotation. No key operation possible by one person alone. All key operations logged in JLB.

FR-7.3	Require mTLS for all system-to-system calls. Each calling system presents an RGoB PKI client certificate whose CN matches its registered system name, plus a valid JWT issued by NDI or SSO (FR-8.1). If either check fails, return HTTP 401. Admin users sign in through NDI, or SSO when NDI is unavailable (FR-6.1).	MUST	Certificate without JWT rejected. JWT without certificate rejected. CN mismatch rejected. Each failure logged (FR-7.6).
FR-7.4	Sign every audit record in the HSM before sending it to JLB. Provide GET /api/v1/audit/{record_id}/verify, for Compliance Auditors only, returning VALID or INVALID.	MUST	100% of records signed. A tampered record returns INVALID. Records signed with a retired key version still verify.
FR-7.5	Handle suspected key compromise. **Signing or encryption key:** revoke it and activate a new key immediately, with no interruption; old signatures stay verifiable. **Pseudonymisation or lookup key:** suspend the affected domain (FR-1.2), then run an approved migration that issues new pseudonyms under a new key, give consuming systems the old-to-new list through a secure channel, and reactivate the domain. Every emergency action needs approval by the Platform Security Officer and a second officer.	MUST	Signing and encryption key replaced with no interruption. Pseudonym key compromise drill completed in a test environment, including domain suspension, migration and consumer handover. All steps logged and approved.
FR-7.6	Log every security event in JLB within 5 seconds: authentication and certificate failures, key operations, scope violations (FR-4.4), suspensions, role changes and admin security actions.	MUST	Events searchable by type and date. Retained per Section 4.9.4.
FR-7.7	Keep all secrets (API credentials, private keys, certificates, passwords) only in an approved secret store; never in source code, configuration files or logs.	MUST	Repository and log scans find zero secrets. Every secret access is logged.
FR-7.8	Alert the Platform Security Officer 30 days and 7 days before any certificate or key expires. Report weak cipher suites or outdated TLS versions.	MUST	Alerts received at both points in a test. Weak cipher test detected and reported.

4.8 Capability 8: Integration and API Management

Integration and API Management defines how IDCB connects to other systems: The systems that call it (My Bhutan Portal, government service systems, and service-provider and back-office systems), how their NDI or SSO tokens are checked, how tokens are checked, how registries are reached (INTP), how events and audit records are sent (EVTB and JLB), how notifications reach people without exposing their identity (NTFB), and how IDCB reports its own health.

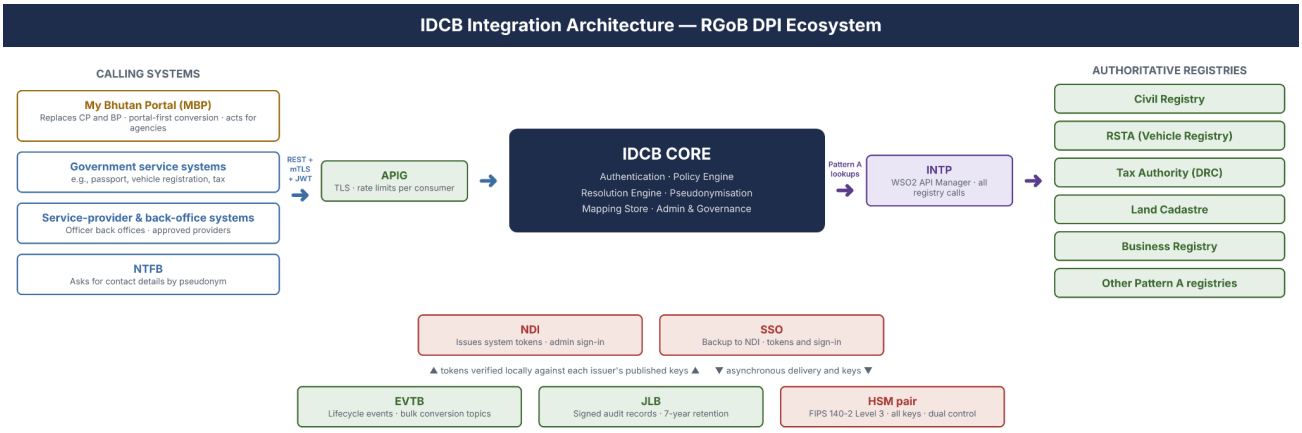


Figure 8: IDCB Integration Architecture - RGoB DPI Ecosystem

4.8.1 Sub-Capabilities

1. **Connected systems:** Serve three kinds of calling system: My Bhutan Portal (replacing CP and BP), government service systems, and service-provider and back-office systems. Each is registered with its own type, domain and limits (FR-6.3).
2. **REST API:** A versioned REST API, documented in OpenAPI, for every endpoint in Appendix C. Every call is checked with an NDI or SSO token and a certificate.
3. **Registry access through INTP:** All registry lookups go through INTP. No direct connections.
4. **Events and audit delivery:** Publish lifecycle events to EVTB and send every signed audit record to JLB, buffering safely if either is down.
5. **Notification support:** Let NTFB reach a person using only a pseudonym; IDCB finds the contact details and never reveals the identifier.
6. **Rate limiting:** Per-system limits, enforced at the API gateway.
7. **Health endpoints:** Liveness, readiness and dependency status for infrastructure monitoring.

4.8.2 Functional Requirements - Integration and API Management

ID	Requirement	Priority	Acceptance Criteria
FR-8.1	Check the JWT on every API call, together with the certificate (FR-7.3). Accept tokens issued by NDI, or by SSO when NDI is unavailable; both are configured as trusted issuers. Required claims: iss (NDI or SSO), sub (system ID), scope (IDCB APIs allowed, e.g., idcb.convert, idcb.resolve, idcb.bulk), iat, exp. Verify signatures locally using each issuer's published keys (JWKS), refreshed at least every 15 minutes and immediately when an unknown key appears. Check revocation using the issuer's revocation information, cached for at most 60 seconds. Which purposes a system may use is decided by IDCB rules (FR-2.1), not by the token.	MUST	Expired, revoked or wrongly signed tokens return HTTP 401. A token without the needed API scope returns HTTP 403. Key refresh and revocation cache timings verified in tests. All failures logged (FR-7.6). Tokens from any issuer other than NDI or SSO are refused. When NDI is down, SSO-issued tokens are accepted with no interruption.
FR-8.2	Provide a versioned REST API (v1 in the URL path) for all endpoints in Appendix C, with a published OpenAPI specification. Announce retirement of an API version at least 6 months in advance, and keep the old version working for at least 12 months after a new version is released.	MUST	Every Appendix C endpoint works as documented. The OpenAPI spec matches the live API. Deprecation headers appear 6 months before retirement.
FR-8.3	Send all registry lookups through INTP only; no direct registry connections. When INTP is down, use the cache (FR-3.6) or refuse with HTTP 503.	MUST	Network rules block direct registry access. Test with INTP down: cached answer with staleness_flag: true, or 503 with retry_after.
FR-8.4	Publish these events to EVTB, using the protocol EVTB provides: mapping.created, mapping.expired, mapping.revoked, mapping.superseded, scope.violation.detected, consumer.suspended, config.changed (identity types, domains, trust boundaries, rules, prefixes) and conversion.summary (counts per domain pair and purpose, every 5 minutes; no per-request data). Each event carries: event	MUST	All 8 event types published and acknowledged by EVTB. No CID patterns in any event. EVTB down: events buffered (FR-8.8) and delivered on recovery with none lost.

	type, mapping_id or object ID, domain pair, purpose, time and actor. No identifiers in events. Delivery is at least once.		
FR-8.5	Support notifications by pseudonym via POST /api/v1/notify/channel. NTFB sends the pseudonym, the domain that issued it, and the purpose. IDCB checks that a rule allows notification for that purpose, gets the person's contact details from the registry that holds them (e.g., Civil Registry) through INTP, and returns only the contact details NTFB needs to deliver the message. The identifier is never returned.	MUST	NTFB receives contact details only, never the CID. No matching rule returns HTTP 403. Revoked or expired pseudonym returns HTTP 410. Every request logged in JLB. End-to-end test with Scenario 1.
FR-8.6	Enforce each consumer's rate limit (FR-6.3) at the API gateway. Return HTTP 429 with a Retry-After header when the limit is exceeded.	MUST	Limit enforced at the configured rate. 429 with correct Retry-After. Rate limit events shown in the consumer dashboard (FR-6.5).
FR-8.7	Provide GET /api/v1/health (liveness), GET /api/v1/health/ready (readiness: database, HSM, cache, JLB connection) and GET /api/v1/health/dependencies status of NDI, SSO, INTP, EVTB, JLB, HSM and each Pattern A registry). The dependencies endpoint is available only to platform monitoring.	MUST	Liveness answers within 100ms. Readiness reports not-ready when a required dependency fails. The dependencies endpoint refuses other callers.
FR-8.8	Send every signed audit record (FR-7.4) to JLB. If JLB or EVTB is down, store records and events in a durable local buffer (on disk, encrypted) that holds at least 24 hours of peak traffic. Retry every 30 seconds and deliver everything on recovery, in order. Alert the operations team when the buffer is 50% full.	MUST	Zero audit records or events lost in a 1-hour JLB and EVTB outage test. Buffer survives a service restart. Alert raised at 50% full.
FR-8.9	Support the three consumer types in FR-6.3. PORTAL (My Bhutan Portal): converts the applicant's identifier into the agency's pseudonym before an application is sent (portal-first conversion, Appendix G), and	MUST	Each type limited as stated. A SERVICE_PROVIDER call to bulk or reverse resolution returns HTTP 403. A portal request without

