Unified Client Support (UCS)

Business Requirements Document (BRD)

Version: 5.0
Date: October 2026
Status: Final Review

Document control

Version	Date	Author	Changes
5.0	October 2026	Cross-functional team	Final Review

Table of contents

Document control..... 1
1. Introduction..... 4
1.1 Purpose and scope..... 4
1.1.1 Purpose..... 4
1.1.2 Scope..... 4
1.1.2.1 In scope..... 4
1.1.2.2 Out of scope..... 6
1.2 Business value..... 7
1.2.1 For citizens..... 7
1.2.2 For agencies..... 8
1.2.3 For GovTech support..... 8
1.3 Success metrics and KPIs..... 8
2. Platform overview..... 10
2.1 Digital government ecosystem position..... 10
2.2 Support model..... 10
2.2.1 Two intake paths..... 10
2.2.2 Three stages on the citizen path..... 11
2.2.3 Priority tier and support level (indicative)..... 11
3. Process flows..... 14
3.1 Path A, citizen initiated..... 14
3.2 Path B, agency initiated..... 16
3.3 Stage 3, GovTech support..... 17
3.4 SLA handling and the reply route..... 17
4. Example User scenarios (indicative for UCS)..... 18
4.1 Scenario 1: Citizen-initiated technical problem..... 18
4.1.1 Context..... 18
4.1.2 Interaction description..... 18
4.2 Scenario 2: Agency-initiated technical problem..... 18
4.2.1 Context..... 18
4.2.2 Interaction description..... 18
4.3 Scenario 3: supervisor dashboard review..... 19
4.3.1 Context..... 19
4.3.2 Interaction description..... 19
5. Platform capabilities..... 19
5.1 Case management..... 19
5.2 Multi-channel gateway..... 19
5.3 Agent workbench..... 20
5.4 Triage and escalation..... 20
5.5 Administration and configuration..... 20
5.6 Analytics and monitoring..... 20
5.7 Security and compliance..... 21

5.8 Citizen experience and accessibility....21
6. Functional requirements....21
6.1 For Unified Client Support (UCS)....21
6.1.1 UCS-FR-1: case management....21
6.1.2 UCS-FR-2: multichannel gateway....24
6.1.3 UCS-FR-3: agent workbench (Business Portal)....25
6.1.4 UCS-FR-4: escalation and triage....26
6.1.5 UCS-FR-5: administration and configuration....28
6.1.6 UCS-FR-6: analytics and reporting....29
6.1.7 UCS-FR-7: accessibility and localisation....30
8. Logical component architecture....31
8.1 Subsystem components (indicative)....31
8.2 Technology stack (indicative)....32
8.3 Dependency register (Indicative)....32
9. Data, security and compliance....35
9.1 for Unified Client Support (UCS)....35
9.1.1 Data model (Indicative)....35
9.2 Data retention (indicative)....36
9.3 Security controls....37
9.3.1 Encryption....37
9.3.2 Access control....37
9.3.3 API security....37
9.3.4 Incident response....37
10. Appendices....38
10.1 Glossary....38

1. Introduction

1.1 Purpose and scope

1.1.1 Purpose

This Business Requirements Document defines the functional, non-functional and integration requirements for the Unified Client Support (UCS). It states why the system is required, the support process it carries, the actors it serves, and the boundary of what is to be procured and delivered. It supersedes all prior capability notes, concept papers and informal scoping material relating to UCS.

UCS is centralized, multi-institution case management for citizen and business support requests across all government digital services. It exists because a citizen who cannot complete a public service has no single place to report it, and the government has no single record of that report from the moment it is raised until it is closed. Complaints reach agencies through channels that do not connect to one another. An agency cannot easily separate a pending action of its own from a fault in the underlying system. Neither the citizen nor the agency can see where a technical problem sits or when it will be fixed.

UCS provides a support process with two entry points, one for the citizen and one for the agency. Technical problems are resolved by GovTech and Vendor according to the priority P1- P4 required and support level required, L1, L2 or L3.

1. **Citizen initiated.** The citizen raises the concern through the Support Services menu on the Government portal(MyBhutan portal). The case is routed to the queue of the agency that owns the service, where back office staff/ service providers receive. When the cause is technical, the agency forwards it to GovTech.
2. **Agency initiated.** The agency raises a technical problem and it is directly forwarded to GovTech, based on priority and level of support GovTech and Vendor resolves the problem.

Every case carries a single reference number from intake to closure, is traceable by the citizen using the reference number or the CID, is answered within a stated SLA, and is rated by the citizen once it is closed.

1.1.2 Scope

1.1.2.1 In scope

ID	In scope
S1	A Support Services menu on the Government Portal(MyBhutan Portal) that takes the citizen.
S2	A support form on the Unified Client Support (UCS) comprising a drop-down list of services (services that are onboarded on Public Service Registry(PSR)), a free text comment field, an optional file or image attachment, and a Submit function.
S3	Creation of a support case on submission, carrying a reference number, the selected service, and the citizen's comment.

ID	In scope
S4	Delivery of the case to the back office staff/ Service Providers of the agency that owns the selected service, with notification on submission.
S5	Back office/Service Providers confirmation of whether any action has already been taken, completion of the pending action, and notification of the outcome to the citizen.
S6	Classification of a case as a dependency on other agency action, can select the service from the drop down-list (from PSR) and forward the case to that agency with case with optional attachment of files and images, if the case is a technical issue, it's forwarding to GovTech, carrying the agency's comment and the record of the action already taken.
S7	An agency-initiated by agency staff / Service Providers where they submit a technical problem to GovTech directly, comprising service selection, upload of files and images, and a text message.
S8	Determination by GovTech of whether the issue requires P1, P2, P3 or P4 priority and L1, L2 or L3 support, if it is needed support from vendors should be able to forward vendors with the issues and support they require via email/notification and both the agency and the citizen can track the status of the issue and the resolution period for that level.
S9	Case status tracking by the citizen using the reference number or the CID, and by the agency.
S10	A reply route on the originating channel for a citizen whose service has not been delivered within the stated SLA, reopening the same case rather than creating a new one.
S11	Closure of the case on resolution, with notification to the citizen and the agency, followed by a satisfaction rating collected from the citizen.
S12	Configuration of agency queues, routing of services to owning agencies, working hours, notification channels, and configurable SLA periods per priority tier and per support level.
S13	Selection of the agency, and of the issue or query, by the citizen, with a free text field for the description.
S14	Attachment of files and images at the point of submission on both routes.
S15	Virus scanning of every attachment, with a configurable maximum file size.
S16	An audit record of case creation, routing, classification, forwarding, closure and rating.
S17	Aggregation of post-case satisfaction feedback and KPI reporting built on it.

ID	In scope
S18	A bilingual support interface, English and Dzongkha, meeting WCAG 2.1 Level AA (Only for User Interface).
S19	An omnichannel support gateway: Government Portal (MyBhutan portal), email, and SMS.
S20	Integration with the building blocks listed in the dependency register at section 8.3.
S21	Operational dashboards and reporting for agency supervisors, GovTech support and institutional leadership, over the platform's own case data.
S22	An administration and configuration console for tenant management, agent roles, queues, SLA rules, channel configuration and knowledge base governance.
S23	Multi-tenant separation by agency, so that a tenant sees only the cases raised against the services it owns.
S24	A per-service report for each institutional tenant over a selectable period, showing case volume, counts by status, response time, SLA compliance rate and average satisfaction rating.
S25	A report for GovTech support covering the technical cases referred to it across all agencies, broken down by service, owning agency and support level.

Whether citizens / service providers need the support from the 1199, they can use this 1199 support to use the UCS.

1.1.2.2 Out of scope

ID	Out of scope
O1	Delivery of the public service itself. The pending action is completed in the agency line of business system; UCS records that it was done.
O2	Diagnosis and repair of the technical fault inside GovTech. UCS covers the handover, the support level decision, the SLA and the notifications, not GovTech's internal incident and problem management.
O4	Survey instruments and feedback collection beyond the satisfaction rating taken at closure, which belong to the Feedback (FDBK) and Survey (SRVB) blocks.
O5	Authorship and governance of FAQ content. UCS consumes FAQB content by API only.
O6	Training, hosting or serving of machine learning models. UCS consumes the AI Processing Platform (AIPP)
O7	Computation of cross-institutional analytics. UCS publishes aggregates to, and consumes the programme view from, the shared analytics platform.

ID	Out of scope
O8	Authentication, identity issuance and credential recovery, which are provided by SSO and, behind it, NDI.
O9	Real time chat between a citizen and an agent. The process defined here is case based with notification.
O10	Change requests and enhancement requests raised by agencies. The agency-initiated route covers technical problems in services already in operation.
O11	Workflow orchestration of service approval chains, which belongs to the Workflow Engine (WFE) or the Service Orchestration Platform (SOP).
O12	Payment processing and financial transactions.
O13	GovStack Product which is held by the IT Asset Repository (ITAR) block. UCS consumes ITAR data and does not maintain a register of its own.
O14	Social media channel management, content moderation and proactive social media monitoring.
O15	HR and staff performance management for support agents. UCS provides case-level performance metrics only.
O16	Outbound marketing and campaign communication. UCS handles reactive support only.
O17	Counter and walk-in support channels until each is configured as a supported channel under this block.

1.2 Business value

1.2.1 For citizens

- One entry point for support on all government digital services. The citizen goes to the Support Services menu rather than working out which agency owns the problem and how to reach it.
- One reference number for the whole life of the case. When the case moves from the agency to agency or agency to GovTech it keeps the same number, and the agency's comment, files, images and record of action already taken move with it, so the citizen does not repeat the story at each transfer.
- The citizen checks status alone, by reference number or CID, instead of calling to ask.
- GovTech states the resolution period when it classifies the issue, so the citizen knows what to expect and when.
- If the service is still not delivered within that period, the reply reopens the same case rather than starting a new one from scratch.
- A choice of channel: the eService portal, email, and SMS

- The interface works in English and Dzongkha and meets WCAG 2.1 Level AA, so language and disability are not barriers to raising a case.
- The satisfaction rating at closure feeds the per-service reports, so the citizen's view of the service counts for something beyond the individual case.

1.2.2 For agencies

- Cases against the agency's services arrive in one queue, routed by service ownership, instead of arriving through unconnected channels.
- The back office/service provider confirms whether the pending action is its own before deciding anything, which separates an agency backlog from a platform fault.
- A defined route from agency to agency for requirement of dependency system action and agency to GovTech for technical faults, carrying the agency comment and the record of action already taken, so the referral does not start a fresh investigation.
- A direct route on the agency's own technical problems, with files and images attached at the point of submission.
- Supervisors and institutional leadership get per-service reports over a selectable period: case volume, counts by status, response time, SLA compliance rate and average satisfaction rating.
- Tenant separation means each agency sees only the cases raised against the services it owns.
- No duplicated helpdesk infrastructure, and a shared knowledge base rather than one per agency.

1.2.3 For GovTech support

- One intake for technical faults from every agency, whether they arrive by citizen referral or direct agency submission.
- P1, P2, P3 or P4 priority and L1, L2 and L3 classification at intake, with the resolution period attached to the level, so triage and resourcing follow a stated rule.
- Evidence arrives with the case: service, agency comment, action already taken, files and images. That cuts the exchange of messages before work can start.
- Service and asset context from PSR, ITAR and OBVP on the case itself, so the failing component and its owner are identified without a separate enquiry.
- A cross-agency report broken down by service, owning agency and support level, which shows where the recurring faults sit.

1.3 Success metrics and KPIs

KPI	Target	Measurement method
First contact resolution rate	75% or more of cases resolved by the owning agency without referral to GovTech	Case lifecycle data, resolved-without-referral flag
P1 response time	Under 1 hour	SLA timer from creation to first agent response

KPI	Target	Measurement method
P2 response time	Under 4 hours	SLA timer from creation to first agent response
P3 response time	Under 1 business day	SLA timer from creation to first agent response
L1 resolution time	Within the configured L1 period	SLA timer from support level assignment to resolution
L2 resolution time	Within the configured L2 period	SLA timer from support level assignment to resolution
L3 resolution time	Within the configured L3 period	SLA timer from support level assignment to resolution
Citizen satisfaction	4.0 out of 5.0 or better, rolling monthly average	Post-closure rating collected via NTFB
SLA breach rate	Under 5% of all cases	Breach events from the audit log
Platform availability	99.5% or better monthly uptime	Infrastructure monitoring and synthetic transactions
Case backlog rate	Under 10% of open cases older than 5 business days	Open case age distribution
Knowledge base coverage	80% or more of the top twenty recurring case categories covered by an article	Pattern detection output against the published article index

2. Platform overview

2.1 Digital government ecosystem position

UCS is a shared support infrastructure. It sits in the Client Support group of the DPI building block taxonomy and serves every government digital service portal and application, rather than belonging to any one agency's application stack. Institutional tenants consume it; none of them owns it.

Its upstream consumers are the Government Portal (MyBhutan Portal), which hosts the support form, the agent workbench and the public self-service entry point respectively. Its downstream dependencies are PSR for service ownership and routing, MDMB for the Master Data, Respective Agency for Single Source of Truth (SSOT) that includes transactional data, SSO and NDI as the identity authority behind it, NTFB for outbound notification, JLB for immutable audit, DMS (DOCS) for attachment storage, NDE (EVTB) for event publishing, ITAR and OBVP for service and asset context.

2.2 Support model

2.2.1 Two intake paths

	Path A, citizen raised	Path B, agency raised
Raised by	Citizen	Agency staff delivering the service
Where	Support Services menu on Government Portal (MyBhutan Portal) / UCS link	Support Services menu on Government Portal(MyBhutan Portal) / UCS link
Form content	Service drop-down, comment, files and images attachment, Submit	Service selection, files and images, Comments, Submit.
First recipient	Agency back office staff	GovTech support
Identity on the case	CID from the session token	Agency staff identity and the institution code
Notified of the outcome	Citizen, and the agency once GovTech is involved	The raising agency
Tracking	Government Portal(MyBhutan Portal)	Government Portal (MyBhutan Portal)
Rated at closure	Yes	No

2.2.2 Three stages on the citizen path

Stage	Who holds the case	What happens	Exit condition
1. Citizen	Citizen,	Menu, login, service selection, comment, submit	Case created and delivered to the owning agency queue.
2. Agency	Back office staff	Confirm whether any action has already been taken. If not, carry it out and notify the citizen. If it was taken and needed another agency action, can be forwarded to that agency and the problem is technical, forward to GovTech with a comment	Resolved at the agency, or forwarded to GovTech
3. GovTech	GTA support, L1 to L3	Assign the support level, notify agency and citizen of the issue and the resolution period, work the fix	Resolved and the case closed

Path B enters at stage 3 and skips stages 1 and 2.

2.2.3 Priority tier and support level (indicative)

The platform runs two independent clocks on a case, and they measure different things. Both are shown on the case and both are configurable per institutional tenant.

	Priority tier	Support level
Values	P1 Critical, P2 High, P3 Standard, P4 Low	L1, L2, L3
What it expresses	How urgent the case is for the requester	How deep the technical fault is
Set by	Triage at creation, adjustable by an agent with a reason	GovTech at intake of a technical case
Applies to	Every case	Technical cases only
Drives	The response target, that is the time to first agent response, and queue order	The resolution target, that is the period quoted to the citizen and the agency.

A non-technical case handled entirely by the agency carries a priority tier and no support level. Its resolution target is the tenant default for the tier.