	acts for an agency only when it sends the agency and the signed-in user. GOVERNMENT_SYSTEM (government service and back-office systems): calls IDCB under the rules that name it and receives its own domain's pseudonyms. SERVICE_PROVIDER (approved non-government providers): allowed only under a rule with a legal basis that names the provider; never allowed bulk conversion or reverse resolution.		agency and user returns HTTP 403. Consumer type recorded in every audit record.
FR-8.10	Each government service registers and signs in its own users. At registration, the service system calls POST /api/v1/convert with its own domain as target and operational_context user_registration; IDCB creates the mapping and returns that service's pseudonym. At every sign-in through NDI or SSO, the service calls it with user_sign_in; IDCB only looks up the existing pseudonym and never creates a mapping.	MUST	Registration creates one mapping per user. Sign-in returns the same pseudonym every time, within 50ms. Sign-in for an unregistered user returns HTTP 404 NOT_REGISTERED.

4.9 Non-Functional Requirements

4.9.1 Performance Requirements

Requirement	Target	Measurement
Real-time conversion from IDCB store or cache (95%)	≤ 50ms	From request received to response sent
Real-time conversion with a live registry query (95%)	≤ 150ms	Same, including the INTP round trip. Applies when INTP and the registry together answer within 100ms; IDCB's own processing must stay within 50ms in all cases.
Reverse resolution (95%)	≤ 50ms	From request to asset identifier returned
Real-time throughput	≥ 1,000 requests per second, sustained peak	Load test for 30 minutes with all real-time targets met

Bulk throughput	≥ 5,000 items per second, sustained	Load test for 10 minutes, with registries replaced by a simulator
Data volume	≥ 20 million active mappings	All targets above met at this volume
Admin UI page load	≤ 2 seconds	First load of the admin dashboard in a standard browser
Consumer dashboard load	≤ 1 second	Including mapping count and usage chart

4.9.2 Availability and Scalability Requirements

1. Service uptime: ≥ 99.9% per month (about 44 minutes of downtime), excluding outages of NDI, SSO, NDE and agency registries. Planned maintenance: at most 4 hours per month, in an agreed low-traffic window, announced 72 hours in advance.
2. Horizontal scaling on the RGoB G-Cloud container platform. Stateless application design: no session state held on any server.
3. Degraded mode: when a registry is down, IDCB keeps serving cached results for registered domain pairs, marked with staleness_flag: true (FR-3.6).
4. Deployment across at least two separate zones or data centres within RGoB G-Cloud.
5. Recovery time (RTO): ≤ 30 minutes after the loss of one zone.
6. Recovery point (RPO): ≤ 5 minutes for mappings and configuration. No loss of audit records (FR-8.8).
7. Backups: daily encrypted backups, kept within RGoB G-Cloud; a restore is tested every quarter.

4.9.3 Security Requirements

1. All security functions as specified in Capability 7 (FR-7.1 to FR-7.8).
2. JWT lifetime at most 1 hour; no long-lived API tokens.
3. Roles as defined in FR-6.7; least privilege applied to all users and calling systems.
4. Application security meets OWASP ASVS Level 2.
5. Independent penetration test before go-live, with no critical or high findings open at go-live. After that, an annual independent penetration test; critical findings fixed within 30 days and high findings within 90 days.

4.9.4 Privacy and Compliance Requirements

1. Privacy by design: base identifiers never appear in API responses, error messages, logs available to calling systems, events or dashboards.
2. Data minimisation: responses contain only the fields the rule allows (FR-4.3).

3. Purpose limitation: every conversion states a purpose, and runs only if an active rule allows it (FR-2.2).
4. Legal basis: every active rule has a legal_basis_ref (FR-2.5).
5. Legal alignment: Bhutanese law, including the Information, Communications and Media Act and the National Digital Identity Act 2023, following recognised principles of data minimisation and privacy by design (as in GDPR Articles 5 and 25).
6. Data location: all IDCB data, keys and backups are kept within RGoB G-Cloud in Bhutan.
7. Retention:
    a. Audit records: kept 7 years in JLB.
    b. IDCB's own copy of the audit log (for traces and dashboards): kept 1 year.
    c. Active mappings: kept while active.
    d. Expired, revoked and superseded mappings: kept 3 years, then deleted, including their encrypted identifiers.
    e. All deletions are automatic and logged in JLB.

4.9.5 Environments, Standards and Operations

1. Environments: development, test, staging and production. Non-production environments use synthetic data only; real identifiers and production keys are never used outside production.
2. Standards: OpenAPI 3 for all APIs; JSON in UTF-8; times in ISO 8601, UTC.
3. Monitoring: logs, metrics and alerts sent to RGoB's central monitoring, with no identifiers in them.
4. Documentation: OpenAPI specification, integration guide for calling systems, admin user guide, and operations runbooks (including the key compromise procedure, FR-7.5).
5. Language: the admin UI is in English.

5. Solution and Integration Architecture

5.1 Logical Component Architecture

IDCB is built as modular services in six layers, each mapping to capabilities in Section 4. Vendors may choose how to package the services, provided all requirements are met.

Layer	Components	Responsibilities
Layer 1: API and Security	API Gateway Adapter, Token Validator (NDI and SSO), mTLS Enforcer	Check certificate and token on every call, check API scopes, apply consumer type limits. Rate limiting is done at APIG

Layer 2: Policy Engine	Trust Boundary Checker, Rule Evaluator, Legal Basis Checker	Check requests in the order: purpose, trust boundary, active rule, permitted caller.
Layer 3: Resolution Engine	Resolver, One-to-Many Expander, Recursive Resolver, Cache Manager, INTP Adapter	Look up registries through INTP (Pattern A) or the mapping store (Pattern B); paging, recursive chains, cache.
Layer 4: Pseudonymisation	HMAC-SHA256 Generator, Domain Key Client (HSM), Response Field Filter, Scope Violation Detector	Make pseudonyms with domain keys, enforce response fields, detect and block violations.
Layer 5: Persistence and Delivery	Mapping Store, Configuration Store, Audit Writer, Durable Buffer, EVTB Publisher	Store mappings and configuration, sign and send audit records to JLB, publish events to EVTB, buffer during outages
Layer 6: Admin and Governance	Admin UI, Rule Editor, Simulation Sandbox, Approval Workflow, Retrace Workflow, Consumer Registry, Dashboards	Setup screens, maker-checker approvals, Authorised Retrace, consumer management, consumer and governance dashboards.

Technology Stack (Example only; vendors may propose equivalents)

Component	Technology
Application runtime	Java (Spring Boot) or Node.js, in containers
Mapping and configuration store	PostgreSQL, encrypted at rest
Cache	Redis, encrypted, with a configurable time per domain; entries removed immediately on revocation
Pseudonymisation	HMAC-SHA256, one key per domain, held in the HSM
Key management	HSM pair, FIPS 140-2 Level 3 or higher, automatic failover; HSM-protected backup under dual control
Events	EVTB, using the protocol EVTB provides
Identity and authentication	NDI and SSO (OIDC) for admin users; NDI- or SSO-issued JWT plus RGoB PKI certificate for systems
Registry access	INTP (WSO2 API Manager)
Container platform	RGoB G-Cloud container platform (e.g., Kubernetes), with automatic scaling
Admin UI	Web application meeting WCAG 2.1 AA

5.2 Integration Architecture

5.2.1 Key Integration Specifications

NDI and SSO: IDCB checks the JWT on every API call, together with the client certificate. Tokens issued by NDI, or by SSO when NDI is unavailable, are accepted. IDCB verifies each token locally against its issuer's published keys (refreshed at least every 15 minutes, and immediately when an unknown key appears), checks expiry, issue time and API scopes, and checks revocation using the issuer's revocation information, cached for at most 60 seconds (FR-8.1). Admin users sign in through NDI, or through SSO during an NDI outage.

Authorisation and service access: Deciding whether a user may use a government service remains the responsibility of that service. IDCB accepts requests only from registered, authenticated systems, and decides whether each conversion is allowed using its own rules, trust boundaries and consumer limits.

My Bhutan Portal: My Bhutan Portal (replacing CP and BP) calls IDCB for portal-first conversion when a citizen or business submits an application, and on behalf of an agency when officers work in the portal. It must send the agency and the signed-in user with each such request (FR-6.3, FR-8.9).

Government service systems and service-provider and back-office systems: These systems call IDCB under the rules that name them and receive only their own domain's pseudonyms (FR-8.9).