1. **Priority tier: impact × urgency**

	Many people (service down, or several agencies)	Some people (one service)	One person
Can't work around it, or a deadline is at risk	P1	P2	P3
Can work around it	P2	P3	P4

Priority	When to use it (criteria)	Example	Response
P1 (critical)	A service used nationally or by several agencies is down, or there is a security breach or leaked data	Citizens can't log in to the Portal through SSO/NDI; the payment gateway is down	< 1 hour
P2 (high)	One service is degraded for many users, or a deadline is at risk	Trade licence renewal fails for all applicants	< 4 hour
P3 (standard)	One user or transaction is blocked, or a minor function fails	One citizen's application is stuck	< 1 business day
P4 (low)	Cosmetic issue, how-to question or enhancement request	Typo in a Dzongkha label	2 business day

2. Support level: fault depth (GovTech) (*indicative*)

Level	Type of problem	Who fixes it	Typical work	Time to fix
L1	A known problem that needs no code or server changes	GovTech service desk	Account or role access, settings changes, resending a failed notification, following a written fix guide, correcting data in the admin screens	1 business day
L2	Something broken in the application or in a link between systems that needs investigating	GovTech / Vendor	Checking logs in OBVP, fixing failed API calls through NDE/WSO2, fixing a service linked to the wrong agency in the Public Service Registry (PSR), fixing database	3 business day

			records, finding a workaround	
L3	A bug or infrastructure problem that needs a proper change	Developers or the vendor, the infrastructure/GDC team, the security team	Fixing and releasing code, changing the database structure or Kubernetes setup, handling security incidents, working with outside parties such as banks and telcos	10 business day or next release

3. Process flows

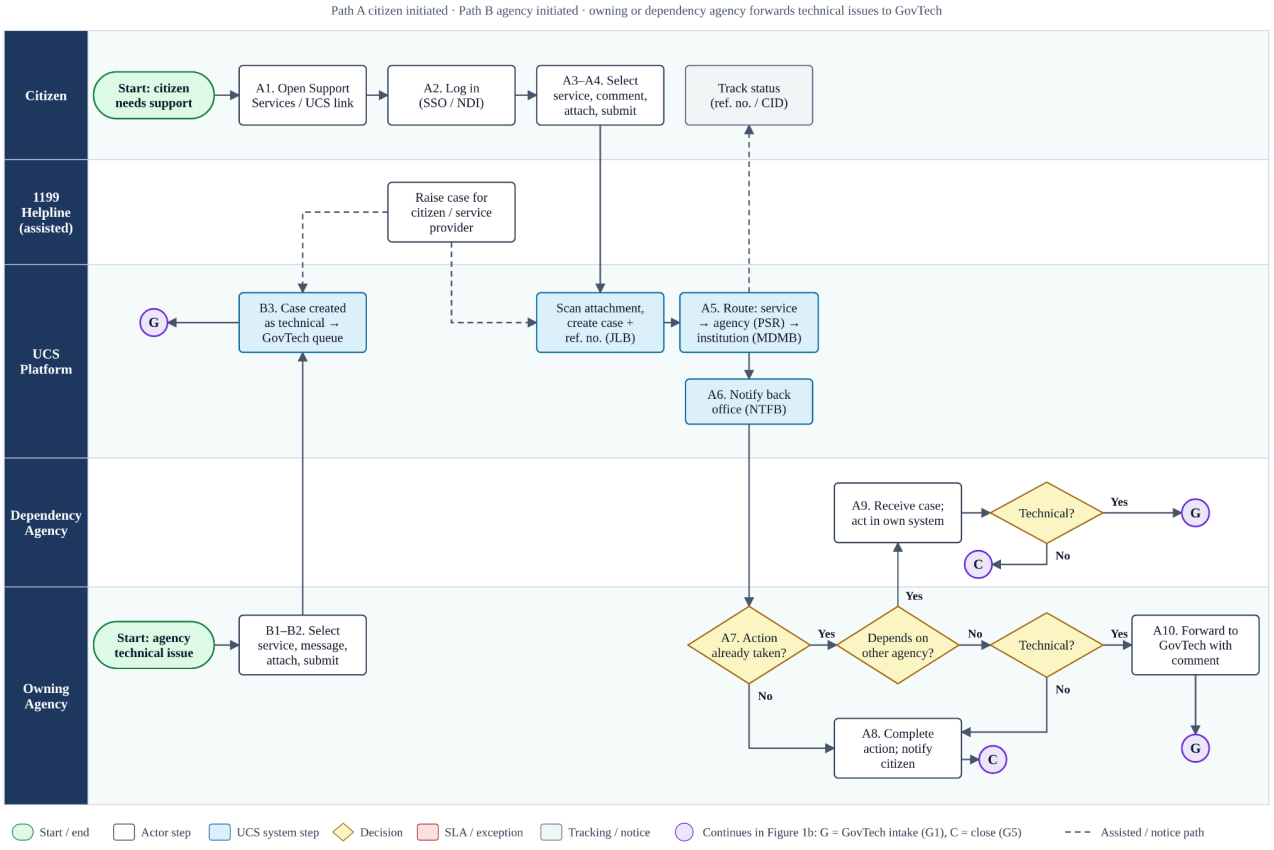


Figure 1a: Citizen Initiated, Agency handling

3.1 Path A, citizen initiated

#	Step	Blocks and interfaces
A1	The citizen opens the Support Services menu / UCS link	Menu rendered with UI/UX
A2	Login, and redirect to the support form	SSO authorisation code flow with PKCE, return address preserved so the citizen lands on the form
A3	The citizen selects a service from the drop-down	PSR service catalogue, returning service code and display name
A4	The citizen writes a comment, optionally attaches a file or image, and submits	Case created in UCS with reference number, service, comment, channel origin; attachment stored in DOCS after virus scanning
A5	The case is routed to the owning agency	Service code from owning agency in PSR, agency to canonical institution code from MDMB, case placed in that agency's queue;
A6	Back office staff are notified	NTFB on the agency's configured channel

#	Step	Blocks and interfaces
A7	Staff confirm whether the action has already been taken	Triage outcome recorded on the case with actor and timestamp
A8	If not taken, staff carry out the action and notify the citizen	Action completed in the agency line of business system; outcome recorded on the case; NTFB reply on the originating channel
A9	If the action needed to be done from another agency dependency system, forward to that agency	Get notified to that agency and action will be taken.
A10	If action is taken already from the agency and the problem is technical, staff forward it to GovTech	Case reclassified as technical, mandatory comment attached, record of action already taken carried forward, reassignment written to JLB
A11	If a citizen is stuck in the steps, citizens can avail the 1199 support service.	Get help from the 1199 to raise the case or to use support service.