INTP: All registry lookups for Pattern A domains go through INTP. IDCB has no direct registry connections. INTP applies its own rate limits, logging and circuit breakers. When INTP is down, IDCB serves cached results marked as possibly out of date, or refuses with HTTP 503 (FR-8.3).

EVTB: IDCB publishes the eight event types in FR-8.4 to EVTB, using the protocol EVTB provides, with at-least-once delivery. If EVTB is down, events are held in the durable buffer (FR-8.8). No events may be lost.

JLB: Every audit record is signed in the HSM and sent to JLB, which keeps it in its append-only store. IDCB never changes or deletes JLB records. If JLB is down, records are held in the durable buffer and delivered in order on recovery (FR-8.8).

NTFB: NTFB sends IDCB a pseudonym and purpose. IDCB checks the rule, gets the person's contact details from the registry that holds them through INTP, and returns only those contact details. NTFB never receives the identifier (FR-8.5).

5.2.2 Failure Handling

Dependency	Failure Behaviour	Recovery

NDI / SSO	If NDI is down, SSO-issued tokens are accepted. If both are down, or revocation information is older than 60 seconds, all requests are refused with HTTP 401 AUTH_UNAVAILABLE and logged.	Automatic retry; alert to the operations team
INTP / Registry	Cached result returned with staleness_flag: true. If nothing is cached: HTTP 503 with retry_after.	Cache serves requests; reconnect on recovery
EVTB	Durable local buffer (FR-8.8); delivered on recovery; zero loss	Retry every 30 seconds; alert at 50% buffer
JLB	Durable local buffer (FR-8.8); delivered in order on recovery; zero loss	Retry every 30 seconds; alert at 50% buffer
HSM	Automatic failover to the second HSM. If both are down, no pseudonyms can be made: HTTP 503 HSM_UNAVAILABLE and all conversions refused.	HSM pair with automatic failover; alert
Cache	Requests served from the mapping store (slower, but still correct).	Cache rebuilt automatically on recovery
Mapping store (database)	Automatic failover to the standby in the second zone. If both are down: HTTP 503 and all conversions refused.	Restore within the RTO and RPO in 4.9.2

6. Data, Security and Compliance

6.1 Data Model (Indicative)

The IDCB data model has seven main tables: identity_domains, identity_types, trust_boundaries, conversion_rules, identity_mappings, conversion_audit_log and registered_consumers. All are held in a relational database (e.g., PostgreSQL), encrypted at rest. Field names are indicative; vendors may adjust them provided every requirement is met.

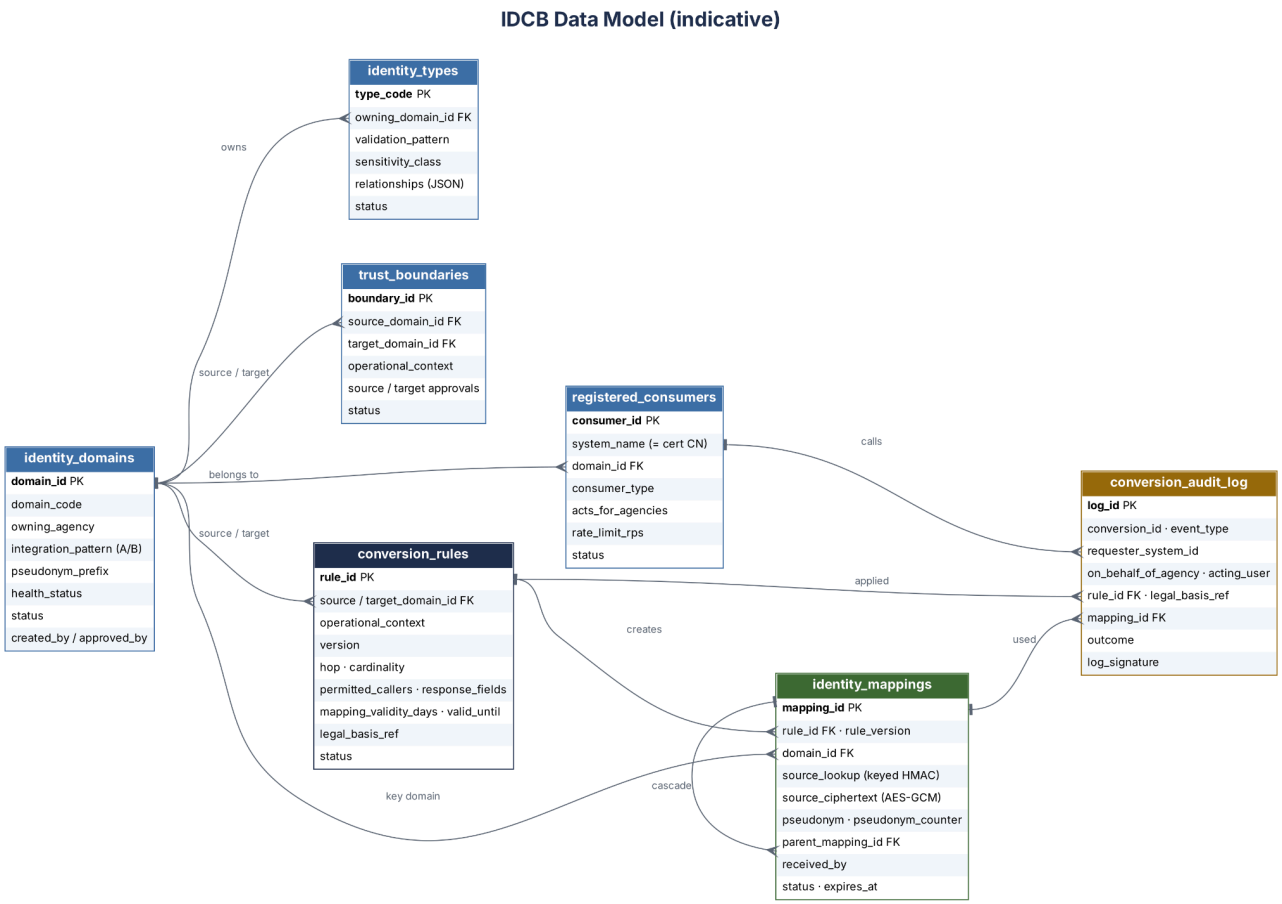


Figure 9: IDCB Data Model - Entity Relationship Diagram

6.1.1 Table: identity_domains

Field	Type	Description
domain_id	UUID PK	Unique domain identifier
domain_code	VARCHAR(50) UNIQUE	UPPER_SNAKE_CASE code (e.g., CIVIL_REG, VEH_REG, TAX)
domain_name	VARCHAR(200)	Full name

owning_agency	VARCHAR(100)	Agency that owns the domain
integration_pattern	ENUM	PATTERN_A | PATTERN_B (Appendix G)
pattern_b_confirmation	JSONB NULL	Pattern B only: owning agency's confirmation that its system stores no CIDs (officer, date)
adapter_config	JSONB NULL	Pattern A only: INTP path, timeout, query format
staleness_threshold_minutes	INTEGER NULL	Pattern A only: alert threshold (FR-1.4)
health_status	ENUM NULL	Pattern A only: UP | DEGRADED | DOWN
last_checked_at	TIMESTAMPTZ NULL	Pattern A only: last registry health check
pseudonym_prefix	VARCHAR(10) UNIQUE	Pseudonym prefix (FR-1.7)
status	ENUM	DRAFT | PENDING_APPROVAL | ACTIVE | SUSPENDED
created_by / approved_by	UUID	Author and approver; must differ (FR-1.6)
created_at / approved_at	TIMESTAMPTZ	Creation and approval times

6.1.2 Table: identity_types

Field	Type	Description
type_code	VARCHAR(10) PK	e.g., CID, VRN, TIN, LPN, BRN
owning_domain_id	UUID FK	Domain that owns the type
validation_pattern	VARCHAR(500)	Regular expression for valid identifiers
sensitivity_class	ENUM	BASE_IDENTIFIER | ASSET_IDENTIFIER
relationships	JSONB	Allowed links to other types for recursive resolution, and maximum depth (FR-1.3)
status	ENUM	ACTIVE | INACTIVE
created_by / approved_by	UUID	Author and approver; must differ

6.1.3 Table: trust_boundaries

Field	Type	Description
boundary_id	UUID PK	Unique boundary identifier
source_domain_id	UUID FK	Source domain
target_domain_id	UUID FK	Target domain
operational_context	VARCHAR(100)	Permitted purpose
source_approved_by / target_approved_by	UUID NULL	Approvals from both domains' Data Stewards (FR-1.5)
status	ENUM	PENDING | ACTIVE | SUSPENDED

6.1.4 Table: conversion_rules

Field	Type	Description
rule_id	UUID PK	Unique rule identifier
source_domain_id / target_domain_id	UUID FK	Domain pair
operational_context	VARCHAR(100)	Purpose this rule covers
version	INTEGER	Version number; only one ACTIVE version per domain pair and purpose
hop_behaviour	ENUM	DIRECT | RECURSIVE
result_cardinality	ENUM	ONE_TO_ONE | ONE_TO_MANY
permitted_callers	JSONB	Registered consumer systems allowed to use the rule
response_fields	JSONB	Fields the response may contain (FR-4.3)
mapping_validity_days	INTEGER NULL	Mapping lifetime; NULL means no expiry
valid_until	DATE NULL	Optional rule end date
reverse_resolution_allowed	BOOLEAN	FR-3.7
retrace_eligible	BOOLEAN	FR-4.6
legal_basis_ref	VARCHAR(500)	Law, directive or MoU reference (FR-2.5)

legal_basis_link	VARCHAR(500) NULL	Optional link to the document
status	ENUM	DRAFT │ PENDING_APPROVAL │ ACTIVE │ SUSPENDED │ RETIRED
created_by / approved_by	UUID	Author and approver; must differ
created_at / approved_at	TIMESTAMPTZ	Creation and approval times

6.1.5 Table: identity_mappings

Field	Type	Description
mapping_id	UUID PK	Unique mapping identifier
rule_id / rule_version	UUID FK / INTEGER	Rule and version that created the mapping
domain_id	UUID FK	Domain whose key made the pseudonym
source_lookup	VARCHAR(64)	Keyed HMAC-SHA256 lookup value of the source identifier; never an unkeyed hash
source_ciphertext	BYTEA	Source identifier encrypted (AES-256-GCM) under the retrace key; used only by Authorised Retrace
pseudonym	VARCHAR(40)	Issued pseudonym; unique per domain
pseudonym_counter	INTEGER DEFAULT 0	Increased on a collision (FR-1.7) or after revocation (FR-5.3), so a new pseudonym is issued
key_version	VARCHAR(50)	HSM key version used

parent_mapping_id	UUID NULL	Mapping this one was created through in a recursive resolution (cascade, FR-5.3)
received_by	JSONB	Calling systems that received this pseudonym (notices, FR-6.6)
status	ENUM	ACTIVE | EXPIRED | REVOKED | SUPERSEDED
expires_at	TIMESTAMPTZ NULL	From the rule's mapping validity period
revoked_at / revoked_by / revocation_reason	TIMESTAMPTZ / UUID / TEXT, all NULL	Revocation details
created_at	TIMESTAMPTZ	Creation time

Constraints: unique (domain_id, pseudonym); at most one ACTIVE mapping per (source_lookup, domain_id, rule_id).

6.1.6 Table: conversion_audit_log

Field	Type	Description
log_id	UUID PK	Unique record identifier
conversion_id	UUID NULL	Conversion this record belongs to (FR-3.1)
event_type	ENUM	CONVERSION | BULK_ITEM | REVERSE_RESOLUTION | NOTIFY_CHANNEL | RETRACE | ADMIN | SECURITY
requester_system_id	VARCHAR(200)	Consumer system, from the certificate CN
consumer_type	ENUM	PORTAL | GOVERNMENT_SYSTEM | SERVICE_PROVIDER
token_issuer	ENUM	NDI | SSO
on_behalf_of_agency	VARCHAR(50) NULL	Agency a portal acted for (FR-6.3)
acting_user	UUID NULL	NDI identity of the signed-in officer or user, where known

source_id_type	VARCHAR(10)	Identity type only (e.g., VRN); the identifier itself is never logged
target_domain	VARCHAR(50)	Target domain code
operational_context	VARCHAR(100)	Declared purpose
rule_id / rule_version	UUID / INTEGER, NULL	Rule applied; NULL for refusals before rule match
legal_basis_ref	VARCHAR(500) NULL	Copied from the rule (FR-2.5)
mapping_id	UUID NULL	Mapping used or created
outcome	ENUM	SUCCESS | DENIED_AUTH | DENIED_BOUNDARY | DENIED_RULE | DENIED_CALLER | DENIED_SCOPE | SUSPENDED | NOT_FOUND | GONE | ERROR
response_time_ms	INTEGER	Processing time
log_timestamp	TIMESTAMPTZ	Record time
log_signature	VARCHAR(256)	HSM signature (FR-7.4)
jlb_event_id	UUID NULL	JLB reference once delivered

This table is IDCB's 1-year working copy (Section 4.9.4); JLB holds the 7-year record. Insert only: no update or delete.

6.1.7 Table: registered_consumers

Field	Type	Description
consumer_id	UUID PK	Unique consumer identifier
agency_code	VARCHAR(50)	Owning agency
system_name	VARCHAR(200)	Must match the certificate CN
domain_id	UUID FK	Domain whose key is used for its pseudonyms (FR-4.1)
consumer_type	ENUM	PORTAL | GOVERNMENT_SYSTEM | SERVICE_PROVIDER
acts_for_agencies	JSONB NULL	PORTAL only: agencies it may act for
api_credential_hash	VARCHAR(64)	Hash of the issued credential; the credential itself is not stored
rate_limit_rps	INTEGER	Requests per second limit
status	ENUM	PENDING_APPROVAL | ACTIVE | SUSPENDED | DEREGISTERED
registered_by / approved_by	UUID	Platform Administrator and approving Data Steward; must differ

registered_at / last_active_at	TIMESTAMPTZ	Registration time and last successful call

6.2 Data Security

Security Dimension	Specification
Encryption in Transit	TLS 1.2 minimum, TLS 1.3 preferred, on all API and admin connections; HSTS on all endpoints; partner certificates validated against the RGoB trust store (FR-7.1)
Encryption at Rest	AES-256 for everything IDCB stores, including the cache and the durable buffer; keys managed by the HSM (FR-7.1)
Base Identifier Protection	Base identifiers are never stored in plaintext. Each one is held as (a) a keyed HMAC-SHA256 lookup value and (b) an AES-256-GCM ciphertext under a separate HSM-held retrace key, usable only through Authorised Retrace (FR-4.6). No plaintext CID, VRN, TIN or other base identifier appears in any database field, log, event or API response.
Key Management	FIPS 140-2 Level 3 (or higher) HSM pair under dual control. Signing and encryption keys rotated every 90 days; pseudonymisation and lookup keys are not rotated on a schedule and are replaced only after a compromise (FR-7.2, FR-7.5).
Audit Log Integrity	Every audit record signed in the HSM before sending to JLB; IDCB's own audit table is insert-only (FR-7.4)
API Authentication	NDI- or SSO-issued JWT plus RGoB PKI client certificate on every system call; NDI or SSO OIDC for admin users (FR-7.3, FR-8.1)
Admin Access Control	Roles as defined in FR-6.7; all actions logged; session timeout 30 minutes
Data Minimisation	Responses contain only the fields the rule allows (FR-4.3)

6.3 Privacy and Compliance

Framework / Principle	IDCB Implementation
Legal basis	Every active rule cites a law, directive or MoU, copied into every audit record
Purpose limitation	Every request states a purpose; it runs only if an active rule allows that purpose
Data minimisation	Only rule-approved fields are returned; identifiers never leave IDCB

Privacy by design	Pseudonymisation and domain isolation are built in, not optional
Accuracy	Out-of-date links are detected and superseded; agencies can report wrong links
Storage limitation	Mappings expire under rule policy; expired, revoked and superseded mappings are deleted after 3 years
Integrity and confidentiality	Encryption, HSM keys, dual control, signed audit records
Accountability	Every conversion, refusal, admin action and retrace is logged in JLB for 7 years

7. Appendices

Appendix A: Glossary

Term	Definition
Identity Conversion	Turning an identifier from one domain into a pseudonym for another domain, under an approved rule and trust boundary
Base Identifier	An identifier that directly identifies a person, such as the CID. IDCB never returns it to calling systems.
Asset Identifier	An identifier for a thing, such as a vehicle number (VRN) or land parcel number (LPN)
CID	Citizen Identity Number: Bhutan's primary national personal identifier
Pseudonym	A stand-in identifier made with HMAC-SHA256 and the receiving domain's secret key. It does not reveal the identifier and cannot be reversed by the receiving system.
Domain	A government sector or system with its own identifiers (e.g., Civil Registry, RSTA, Tax Authority)
Domain Isolation	The same person gets a different pseudonym in each domain, so domains cannot link their records without IDCB
Operational Context (Purpose)	The declared reason for a request (e.g., traffic_enforcement). Decides which rule applies.
Trust Boundary	An approved permission for one domain to convert to another for a stated purpose. Everything else is refused.
Conversion Rule	The approved settings for one domain pair and purpose: who may call, what may be returned, how long mappings last, and the legal basis
Legal Basis Reference	The law, directive or data-sharing agreement (MoU) that permits a rule
Mapping	IDCB's stored link between a person or asset and the pseudonym issued for it in one domain under one rule
Cascade Revocation	When a mapping is revoked, the mappings created through it in a recursive resolution are revoked too
Superseded Mapping	A mapping replaced because a new conversion returned a different result (e.g., a new vehicle owner)
Scope Violation	A request refused for having no trust boundary, no active rule, a caller not permitted, or a missing API scope. Blocked before any lookup.
Authorised Retrace	The tightly controlled process for recovering the real identity behind a pseudonym, needing a case reference and approval by a Retrace Approver