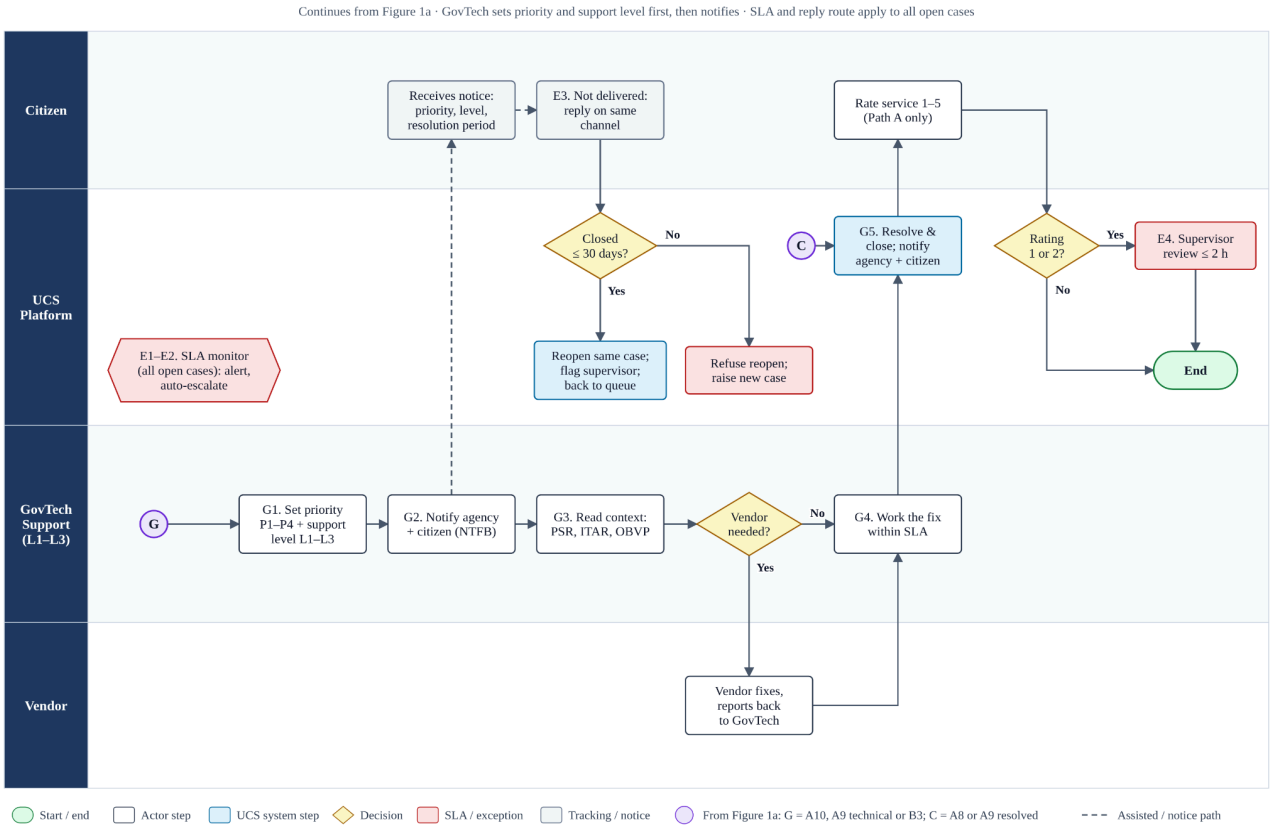


Figure 1b: Agency Initiated, GovTech Support, closure and SLA handling

3.2 Path B, agency initiated

#	Step	Blocks and interfaces
B1	Agency staff open the support form	Requester identity and institution code taken from the session token
B2	Staff select the service,optionally attaches a file or image, and write the message, and submits	PSR service catalogue; attachments stored in DOCS after virus scanning
B3	Staff submit the case to GovTech	Case created with case_origin set to agency, classified as technical at creation, routed to the GTA queue without agency triage, creation written to JLB
B4	If a Service Provider is stuck in the steps, Service Providers can avail the 1199 support service.	Get help from the 1199 to raise the case or to use support service.

3.3 Stage 3, GovTech support

#	Step	Blocks and interfaces
G1	GovTech opens the case and reads the context	PSR names the system behind the service, ITAR gives the service instance and its owner, OBVP shows whether it is degraded. Visible to support staff only
G2	GovTech assigns P1-P4 priority and L1, L2 or L3 support	Support level recorded on the case, resolution period drawn from the configured SLA for that level
G3	GovTech notifies the agency and, on path A, the citizen	One NTFB notice to each, carrying the reference number, the issue statement and the resolution period
G4	The fix is worked within the SLA	Progress recorded on the case thread; internal notes excluded from the citizen view
G5	The case is resolved and closed	Resolution recorded, agency and citizen notified, linked cases closed together, satisfaction rating requested from each citizen requester

3.4 SLA handling and the reply route

#	Condition	What happens
E1	30 minutes (should be configurable) before the response target expires	Pre-breach alert to the supervisor holding the queue
E2	The response target expires	The case auto-escalates to the supervisor queue, a breach event is written to JLB, the original agent keeps visibility
E3	The resolution period passes and the citizen has not received the service	The citizen replies on the originating channel. The reply appends to the existing thread, reopens the same case and flags it for supervisor review. No new reference number is issued
E4	The citizen returns a rating of 1 or 2 at closure	The case is flagged for supervisor quality review within 2 hours
E5	The case has been closed for more than 30 days (should be configurable)	Reopening is refused and the citizen is directed to raise a new case, with the original retained read only

4. Example User scenarios (indicative for UCS)

Four scenarios illustrate how citizens, businesses, agency staff and supervisors use the platform across contexts and channels. They demonstrate capability coverage without reference to process flow diagrams.

4.1 Scenario 1: Citizen-initiated technical problem

4.1.1 Context

Pema Dorji, a small business owner in Thimphu, has signed in and is renewing his business licence on the Government Portal. The transaction fails at the payment step and he cannot continue.

4.1.2 Interaction description

Pema opens the Support Services menu on the eService Portal, selects the service from the drop-down list, describes the problem he met while trying to complete it, attaches a screenshot of the error, and submits the form. eService Portal passes the service identifier and the failed transaction reference to UCS with the submission, so Pema does not retype them.

UCS creates a case with reference UCS-2026-03471, classifies it as a service issue against business licence renewal, and uses PSR to place it in the Business Licencing Support queue at the owning ministry. NTFB sends Pema a confirmation carrying the case reference and the four hour response target that applies to a P2 case.

A ministry agent opens the case, reads the service context UCS captured at submission, and finds the payment failed because the address on the business registry record no longer matches the address held against the payment instruction. The agent corrects the registry record, records the action on the case, and closes it two hours after it was raised. NTFB sends Pema a closure notice and a rating request. Pema rates the resolution 5 out of 5 and adds a comment. UCS holds the rating against the case and counts it in the owning ministry's support reporting.

4.2 Scenario 2: Agency-initiated technical problem

4.2.1 Context

Dechen Wangmo is a licensing officer at the Ministry of Economic Affairs. While issuing a trade licence on the Business Portal, the document generation step fails for every application she opens.

4.2.2 Interaction description

Dechen opens the support form, selects Trade Licence Issuance from the service list, writes what she has tried, and attaches two screenshots of the failure. She submits the case to GovTech.

UCS creates the case with the agency as requester, classifies it as technical at creation, and routes it to the GTA queue without agency triage. GovTech support opens the case and reads the asset context panel, which identifies the document generation service instance and its owner. Support assigns L2 and notifies the ministry with the issue statement and the resolution period for that level.

Six citizen cases raised the same morning against the same service are linked to it, so all seven close together when the fix is confirmed. UCS requests a satisfaction rating from the six citizens. The agency case closes without one.

4.3 Scenario 3: supervisor dashboard review

4.3.1 Context

Sonam Wangchuk is a Senior Support Supervisor at the Ministry of Finance. She oversees the Tax Filing Support queue through the annual corporate tax filing period.

4.3.2 Interaction description

Sonam opens the supervisor dashboard. It shows 24/7 open cases, an average response time of 1 hour 42 minutes, SLA compliance of 91.2 per cent against the tenant target, and a queue depth chart for Tax Filing Support. The dashboard shows Ministry of Finance queues only.

She notices a spike in cases carrying the keyword cluster "e-filing portal, attachment upload error", which the nightly pattern detection surfaced as a recurring issue accounting for 18 per cent of this week's case volume.

Sonam filters the open cases in that cluster, reassigns them as a batch to a senior agent who works on the e-filing portal, and records the reason for the move.

She raises one technical case to GovTech against the e-filing portal and links the cluster to it. Each requester keeps their own case reference while the underlying fault is worked once. She exports the cluster data for the ministry's technology operations meeting, and UCS records the export against her account.

Three cases breach SLA during the morning. UCS alerts Sonam 30 minutes before each expiry and auto-escalates the cases on breach. Sonam reviews them, adds a supervisory note, and reassigns them to the escalation queue.

5. Platform capabilities

5.1 Case management

- Case creation with a unique, opaque reference number that is neither sequential nor guessable.
- Case status lifecycle enforcement: New, Assigned, In Progress, Pending Customer, Escalated, Resolved, Closed, Cancelled. Ownership is carried by the assigned queue rather than by the status.
- Priority tier management (P1 Critical, P2 High, P3 Standard, P4 Low) driving queue order and the first response clock, applied independently of the L1 to L3 support level on technical cases.
- Separate response and resolution SLA timers per case, with configurable pause conditions, pre-breach alerts, and auto-escalation to the supervisor holding the queue on breach.
- File attachment management with virus scanning and a configurable size limit.
- Auto-close after a configurable confirmation period following resolution, with a satisfaction rating requested from the citizen at closure.
- Case origin recorded as citizen or agency, with the requester model and the rating rule following from it.

5.2 Multi-channel gateway

- Inbound normalisation from portal widget, email, and SMS
- Unified canonical case payload construction from all channel formats.
- Bidirectional communication on every digital channel.
- Channel-specific metadata preservation: origin URL, device type, session token.
- Out-of-hours queue management with next-business-day routing.
- Inbound message queuing during maintenance with zero message loss.

5.3 Agent workbench

- Real-time queue view with priority, age, SLA status and service category.
- Complete support history for an authenticated requester, linked by the identifier on the session token.
- Communication thread management with internal notes visible to agents and supervisors only.
- File attachment handling within the case thread.
- Portal session context display: page URL, transaction step, error code.
- Service and asset context on technical cases: the service from PSR, the running instance and GovStack usage from ITAR, and the current degradation signal from OBVP.

5.4 Triage and escalation

- Pre-breach alert to the supervisor 30 minutes before the response target expires.
- Auto-escalation to the supervisor queue on breach.
- Agency triage outcome recording: whether the requested action had already been taken, and whether the citizen remains blocked by a technical failure.
- Reclassification to technical and forwarding to the GTA queue with a mandatory comment.
- Support level assignment of L1, L2 or L3 on every technical case, with the resolution period notified to the agency and, on citizen cases, to the citizen.
- Low rating flagging for supervisor quality review within 2 hours.
- A GTA-owned queue for cases about the login and the platform itself, where no service-owning ministry applies.

5.5 Administration and configuration

- Multi-tenant institutional tenant creation, configuration and lifecycle management.
- Agent role definition, queue assignment and escalation hierarchy configuration.
- SLA rule configuration per priority tier and per support level, per institutional tenant.
- Working hours and out-of-hours routing configuration per queue.
- Channel enablement and routing rule setup with sandbox testing.
- Knowledge base administration with an Author, Review, Approve, Publish, Retire lifecycle.
- Dashboard and KPI widget configuration with PDF and CSV export and scheduled delivery.

5.6 Analytics and monitoring

Operational reporting over the platform's own case data stays within the platform, because a case management system reporting on itself needs no external dependency. Cross-institutional reporting is national business intelligence and is served by the shared analytics platform.

- Real-time operational dashboards for all primary support KPIs with a 60 second refresh, computed from UCS case data.
- Automated daily, weekly and monthly performance reports per institution, delivered via NTFB.
- Satisfaction score aggregation by service category, institution, channel, agent and period.
- Per-service reporting for each tenant for GovTech support.

5.7 Security and compliance

- Identity resolution for all authenticated sessions through the SSO-issued token, with NDI as the identity authority behind SSO.
- OIDC and RS256 JWT session security with PKCE-secured token refresh.
- Role-based access control enforced at the API gateway and at the application service layer, with role claims taken from the session token.
- Data masking and k-anonymity anonymisation for cross-institutional analytics.
- TLS 1.3 in transit and AES-256 at rest for all persistent data.
- Immutable audit trail via JLB with hash chaining and tamper detection.
- Column-level PII encryption in addition to tablespace-level encryption.
- Tenant data boundaries enforced at storage and API level, with any cross-tenant access attempt refused and logged.

5.8 Citizen experience and accessibility

- Omnichannel access continuity across portal, email and phone without context loss.
- Contextual in-transaction help surfaced at the point of service friction.
- Bilingual interface in Dzongkha, rendered in the DDC Uchen font, and English.
- Real-time case status visibility on Portal and the public portal without a separate login.
- Post-case satisfaction collection via NTFB within 2 hours of closure.
- WCAG 2.1 Level AA compliance

6. Functional requirements

Requirements are classified using MoSCoW priority notation: MUST is mandatory for go-live, SHOULD is strongly recommended, MAY is an optional enhancement. All acceptance criteria are stated as verifiable conditions. Identifiers carry the UCS module prefix; the number after the prefix is unchanged from the source BRD.

6.1 For Unified Client Support (UCS)

6.1.1 UCS-FR-1: case management

ID	Requirement	Priority	Acceptance criteria
UCS-FR-1.1	The platform creates a case for every inbound support request on every channel and assigns it a	MUST	The platform creates the case within 500 ms. The reference number is unique, non-sequential and not guessable. Every mandatory field

ID	Requirement	Priority	Acceptance criteria
	unique reference number. The reference number format is UCS-YYYY-NNNNN and the format is configurable.		carries a value. The API returns HTTP 201 on success.
UCS-FR-1.2	The platform enforces the case status lifecycle across eight statuses: New, Assigned, In Progress, Pending Customer, Escalated, Resolved, Closed and Cancelled.	MUST	The platform rejects an invalid transition with HTTP 422. It writes every status change to JLB with the actor, the timestamp and the reason. The assigned queue carries ownership of the case; the status does not.
UCS-FR-1.3	Support four priority tiers, P1 Critical, P2 High, P3 Standard and P4 Low, with a configurable response target per tier per institutional tenant.	MUST	The platform applies a priority at creation and starts the response timer immediately. On expiry it generates a breach event and publishes it to EVTB. The priority tier is distinct from the support level, and the case displays both.
UCS-FR-1.4	The platform maintains an immutable communication thread on every case holding requester messages, agent replies and system events in chronological order.	MUST	The agent and the requester both see the thread. The requester view excludes internal notes. The thread is append-only. Every entry carries a timestamp to millisecond precision.
UCS-FR-1.5	The platform merges duplicate submissions of the same request into a primary case and keeps every message thread from the merged cases. Linking distinct cases that share one fault is covered by UCS-FR-1.10.	SHOULD	The platform links the merged reference to the primary case. Every message from the merged cases appears on the primary thread. The platform notifies each submitter of the merge through NTFB.
UCS-FR-1.6	The platform allows a requester on any intake route to attach files and images. It scans every	MUST	The platform stores the attachment in DOCS and references it from the case. The scan completes before the agent can see the attachment. The

ID	Requirement	Priority	Acceptance criteria
	attachment for viruses before the attachment becomes available and enforces a configurable maximum size.		attachment record carries a clean or infected status. The size limit is configurable per tenant with a default of 10 MB per file. The permitted MIME types (file formats) are configurable.
UCS-FR-1.7	The platform requests a satisfaction rating through NTFB within 2 hours (it should be configurable) of closure on every citizen-raised case, however that closure was reached.	MUST	The platform dispatches the notification within 2 hours of closure. The rating form is reachable from the notification. The rating token is single use and expires after 7 days. The platform requests no rating on an agency-raised case and excludes those cases from the satisfaction KPI.
UCS-FR-1.8	The platform reopens a closed case on the reply route in section 3.4 E3 while the case has been closed for 30 days or less, keeping the original reference number. After 30 days it refuses to reopen and directs the requester to raise a new case.	SHOULD	A reopen inside the window moves the case from Closed to Assigned, routes it to the supervisor queue of the owning tenant, keeps the reference number and increments a reopen counter. The platform writes the reopen to JLB with the actor and the reason code. A reopen attempt after 30 days returns HTTP 409 with a route to raise a new case, and the original case stays read only.
UCS-FR-1.9	The platform records the case origin as citizen or agency, and holds the requester as the authenticated identity from the session token, or the agency staff identity with its institution code.	MUST	case_origin set at creation and immutable thereafter; requester type determines whether a rating is requested at closure per UCS-FR-1.9; agency-raised cases carry institution_code and no CID; reporting distinguishes the two origins per UCS-FR-8.7.
UCS-FR-1.10	The platform allows agency staff to create a case on the Portal reporting a technical problem in a service their agency owns. The submission carries a	MUST	The platform creates the case with case_origin set to agency and takes the requester identity and institution_code from the session token. It resolves the service identifier through PSR, classifies the case as technical at creation and

ID	Requirement	Priority	Acceptance criteria
	service selection, a text message, and file and image attachments, and goes directly to the GTA queue.		routes it to the GTA queue without agency triage. Attachments follow UCS-FR-1.6. The platform records no CID and writes the creation to JLB.
UCS-FR-1.11	The platform allows an authenticated citizen to look up their own cases on the Portal by reference number, and to list every case held against their CID.	MUST	The platform scopes the lookup to the authenticated session. A reference number belonging to another citizen returns not found rather than a permission error. The platform never accepts a CID as a search input from an unauthenticated session. The view shows the status, the service, the support level where one is assigned, the stated resolution period, and the thread excluding internal notes.
UCS-FR-1.12	The platform closes a resolved case automatically after a configurable confirmation period, during which the requester may reject the resolution.	MUST	The confirmation period is configurable per tenant with a default of 5 business days. A rejection inside the period returns the case to In Progress on the same reference number. The platform writes the auto-closure to JLB. Closure triggers the rating request under UCS-FR-1.8.

6.1.2 UCS-FR-2: multichannel gateway

ID	Requirement	Priority	Acceptance criteria
UCS-FR-2.1	The platform accepts an inbound case payload from every channel configured as supported and normalises it into the canonical UCS case schema. It sets channel_origin from the channel the request arrived on.	MUST	A payload from each supported channel, meaning the CSP, CP and BP widgets, email, phone and WhatsApp, validates against the canonical case schema. The platform sets channel_origin at creation and the field is immutable afterwards. A payload that fails validation creates no case and follows UCS-FR-2.6. A channel that is not configured as supported creates no case.