Pattern A / Pattern B	How a domain is connected: A = IDCB looks up the domain's registry; B = the domain stores only pseudonyms and IDCB holds the link (Appendix G)
Portal-first Conversion	My Bhutan Portal gets the agency's pseudonym from IDCB before sending an application, so the agency never receives the CID
Consumer	A registered system that calls IDCB: My Bhutan Portal, a government service system, or a service-provider or back-office system
MBP	My Bhutan Portal: the single government portal for citizens, businesses and service-provider officers, replacing PSP, CBP, CP and BP
NDI / SSO	National Digital Identity, and Single Sign-On (the backup to NDI). Both issue the tokens IDCB accepts.
NDE	National Data Exchange platform, including APIG (API gateway), INTP (registry access) and EVTB (events)
JLB / NTFB	Journaling Block (long-term signed audit record) and Notification Block (message delivery)
HSM	Hardware Security Module: certified hardware that holds and uses cryptographic keys
HMAC-SHA256	A keyed hash function used to make pseudonyms; the same input and key always give the same output
mTLS	Mutual TLS: both sides prove their identity with certificates
Mediated Check	A yes/no question answered by the agency that holds the data, carried by IDCB, so the asking agency never learns the other agency's identifier for the person

Appendix B: Pseudonymisation Algorithms

Algorithm	Type	Use Case	Properties
HMAC-SHA256	Deterministic, domain-keyed hash	Standard conversion results where consistency across calls is required (same input + key = same pseudonym)	Cannot be reversed or computed without the domain key held in the HSM. One key per domain. Collisions handled under FR-1.7. A new pseudonym is issued after revocation (FR-5.3).

Appendix C: API Reference Summary

Method	Endpoint	Description
POST	/api/v1/convert	Convert an identifier into a pseudonym (FR-3.1)

EVTB	idcb.bulk.request / idcb.bulk.result	Submit up to 1,000 conversions and receive per-item results (FR-3.2)
POST	/api/v1/resolve	Turn a pseudonym back into its asset identifier; never a personal identifier (FR-3.7)
POST	/api/v1/check	Ask a registered yes/no question using another domain's data (FR-3.8)
POST	/api/v1/notify/channel	Get contact details for a pseudonym so a notice can be delivered (FR-8.5)
GET	/api/v1/convert/{conversion_id}/trace	How a conversion was produced (FR-3.5)
GET	/api/v1/mappings/{mapping_id}	Mapping details, never the underlying identifier
DELETE	/api/v1/mappings/{mapping_id}	Revoke a mapping with a reason; cascades (FR-5.3)
GET	/api/v1/audit/{record_id}/verify	Verify an audit record's signature (FR-7.4)
GET	/api/v1/health	Liveness (FR-8.7)
GET	/api/v1/health/ready	Readiness: database, HSM, cache, JLB
GET	/api/v1/health/dependencies	Status of NDI, SSO, INTP, EVTB, JLB, HSM and each Pattern A registry
GET / POST	/api/v1/admin/domains, /identity-types, /trust-boundaries, /rules	Admin API for all setup in the admin UI (FR-6.1); changes go through approval
GET / POST	/api/v1/admin/consumers	Register and manage consumers (FR-6.3, FR-6.4)
POST	/api/v1/admin/retrace	Request, approve and view Authorised Retrace (FR-4.6)

Appendix D: Use Case Domain Reference

Source Domain	Target Domain	Context	Use Case
CIVIL_REG (CID)	VEH_REG	register_subject	Portal-first conversion when a citizen applies for vehicle registration on My Bhutan Portal
CIVIL_REG (CID)	VEH_REG (VRN)	owner_lookup	Find all vehicles registered to a citizen
VEH_REG (VRN)	CIVIL_REG	traffic_enforcement	Identify a vehicle's owner for a traffic notice

CIVIL_REG (CID)	HEALTH	emergency_care	Get the Health pseudonym so records can be retrieved across hospitals
BIZ_REG (BRN)	LAND (LPN)	tax_assessment	Find land parcels held through a business, for property tax
LAND (LPN)	CIVIL_REG	notify_landowner	Notify a landowner through NTFB
CIVIL_REG (CID)	TAX (TIN)	taxpayer_verification	Verify a taxpayer in a cross-agency service
BIZ_REG (BRN)	CUSTOMS (IMPNo)	customs_clearance	Identify an importer for customs processing
IMMIGRATION	VEH_REG	passport_issuance_check	Mediated check for unpaid traffic fines before issuing a passport
CIVIL_REG (CID)	Service's own domain (e.g., VEH_REG)	user_registration	Create the user's mapping when they register with the service
CIVIL_REG (CID)	Service's own domain (e.g., VEH_REG)	user_sign_in	Find the registered user's pseudonym at sign-in

Appendix E: Key Performance Indicators

KPI	Unit	Description
Conversions performed	Count	Total conversions, by domain pair and purpose
Conversion time	Milliseconds	95th percentile, store or cache vs registry
Active rules	Count	Number of ACTIVE conversion rules
Rules with a legal basis	Percentage	Target 100%
Registry-related failures	Count	Conversions refused or marked stale because a registry was down
Connected consumers	Count	Approved consumer systems, by type
Identity types in use	Count	Persons, vehicles, parcels and others
Recursive conversions	Count	Conversions that followed a chain
Scope violations	Count	Refused out-of-policy requests; target zero

Superseded mappings	Count	Out-of-date links detected and replaced
Authorised Retraces	Count	Retrace requests, approvals and rejections

Appendix F: External References

1. Bhutan DPI Blueprint 2025, Royal Government of Bhutan
2. Information, Communications and Media Act of Bhutan
3. National Digital Identity Act of Bhutan 2023
4. Government Enterprise Architecture Framework (GEA-F) v3.0, GovTech Agency, Bhutan
5. Related DPI BRDs: NDI, SSO, My Bhutan Portal, PSR, NDE (APIG, INTP, EVTB), JLB, NTFB
6. GovStack Building Block Specifications: https://www.govstack.global/
7. GDPR, Regulation (EU) 2016/679, Articles 5 and 25 (reference principles only)
8. NIST SP 800-188: De-Identifying Government Datasets
9. NIST SP 800-175B: Guideline for Using Cryptographic Standards
10. FIPS 140-2 / FIPS 140-3: Security Requirements for Cryptographic Modules
11. RFC 2104 (HMAC) and RFC 4648 (Base32 encoding)
12. OWASP Application Security Verification Standard (ASVS), Level 2
13. ISO/IEC 29101:2018, Privacy Architecture Framework
14. ISO/IEC 27001:2022, Information Security Management Systems

Appendix G: Domain Integration Patterns

IDCB supports two integration patterns. Each domain's pattern is recorded in its domain registration (integration_pattern, FR-1.2).

Pattern A: Registry-backed conversion (existing systems). The domain's registry keeps its own records, including the CID link. When a conversion is requested, IDCB looks up the registry through INTP and returns only a pseudonym to the caller. Used in Scenarios 1 and 3.

Pattern B: Pseudonym at registration (new or re-engineered systems). When a person registers with a domain system (e.g., RSTA vehicle registration), the CID is converted once into the domain's pseudonym. IDCB stores the protected CID with the pseudonym. The domain system stores only the pseudonym as its key, together with its own business data, and never stores the CID. Later

cross-domain conversions for this domain are answered from IDCB's own mapping store. The owning agency must confirm in writing that its system stores no CIDs before the domain is activated.

Portal-first conversion (recommended for My Bhutan Portal services). When a person applies through My Bhutan Portal, the portal calls IDCB to convert the CID into the agency's pseudonym before sending the application. The agency system receives the pseudonym only, never the CID, not even briefly. IDCB returns only the pseudonym and does not carry the application.

Moving from Pattern A to Pattern B. An agency can move an existing system to Pattern B by converting its stored CIDs in bulk (FR-3.2), replacing them with pseudonyms, and then deleting the CIDs. The change of pattern needs approval (FR-1.6).

Under Pattern B, the domain's own administrators can see all of the domain's data but cannot link a pseudonym to a real person. If the domain lawfully needs the real identity (e.g., a legal request or a data correction), it must use Authorised Retrace (FR-4.6), which needs a case reference and approval by a Retrace Approver. Every retrace is logged separately.

8. Usage Scenarios

8.1 Scenario 1: Vehicle Owner Identification Without CID Exposure

Persona: Traffic Police Officer, roadside vehicle check

Context: The RSTA traffic enforcement system needs to notify a vehicle's registered owner of a violation, without the owner's CID reaching the enforcement system, the officer's terminal or NTFB.

Step	Actor/System	Action
1	**Traffic Officer / RSTA Enforcement System**	The officer enters the vehicle number (VRN: BT-123456). The enforcement system sends a conversion request.
2	**RSTA Enforcement System → IDCB**	POST /api/v1/convert { source_id: 'VRN:BT-123456', target_domain: 'CIVIL_REG', operational_context: 'traffic_enforcement' }
3	**IDCB, Authentication**	Checks the RGoB PKI certificate and the NDI-issued token (or SSO-issued, if NDI is down), including the idcb.convert API scope.
4	**IDCB, Policy Check**	Checks in order: purpose stated, trust boundary VEH_REG → CIVIL_REG for traffic_enforcement exists, active rule found (legal basis: Road Safety Act S.47), and the enforcement system is a permitted caller.