ID	Requirement	Priority	Acceptance criteria
UCS-FR-2.2	Support bidirectional communication with authenticated requesters on every digital channel.	MUST	The platform dispatches agent replies and system notifications through NTFB on the channel that created the case. Every outbound message carries the case reference number. A requester reply on that channel appends to the existing thread under UCS-FR-1.4 and keeps the reference number.
UCS-FR-2.3	The platform queues inbound channel messages while it cannot process them, whether the interruption is planned or not, and processes the queue on restoration.	MUST	Zero message loss during planned windows; queue processed in order on restoration; delayed delivery noted in the thread timestamp.
UCS-FR-2.4	Reject and quarantine inbound payloads that fail schema validation, returning a structured error to the sending system.	MUST	Malformed payloads stored in a quarantine table; sender receives HTTP 400 with validation detail; quarantine reviewed by an administrator daily.

6.1.3 UCS-FR-3: agent workbench (Business Portal)

ID	Requirement	Priority	Acceptance criteria
UCS-FR-3.1	Display a real-time queue view of assigned cases with priority, age, SLA status, service category and requester reference.	MUST	View refreshes within 10 seconds; sortable and filterable on every displayed attribute; new arrivals indicated without a page reload.
UCS-FR-3.2	Display the complete support history for an authenticated requester on the case detail view.	MUST	History loaded within 2 seconds of opening the case; includes prior cases, channels, ratings and resolution summaries; anonymous sessions show no history.
UCS-FR-3.3	Support internal notes visible to agents and supervisors only.	MUST	Internal flag set at creation; notes excluded from the requester-facing thread; included in the JLB record with an is_internal flag.
UCS-FR-3.4	Allow agents to adjust classification, priority and	MUST	Overrides require a mandatory reason; change recorded in the

ID	Requirement	Priority	Acceptance criteria
	queue assignment, with every change recorded in the audit trail.		thread and in JLB with actor, timestamp, original value and new value.
UCS-FR-3.5	Display the requester's portal transaction context, that is page URL, transaction step and error code, where the case originated from an embedded widget.	SHOULD	Context metadata shown in the case metadata panel; URL opens the originating page in a new tab.
UCS-FR-3.6	Display a service and asset context panel on technical cases, naming the system behind the service, its running instance and owner, and its current degradation state.	MUST	Service resolved from PSR, instance and owner from ITAR, degradation signal from OBVP; panel visible to GovTech support and agency supervisors only, never to the citizen; absence of an ITAR or OBVP record shows as unknown rather than blocking the case.

6.1.4 UCS-FR-4: escalation and triage

ID	Requirement	Priority	Acceptance criteria
UCS-FR-4.1	classify every incoming case by service category, urgency and queue.	MUST	Classification should be done with the service category, urgency and queue
UCS-FR-4.2	Trigger a pre-breach alert to the supervisor 30 minutes before the response target expires.	MUST	Alert dispatched via NTFB to the supervisor role; content includes reference, priority, elapsed time and expiry timestamp.
UCS-FR-4.3	Auto-escalate cases to the supervisor queue on SLA breach.	MUST	Escalation triggered at expiry; supervisor notified via NTFB; breach event written to JLB with all mandatory audit fields; the original agent retains visibility.
UCS-FR-4.4	Flag low satisfaction responses of 1 or 2 for supervisor quality review	MUST	Flag triggers an NTFB notification to the supervisor; flagged case visible in the quality review queue;
UCS-FR-4.5	Provide fallback routing where the owning agency cannot be resolved, and a	MUST	A case whose service cannot be resolved through PSR routes to the GTA default queue rather than failing;

ID	Requirement	Priority	Acceptance criteria
	GTA-owned queue for cases raised about the login, the portals or the platform itself.		cases originating from an authentication failure route to the GTA support queue; fallback routing decisions logged with the reason; the queue is configurable like any other tenant queue.
UCS-FR-4.6	Record the agency triage outcome on every citizen-raised case: whether the requested action had already been taken, and where it had, whether the citizen remains blocked by a technical failure. Allow the agency to reclassify the case as technical and forward it to the GTA queue with a mandatory comment.	MUST	Triage outcome recorded as a case attribute with actor and timestamp; forwarding requires a non-empty comment; the record of the action already taken is carried on the case; reassignment written to JLB per UCS-FR-1.5; the case retains its original reference number; the owning agency retains read access after forwarding.
UCS-FR-4.7	Assign a support level of L1, L2 or L3 to every technical case, and notify the owning agency and, on citizen-raised cases, the citizen, stating the issue and the resolution period for that level.	MUST	Support level recorded on the case; the resolution period drawn from the configured SLA for that level per UCS-FR-7.3; one NTFB notification to the agency and one to the citizen, each carrying the reference number, the issue statement and the resolution period; level changes logged to JLB with a mandatory reason; support level is distinct from the P1 to P4 priority tier in UCS-FR-1.3 and both are displayed on the case.
UCS-FR-4.8	Allow a citizen whose case has not been resolved within the stated period to reply on the originating channel, reopening the same case for supervisor attention rather than creating a new one.	MUST	Reply appended to the existing thread per UCS-FR-2.2; the case is flagged for supervisor review and appears in the quality review queue; no new reference number issued; reply recorded in JLB; the breach escalation in UCS-FR-5.3 fires on its own timer and does not depend on a citizen reply.

6.1.5 UCS-FR-5: administration and configuration

ID	Requirement	Priority	Acceptance criteria
UCS-FR-5.1	Provide a multi-tenant administration console for creating and managing institutional tenants.	MUST	The GTA administrator can create, edit, suspend and deactivate tenants; the data boundary is enforced at storage and API level; all changes logged to JLB.
UCS-FR-5.2	Allow configuration of agent roles, queue assignments and escalation hierarchies per tenant.	MUST	Role assignment interface available; changes take immediate effect; configuration history with actor identity logged to JLB.
UCS-FR-5.3	Support configurable SLA rules per priority tier and per support level, per institutional tenant.	MUST	Response targets configurable per priority tier; resolution targets configurable per support level L1, L2 and L3; both sets configurable per tenant; changes reflected in active case timers within 1 hour; timers on pre-existing cases grandfathered.
UCS-FR-5.4	Provide channel enablement controls and routing rule configuration per tenant, with sandbox testing before activation.	MUST	Channels enabled or disabled without service interruption; routing rule changes testable in a sandbox; activation logged to JLB.
UCS-FR-5.5	Expose operational and performance dashboards to supervisor and administrator roles with configurable KPI widgets.	MUST	Dashboards render within 3 seconds; data no more than 60 seconds stale; filterable by institution, service, channel, agent and date range; exportable to PDF and CSV; every export logged against the requesting account and scoped to the requester's tenant.
UCS-FR-5.6	Provide a knowledge base administration interface with an approval workflow and full version history.	MUST	Author, reviewer and approver roles are enforced; articles cannot be published without approval; full version history retained; retired articles suppressed from the citizen view.
UCS-FR-5.7	Configure working hours, holidays and out-of-hours routing per queue.	MUST	Working hours and holiday calendar set per queue; SLA timers pause outside working hours where the tenant has configured them to;

ID	Requirement	Priority	Acceptance criteria
			out-of-hours submissions accepted and routed to the next business day with the requester told so in the acknowledgement; changes logged to JLB.

6.1.6 UCS-FR-6: analytics and reporting

ID	Requirement	Priority	Acceptance criteria
UCS-FR-6.1	Provide real-time operational dashboards displaying the primary UCS KPIs, updated within 60 seconds.	MUST	Dashboards render within 3 seconds; every KPI in section 1.4 displayed; filterable by institution, service, channel, agent and date range.
UCS-FR-6.2	Generate automated daily, weekly and monthly performance reports per institution, delivered via NTFB.	MUST	Reports scheduled from the admin console; delivered in PDF and CSV; delivery failure alerted to the institution administrator.
UCS-FR-6.3	Track and display recurring issue patterns and top-searched keywords, updated nightly.	SHOULD	Nightly analysis; results on the supervisor dashboard within 6 hours of completion; exportable to CSV.
UCS-FR-6.4	Aggregate satisfaction scores by service category, institution, channel, agent and period.	MUST	Scores shown on dashboards; time series trend available; drill-down to the individual case score; low scores flagged automatically per UCS-FR-5.5.
UCS-FR-6.5	Provide a programme-level view aggregating KPIs across all institutional tenants for GTA leadership.	MUST	Restricted to the GTA administrator role; aggregated without individual personal data; all tenants included; refreshed on the same schedule as institutional dashboards.
UCS-FR-6.6	Provide each institutional tenant with a report of the cases raised against the services it owns, over a selectable period, broken down by service.	MUST	Per service: case volume, counts by status, average first response time, SLA compliance rate and average satisfaction. Period selectable; exportable to PDF and CSV per UCS-FR-7.5; a tenant cannot select or view another tenant's services or

ID	Requirement	Priority	Acceptance criteria
			cases, and any attempt returns no data and is logged to JLB.
UCS-FR-6.7	Provide GovTech support with a report of the technical cases referred to it across all tenants, over a selectable period, broken down by service, owning agency and support level.	MUST	Counts resolved, in progress and pending per support level; average response time and SLA compliance rate per support level; citizen-raised and agency-raised cases distinguished; exportable to PDF and CSV.
UCS-FR-6.8	Show the owning agency the current status, support level and stated resolution period of the technical cases it has referred to GovTech.	SHOULD	Visible on the BP; limited to cases the agency referred to or that concern services it owns; GovTech internal notes are not disclosed.

Status vocabulary for the reports, mapped to the lifecycle in UCS-FR-1.2: under process means In Progress or Escalated; pending means Pending Customer; resolved means Resolved or Closed. Without this mapping the agency report and the GovTech report will count the same case differently.

6.1.7 UCS-FR-7: accessibility and localisation

ID	Requirement	Priority	Acceptance criteria
UCS-FR-7.1	All user-facing interfaces comply with WCAG 2.1 Level AA.	MUST	Accessibility audit report produced before go-live; zero Level A or AA violations; tested with NVDA and JAWS;
UCS-FR-7.2	Support Dzongkha and English throughout all user-facing and agent-facing interfaces.	MUST	All UI elements available in both languages; language switching in one user action without a page reload.
UCS-FR-7.3	Support mobile-responsive interfaces at a minimum viewport width of 320 px.	MUST	All citizen-facing interfaces are functional at 320 px; touch targets at least 44 by 44 px; no horizontal scrolling at 320 px; tested on Android and iOS.
UCS-FR-7.4	Render Dzongkha text in the DDC Uchen font with full Tibetan script character support.	MUST	Font loaded for all Dzongkha content; no character substitution or rendering artefact; verified on Chrome, Firefox and Safari.

8. Logical component architecture

8.1 Subsystem components (indicative)

Component	Responsibility	Primary technology
Case Management Service	Case CRUD, status lifecycle state machine, SLA timer management, routing rule evaluation, queue management. Exposes the primary UCS REST API.	Node.js or Java (Spring Boot); PostgreSQL; Redis
Multichannel Gateway	Channel adapter normalisation for portal widget, email, WhatsApp and phone CTI. Constructs the canonical case payload from every inbound format.	Node.js; REST channel adapters; Kafka consumer
Agent Workbench UI	Agent-facing application: queue view, case detail, communication thread, internal notes, article sidebar, escalation controls, SLA indicators, service and asset context panel.	React or Angular; UDS components exclusively
Self-Service Layer	FAQB search proxy, article suggestion, guided walkthrough controller, auto-reply dispatcher, anonymous query handler.	Node.js; Elasticsearch; FAQB API client
Triage and Routing Service	Calls AIPP for classification, urgency scoring and queue recommendation; applies static fallback rules below the confidence threshold; records overrides for model feedback.	Node.js; AIPP API client
Notification Dispatcher	NTFB client managing outbound notification: template selection, variable substitution, delivery status tracking, retry on failure.	Node.js; NTFB REST client
Event Streaming Service	Publishes UCS domain events to EVTB. Consumes FAQB update and portal session context events. Manages the local fallback queue.	Kafka producer and consumer; CloudEvents SDK
Analytics Engine	Aggregates KPI data from case and interaction records, serves the dashboard API, schedules report generation, runs nightly pattern detection, publishes anonymised aggregates to the shared analytics platform.	Elasticsearch; Kibana; Python batch scheduler
Administration Console	Tenant, agent, queue, SLA, working hours, channel and knowledge base configuration. Hosts supervisor dashboards.	React; UDS components exclusively

Component	Responsibility	Primary technology
Widget SDK	Lightweight JavaScript library embedded in the portals. Manages widget lifecycle, session context capture, article display and form rendering without a page reload.	Vanilla JavaScript; UDS design tokens
API Gateway	Rate limiting, JWT enforcement, API versioning, request routing and usage analytics for all external and inter-component traffic.	WSO2 via NDE
JLB Audit Publisher	Dedicated Kafka producer for audit events. Maintains a local append-only buffer. Guarantees at-least-once delivery with deduplication on JLB recovery.	Kafka producer; PostgreSQL append-only log

8.2 Technology stack (indicative)

Layer	Technology
API protocols	REST (OpenAPI 3.0); WebSocket (RFC 6455) for real-time workbench updates; Kafka with CloudEvents v1.0 for event streaming
Security	TLS 1.3; OIDC; OAuth 2.0 with PKCE; RS256 JWT; AES-256 at rest; mTLS between services; API gateway enforcement at NDE
Databases	PostgreSQL for cases, messages, profiles and knowledge content; Redis for session and FAQ cache with TTL; Elasticsearch for full-text search and analytics indices
Event streaming	Apache Kafka via EVTB; CloudEvents v1.0; acks=all; idempotent delivery
Classification	No model is trained, hosted or served inside UCS
Frontend	React or Angular for workbench and console; vanilla JavaScript for the Widget SDK; UDS components throughout; DDC Uchen for Dzongkha
Container platform	Kubernetes on the government cloud; independent horizontal pod autoscaling per microservice; blue-green deployment; GitOps release pipeline
Observability	Prometheus and Grafana for metrics; Elasticsearch and Kibana for logs; Jaeger for distributed tracing by correlation ID; GTA SIEM integration

8.3 Dependency register (Indicative)

Strength is rated 1 for an optional enhancement to 3 for a hard dependency, where core UCS functions fail without it. Behaviour under outage reflects the circuit breaker and degraded-mode requirement in UCS-FR-6.9.

Code	Building block	Direction	Integration mechanism	Purpose and behaviour if unavailable
Government Portal	Government Portal	Inbound	NDE	Support Services menu, public self-service and anonymous submission. If unavailable: the public widget is gone; the authenticated CP channel is unaffected.
NDI/SSO	National Digital Identity	Outbound	NDE	The authority behind citizen credentials. UCS makes no call to NDI. If unavailable: the effect on UCS is whatever SSO does in response, and UCS has no failure path of its own.
PSR	Public Service Registry	Outbound	NDE	Populates the service drop-down and resolves the owning agency. If unavailable: the last cached catalogue serves the drop-down and unresolved cases route to the GTA default queue per UCS-FR-5.6.
MDMB	Master Data Management	Outbound	NDE	Canonical institution code held on the case and the queue. If unavailable: the cached code is used and new tenant onboarding is deferred.
NTFB	Notification Block	Outbound	NDE	Every user-facing notification and rating request. If unavailable: notifications queue locally with retry; in-portal status remains accurate.
JLB	Journaling Block	Outbound	NDE	Immutable audit trail. If unavailable: events buffer in the local fallback queue and replay on recovery, with zero loss by design.
DOCS	Document Store	Outbound	NDE	Storage for case attachments. If unavailable: submission with an attachment is refused with a clear message; text-only submission continues.

Code	Building block	Direction	Integration mechanism	Purpose and behaviour if unavailable
ITAR	IT Asset Repository	Outbound	NDE	Identifies the running instance behind a failing service and its owner. If unavailable: the asset panel shows unknown and the case proceeds.
OBVP	Observability Platform	Outbound	NDE	Shows whether the affected service is currently degraded. If unavailable: the signal shows unknown and the case proceeds.
NDE	National Data Exchange and API gateway	Outbound	NDE	Authentication enforcement, rate limiting and versioning. If unavailable: external API access stops; this is a platform-level outage.