5	**IDCB → INTP → Vehicle Registry**	Looks up the vehicle's registered owner through INTP (Pattern A).
6	**IDCB, Pseudonymisation**	Makes the owner's pseudonym with the RSTA domain key: TRF_k3m9q2x7p4a8r5tn. The CID stays inside IDCB.
7	**IDCB → JLB and EVTB**	Signed audit record sent to JLB: conversion_id, source type VRN, target CIVIL_REG, purpose traffic_enforcement, caller, rule and legal basis. mapping.created published to EVTB if this is a new mapping.
8	**IDCB → RSTA Enforcement System**	HTTP 200 { conversion_id, pseudonym: 'TRF_k3m9q2x7p4a8r5tn', rule_id, rule_version, staleness_flag: false }
9	**RSTA → NTFB → IDCB**	RSTA asks NTFB to send the notice to pseudonym TRF_k3m9q2x7p4a8r5tn. NTFB calls POST /api/v1/notify/channel; IDCB checks the rule, gets the owner's contact details through INTP, and returns only those contact details (FR-8.5).
10	**NTFB → Owner**	NTFB delivers the notice. The enforcement system, the officer's terminal and NTFB never received the CID.

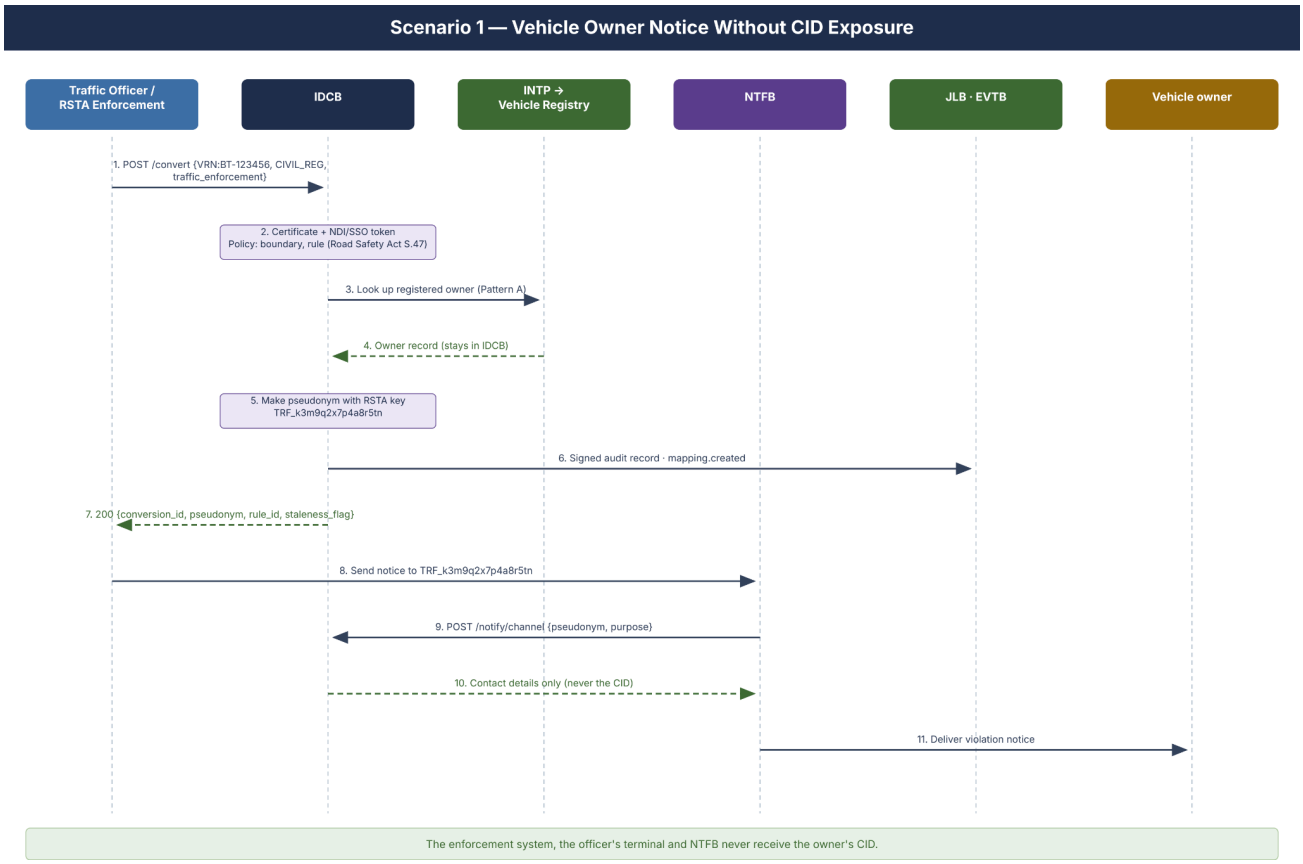


Figure 10: Scenario 1 - vehicle owner identification without CID exposure process flow

Key IDCB Capabilities Exercised: Purpose and policy check, registry lookup through INTP, HMAC-SHA256 pseudonymisation, domain isolation, audit logging, notification support for NTFB.

8.2 Scenario 2: Emergency Health Access Without CID Sharing

Persona: Dr. Sonam Wangchuk — Emergency Department Physician, JDWNRH

Context: A patient arrives unconscious at Jigme Dorji Wangchuck National Referral Hospital. The emergency team needs the patient's records from other hospitals quickly, without any hospital system receiving the CID.

Step	Actor/System	Action
1	**Emergency System → NDI**	Accompanying family members identify the patient through NDI. The emergency system receives the authenticated session.
2	**Emergency System → IDCB**	POST /api/v1/convert { source_id: 'CID:11501001234', target_domain: 'HEALTH', operational_context: 'emergency_care' }, with the physician's NDI identity as the acting user.
3	**IDCB, Policy Check**	Confirms the trust boundary, the active emergency_care rule, its legal basis (Emergency Health Regulations), and that the emergency system is a permitted caller.
4	**IDCB → Emergency System**	Returns the patient's Health domain pseudonym: HLTH_w6c2y8dek3m9q2x7. The CID is not returned.
5	**Emergency System → Hospital Systems**	Requests the patient's records from other hospitals using the same Health pseudonym. All hospitals are in the Health domain, so they recognise it (FR-4.2). No hospital receives the CID.
6	**IDCB → JLB**	The conversion is logged with the system, the physician's NDI identity, the purpose, the legal basis and the time.

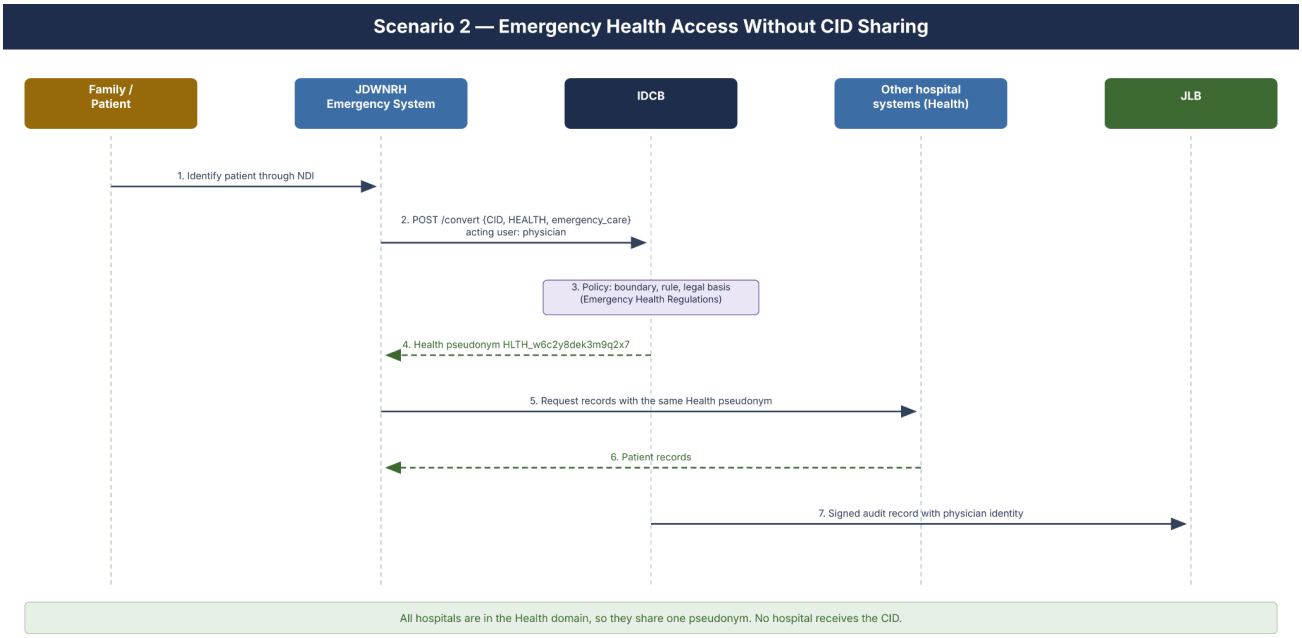


Figure 11: Scenario 2 - emergency health access process flow

Key IDCB Capabilities Exercised: Purpose and policy check, legal basis, pseudonym generation, domain isolation, audit logging with acting user.