Each row must be reciprocated in the partner block's own dependency register before sign-off. Asymmetric declarations are a sign-off blocker.

9. Data, security and compliance

9.1 for Unified Client Support (UCS)

9.1.1 Data model (Indicative)

All entities are stored in PostgreSQL unless stated otherwise. Fields holding personal data are encrypted at column level with AES-256 in addition to tablespace-level encryption.

Entity	Storage	Key attributes
Case	PostgreSQL	case_id (UUID PK), reference_number (UCS-YYYY-NNNNN), status, priority, support_level (nullable), case_origin (citizen or agency), service_code, institution_code, channel_origin, cid (nullable), requester_email (nullable), requester_staff_id (nullable), assigned_agent_id, queue_id, parent_case_id (nullable), response_due_at, resolution_due_at, triage_outcome, created_at, updated_at, resolved_at, closed_at, csat_score (nullable)
Case Message	PostgreSQL	message_id (UUID PK), case_id (FK), sender_type (citizen, agent, system), sender_id, content (encrypted), attachment_ids[], is_internal, sent_at
Case Attachment	PostgreSQL and DOCS	attachment_id (UUID PK), case_id (FK), filename, mime_type, size_bytes, storage_key (encrypted), virus_scan_status, uploaded_at, uploaded_by
Support History	PostgreSQL	history_id (UUID PK), subject_identifier (indexed), case_ids[], first_contact_at, last_contact_at, total_cases, avg_csat, preferred_channel
Knowledge Article	PostgreSQL and Elasticsearch	article_id (UUID PK), title (multilingual), content (multilingual, encrypted), status, version_number, institution_code, service_refs[], tags[], author_id, published_at, retired_at, usage_count
Satisfaction Response	PostgreSQL	Csat _id (UUID PK), case_id (FK), rating (1 to 5), comment (nullable, encrypted), submitted_at, channel
Agent Profile	PostgreSQL	agent_id (UUID PK), name, institution_code, role, queue_ids[], language_preference, is_active, created_at, last_login_at. Role assignments are a read-only projection of the claims on the session token
Queue	PostgreSQL	queue_id (UUID PK), name, institution_code, service_categories[], sla_config (JSON per priority tier and per support level), agent_ids[], routing_rules (JSON),

Entity	Storage	Key attributes
		channels_enabled[], working_hours (JSON), holiday_calendar (JSON), after_hours_template_id
Routing Rule	PostgreSQL	rule_id (UUID PK), tenant_id (FK), priority_order, match_conditions (JSON), target_queue_id, is_active, created_at, modified_at
Audit Log	PostgreSQL append-only and JLB	log_id (UUID PK), timestamp (ISO 8601 UTC), event_type, actor_id, actor_role, case_id (nullable), action, result, ip_address, user_agent, session_id, hash_of_previous_entry
Session Cache	Redis, TTL managed	session_id (key), subject_identifier, agent_id, channel, context_metadata (JSON), created_at

9.2 Data retention (indicative)

Data category	Hot retention	Archive retention	Notes
Active case data	Until closed plus 90 days	3 years from closure	PostgreSQL hot store, then cold object storage
Closed case data and messages	90 days after closure	7 years from closure	Encrypted object store with WORM on archival; retrievable within 4 hours
Chat transcripts and session logs	90 days	3 years	AES-256 throughout
Audit logs, support and case events	1 year hot	7 years minimum	JLB managed, WORM, 4 hour retrieval for authorised auditors
Audit logs, security events	1 year hot	10 years minimum	JLB WORM with encrypted archival; decryption restricted to the GTA security team
Satisfaction responses	3 years hot	5 years total	Pseudonymised after 3 years; individual comments redacted at pseudonymisation
Analytics aggregates	3 months hot	3 years anonymised	Warm and cold tiering; personal data removed at aggregation and not restorable
Knowledge articles, published	Indefinite while active	7 years after retirement	Full version history retained; retired articles hidden from the citizen view
Session cache	Per token lifetime	Not archived	Auto-expired by Redis; no persistent backup

9.3 Security controls

9.3.1 Encryption

- TLS 1.3 minimum on all inbound, outbound and internal service-to-service communication. TLS 1.2 and below are disabled on every UCS endpoint.
- AES-256 for all data at rest: PostgreSQL tablespaces, Redis persistence files, Elasticsearch indices, object store attachments, and Kafka partitions carrying personal data.
- A dedicated AES-256 key for audit log storage, rotated every 90 days through the GTA key management service. Decryption is restricted to authorised auditors and every decryption is logged.
- Column-level encryption on high-sensitivity fields (identifier, phone, email, address, message content) in addition to tablespace encryption.

9.3.2 Access control

- Role-based access control enforced at the NDE API gateway and at the application service layer. Role claims on the session token are authoritative; UCS maintains no independent role authority.
- Least privilege throughout: citizens see only their own cases; agents see only their assigned queue; supervisors see all data within their institution; GTA administrators reach all tenants for programme analytics only. Cross-institutional access requires written justification and is fully audited.
- Privileged administrative actions, that is tenant creation, role assignment, SLA modification and bulk data operations, require two-factor confirmation in the administration console.
- A tenant that requests another tenant's data receives an empty result rather than a permission error, and the attempt is written to JLB.

9.3.3 API security

- Every endpoint is protected by JWT validation at the gateway. Unauthenticated requests are rejected with HTTP 401 before reaching any service.
- Rate limiting per API consumer with configurable thresholds per endpoint tier. Breaches raise an automated alert to the GTA SIEM.
- Service-to-service communication uses mTLS with short-lived certificates rotated every 24 hours.
- All inputs are validated against strict OpenAPI 3.0 schemas. Inputs exceeding field limits or carrying injection patterns are rejected with HTTP 400 and logged to JLB.

9.3.4 Incident response

- Security incidents are classified P1 for a confirmed breach or active compromise, P2 for detected attempted unauthorised access, P3 for a policy violation or anomalous access pattern, and P4 for a minor anomaly requiring review.
- P1 incidents raise an immediate automated alert to the GTA security team and the DPI programme director. Breach notification to the relevant regulatory authority is completed within 72 hours of confirmation.

- All incidents are documented in the GTA incident management system. Root cause analysis and remediation are tracked to formal closure, with the post-incident review completed within 10 working days of P1 resolution.

10. Appendices

10.1 Glossary

Term	Definition
AIPP	AI Processing Platform. Provides classification, urgency scoring and routing recommendation to UCS by API.
CID	Citizen Identity Document number. National unique identifier for citizens.
CTI	Computer Telephony Integration. Lets inbound calls create and update cases.
DAP	The shared analytics platform serving national business intelligence.
DOCS	Document Store. Holds case attachments.
EVTB	Event Bus. Kafka-based asynchronous event streaming block.
GEA-F	Government Enterprise Architecture Framework v3.0.
GTA	GovTech Agency. Lead institution for digital transformation, and the operator of L1 to L3 support.
ITAR	IT Asset Repository.
JLB	Journaling Block. Immutable, tamper-evident audit log.
L1, L2, L3	Support levels expressing the depth of a technical fault, set by GovTech and driving the resolution target.
MDMB	Master Data Management Block. Source of the canonical institution code.
NDE	National Data Exchange. Hosts the WSO2 API gateway fronting UCS.
NDI	National Digital Identity. The identity authority behind SSO.
NTFB	Notification Block. Carries every outbound user-facing message.
OBVP	Observability Platform. Supplies the current degradation signal for a service.
P1 to P4	Priority tiers expressing urgency, driving queue order and the response target.
PSR	Public Service Registry. Source of the service catalogue and the service-to-agency mapping.
SLA	Service level agreement. In UCS, a response target set by priority tier and a resolution target set by support level.
SOP	Service Orchestration Platform.

Term	Definition
SSO	Single Sign-On. Issues the session token UCS validates.
UCS	Unified Client Support. The block defined in this document.
UDS	Unified Design System. Component library used exclusively for all UCS interfaces.
WCAG	Web Content Accessibility Guidelines v2.1 Level AA.
WFE	Workflow Engine.
WORM	Write Once Read Many. Storage property required for audit archival.