8.3 Scenario 3: Property Tax Assessment with Multi-Domain Resolution

Persona: Revenue Officer, Department of Revenue and Customs

Context: DRC needs every land parcel held through a business for annual property tax, without the business owner's or the director's CID reaching the tax system.

Step	Actor/System	Action
1	**DRC Revenue System → IDCB**	POST /api/v1/convert { source_id: 'BRN:BHCO001234', target_domain: 'LAND', operational_context: 'tax_assessment' }. The rule sets recursive, one-to-many.
2	**IDCB, Recursive Resolution**	Step 1: Business Registry finds the director. Step 2: Land Cadastre finds the director's parcels. Policy is checked at each step (FR-3.4). The director's identity stays inside IDCB.
3	**IDCB → DRC Revenue System**	Returns an array of parcel pseudonyms made with the TAX domain key: [TAX_p4a8r5tnw6c2y8de, TAX_m9q2x7p4a8r5tnw6, TAX_c2y8dek3m9q2x7p4].
4	**DRC Revenue System → IDCB**	Turns each parcel pseudonym into its parcel number through POST /api/v1/resolve. This is allowed because parcel numbers are asset identifiers and the rule permits reverse resolution (FR-3.7).

5	**DRC Revenue System**	Gets parcel details from the Land Cadastre using the parcel numbers, and calculates tax. No personal identifier was received at any point.

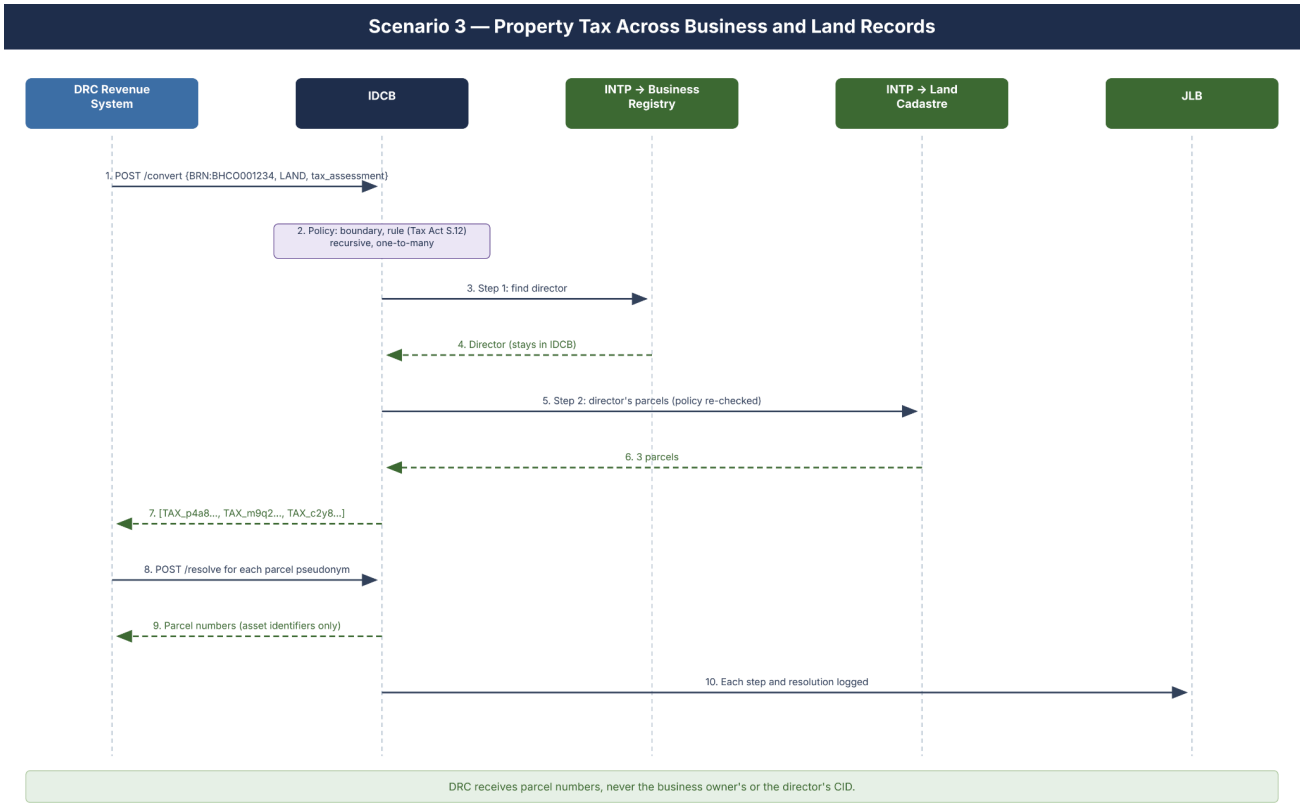


Figure 12: Scenario 3 - property tax assessment process flow

Key IDCB capabilities used: Recursive resolution with per-step policy checks, one-to-many results, reverse resolution for asset identifiers, audit logging.

8.4 Scenario 4: Applying for Vehicle Registration on My Bhutan Portal

Persona: Passport Officer, Department of Immigration

Context: Before issuing a passport, the officer must confirm the applicant has no unpaid traffic fines. Immigration and RSTA hold the applicant under different pseudonyms and must not be able to link their records.

Step	Actor/System	Action
1	**Passport System → IDCB**	POST /api/v1/check { subject_ref: 'IMM_r5tnw6c2y8dek3m9', target_domain: 'VEH_REG', check_code: 'unpaid_fines', operational_context: 'passport_issuance_check' }
2	**IDCB, Policy Check**	Confirms the check is registered by RSTA, the trust boundary exists and the legal basis is recorded.

3	**IDCB, Conversion**	Converts the Immigration pseudonym to the RSTA pseudonym internally. Neither pseudonym leaves IDCB.
4	**IDCB → INTP → RSTA**	Asks RSTA's registered check endpoint "unpaid fines?" for the RSTA pseudonym. RSTA answers "yes".
5	**IDCB → Passport System**	Returns { answer: 'yes' } and nothing else.
6	**IDCB → JLB**	Logs the check with caller, purpose and outcome.

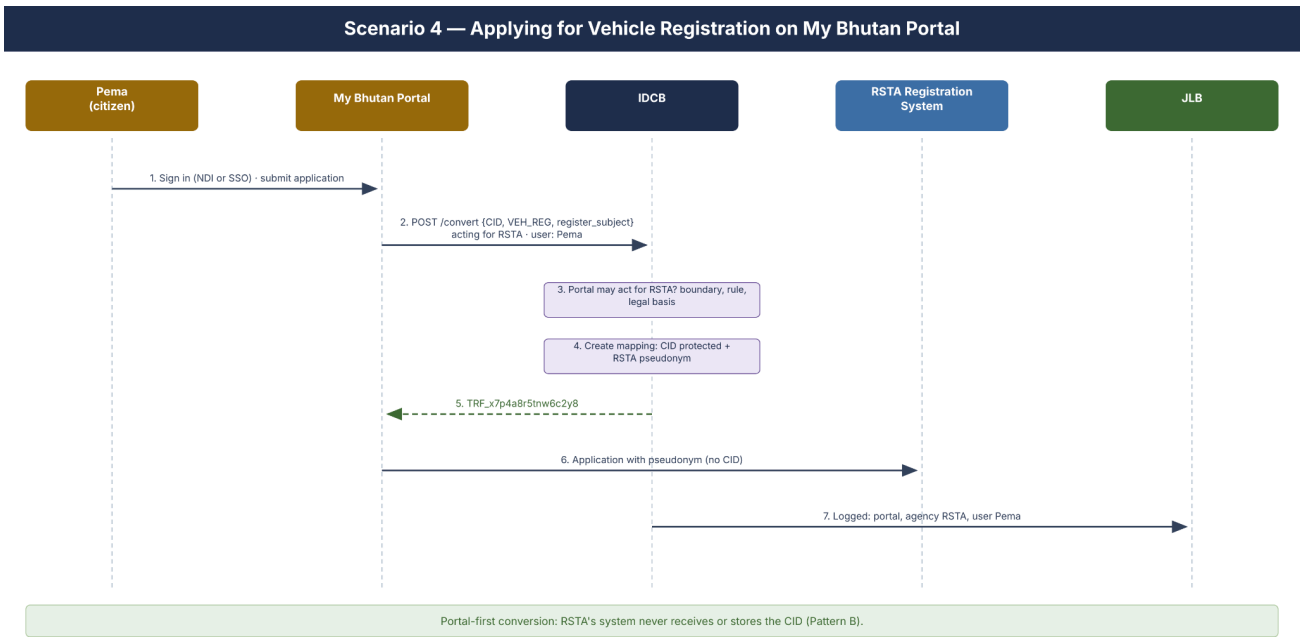


Figure 13: Scenario 4 - portal-first vehicle registration

8.5 Scenario 5: Passport Fine Check Without Linking Records

Persona: Passport Officer, Department of Immigration

Context: Before issuing a passport, the officer must confirm that the applicant has no unpaid traffic fines. Immigration and RSTA hold the applicant under different pseudonyms and must not be able to link their records.

Step	Actor/System	Action

1	**Passport System → IDCB**	POST /api/v1/check { subject_ref: IMM_r5tnw6c2y8dek3m9, target_domain: 'VEH_REG', check_code: 'unpaid_fines', context: operational_context }
2	**IDCB, Policy Check**	Confirms the check is registered by RSTA, the trust boundary exists, and the legal basis is recorded.
3	**IDCB, Conversion**	Converts the passport pseudonym to the RSTA pseudonym internally. Neither pseudonym leaves IDCB.
4	**IDCB → INTP → RSTA**	Asks RSTA's registered check endpoint "unpaid fines?" for the RSTA pseudonym. RSTA answers "yes".
5	**IDCB → Passport System**	Returns { answer: 'yes' }. Nothing else.
6	**IDCB → JLB**	Logs the check with caller, purpose and outcome.

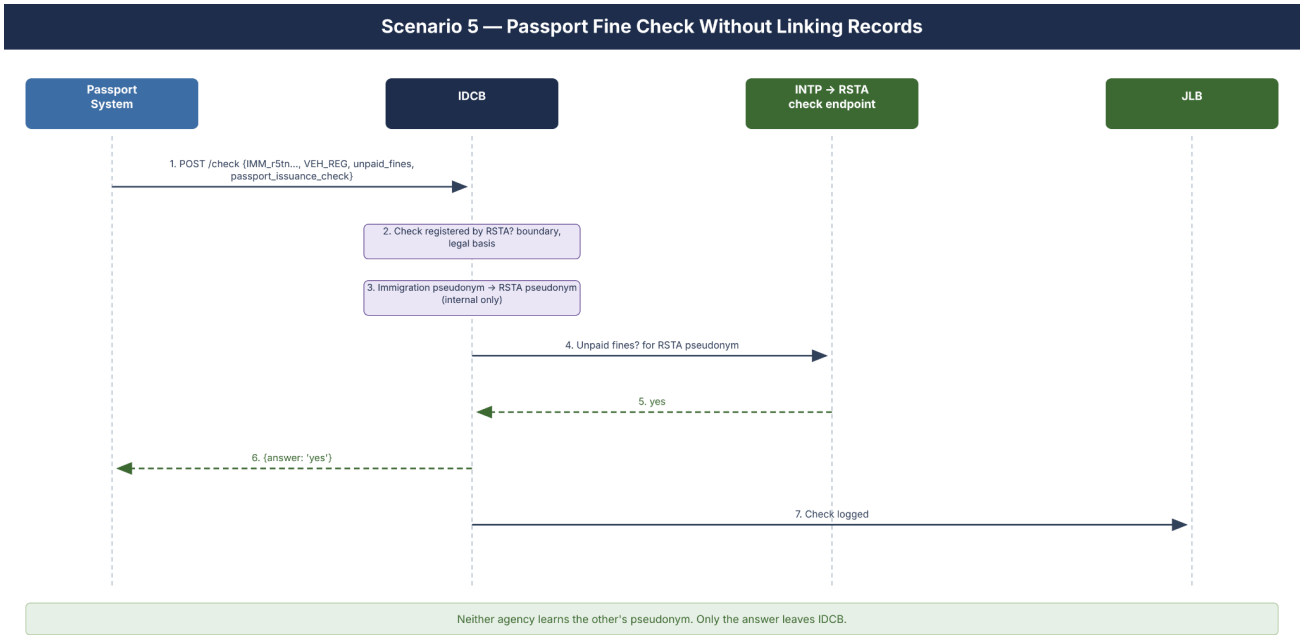


Figure 14: Scenario 5 - passport fine check

Key IDCB capabilities used: Mediated check, internal pseudonym conversion, legal basis check, audit logging.

8.6 Scenario 6: Registering and Signing In to a Government Service

Persona: Pema Choden, citizen

Context: Each government service (e.g., RSTA) registers its own users and stores them only under its own pseudonym, never the CID. So when Pema registers, IDCB creates her RSTA pseudonym once. Every time she signs in, RSTA asks IDCB for that same pseudonym to find her records.

Step	Action
1	**Registration (once):** The RSTA service sends Pema's CID with user_registration. IDCB creates the mapping and returns TRF_r5tnw6c2y8dek3m9. RSTA stores only this pseudonym.
2	**Sign-in (every time):** Pema signs in to the RSTA service with NDI (or SSO). RSTA sends her CID with user_sign_in. IDCB looks up and returns the same pseudonym, and RSTA opens her records.
3	**Not registered:** IDCB returns 404 NOT_REGISTERED, and the service asks her to register.

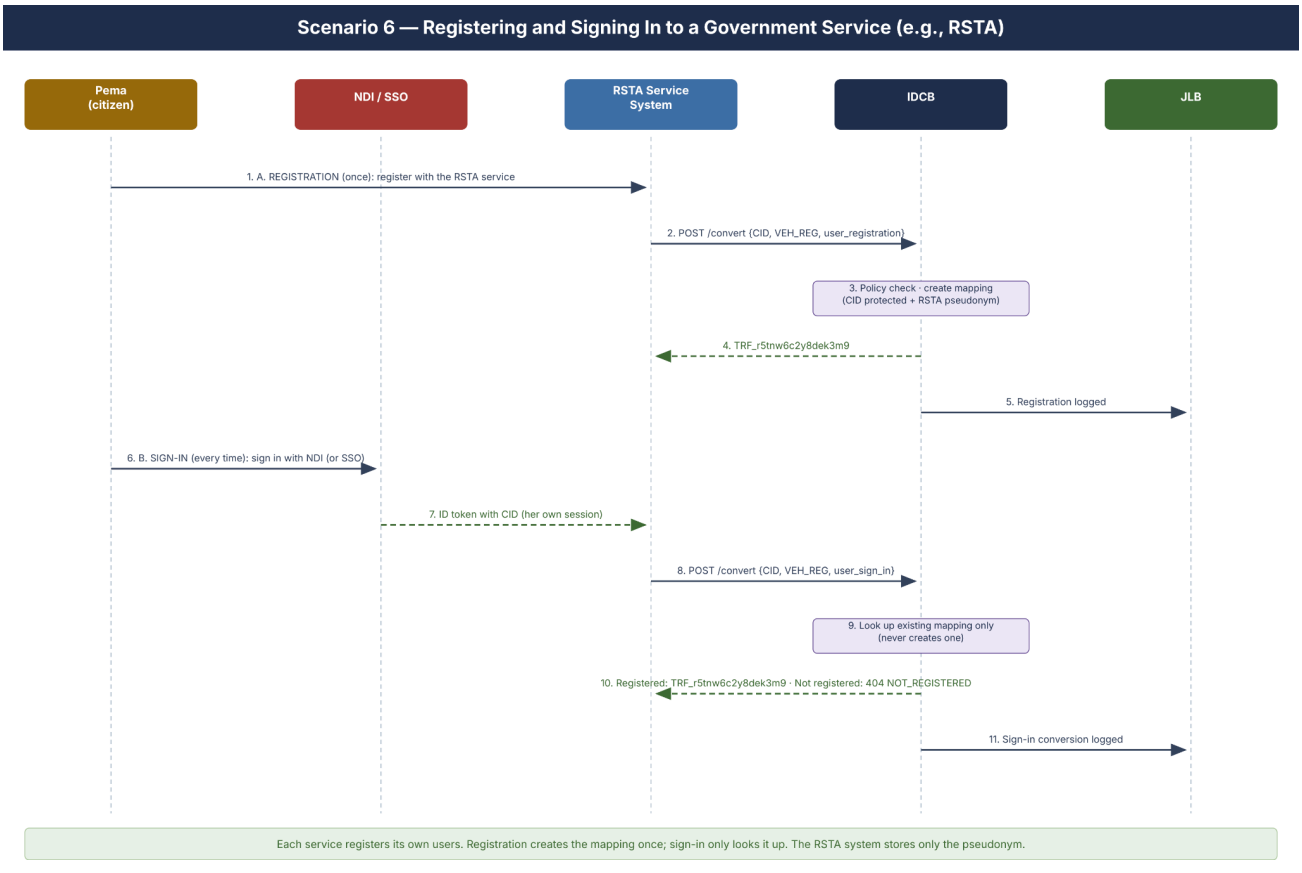


Figure 15 : Scenario 6 - Registration and Sign_In

Key IDCB capabilities used: Mapping creation at registration, sign-in lookup, domain isolation, audit logging.