

Single Sign-On (SSO)

Business Requirements Document

Version: 4.0
Date: September, 2026
Status: Final Review

Document Control

Version	Date	Author	Changes
4.0	September, 2026	Cross-Functional Team	Final Review

Table of Contents

1. Overview.....4
1.1 Purpose and Scope.....4
1.1.1 Purpose.....4
1.1.2 In Scope.....6
1.1.3 Out of Scope.....8
1.2 Users.....9
1.3 Business Value.....10
1.3.1 For Citizens.....10
1.3.2 For Government Agencies.....10
2. Single Sign-On Building Blocks Overview.....11
2.1 SSO Overview.....11
2.1.1 Digital Government Ecosystem.....11
2.2 SSO Roles and Responsibilities.....12
2.3 Integration with Building Blocks.....14
3. Usage Scenarios.....15
4. SSO Capabilities & Requirements.....15
4.1 Functional Requirements.....15
4.1.1 FR-1: Single Sign-On Core Requirements.....15
4.1.2 FR-2: User Type Management Requirements.....17
4.1.3 FR-3: Authentication Methods Requirements.....18
4.1.4 FR-4: Single Logout (SLO) Requirements.....19
4.1.5 FR-5: SSO Protocol Support Requirements.....20
4.1.6 FR-6: SSO Session Management Requirements.....21
4.1.7 FR-7: Token Management for SSO Requirements.....22
4.1.8 FR-8: Service Provider Integration Requirements.....23
4.1.9 FR-9: SSO User Experience Requirements.....25
4.1.10 FR-10: SSO Security Requirements.....27
4.1.11 FR-11:Fallback Registration and Authentication Requirements.....30
4.2 Non-Functional Requirements.....33
4.2.1 NFR-1: Performance Requirements.....33
4.2.2 NFR-2: Availability and Reliability Requirements.....33
4.2.3 NFR-3: Scalability Requirements.....34
4.2.4 NFR-4: Security and Compliance Requirements.....34
4.2.5 NFR-5: Usability Requirements.....34
6. Data, Security and Compliance (Indicative).....35
6.1 Data Model (Indicative).....35
6.1.1 User Data (E.g. PostgreSQL).....35

6.1.2 Multi-Factor Authentication Data (E.g. PostgreSQL)..... 36
6.1.3 Session Data (E.g. Redis).....36
6.1.4 Token Metadata (E.g. PostgreSQL)..... 37
6.1.5 Service Provider Data (E.g. PostgreSQL).....37
6.1.6 Audit Log Data (E.g. PostgreSQL + JLB).....38
6.2 Data Security (indicative)..... 39
6.2.1 Encryption Standards.....39
6.2.2 Key Management.....39
6.3 Data Security Controls.....40
6.3.1 Authentication and Authorization.....40
6.3.2 API Security.....40
6.3.3 Data Privacy.....40
6.4 Compliance Requirements.....41
6.4.1 Data Protection Compliance..... 41
6.4.2 Security Standards Compliance..... 41
6.4.3 Accessibility Standards Compliance.....41
6.4.4 API and Interoperability Standards.....41
7. Appendices.....42
7.1 Glossary of Terms..... 42
8. Annexure: Example Scenario for SSO.....44
Scenario 2: Business User Login with Password Reset.....48
Scenario 3: Existing NDI-Registered Citizen Login During Bhutan NDI Outage.....49
Scenario 4: Admin Account Unlock and Security Review.....54

1. Overview

1.1 Purpose and Scope

1.1.1 Purpose

This Business Requirements Document defines the business requirements for the Single Sign-On (SSO) building block of Bhutan's Digital Public Infrastructure (DPI). SSO is a standalone authentication system that acts as the backup to NDI. It keeps government services reachable when NDI is down or fails. Bhutan NDI is the foundational and primary identity for government digital services. A user who registers and logs in through NDI does so without an SSO username or password, and reaches every service they are eligible for, including GA services, and the Government Portal (MyBhutan Portal).

So that the backup is ready before it is needed, a username and password is created in the backend for every user who registers through NDI, saves it in the SSO database, and sends it to the user once, for use only when NDI is unavailable. A user who is not yet registered when NDI is down can register directly in SSO using the same registration form as NDI, and sets their own username and password there.

For the backup to hold, SSO must sit in a failure domain separate from NDI, with its own credential store, session store and health checking. A backup that shares a failure domain with NDI fails in the outage it exists to cover.

The problem it addresses

Each government system today keeps its own user accounts and its own authentication method. Users must remember several sets of credentials, enter the same details again at each system, and meet different security rules in each one. This adds friction for users and raises support costs. It also weakens the security posture across governments, prevents a user from carrying an authenticated session from one service to the next, and leaves no single record of who authenticated where.

What SSO provides

SSO authenticates citizens, businesses, and other users of government digital services, and lets a user reach every service they are eligible for within one authenticated session. It populates the user profile from trusted sources rather than self-declaration, the NDI wallet first, then the responsible agency's source of truth, and manual entry only for what no source holds. It applies one set of security controls across all integrated services, and writes every authentication event to one audit trail through the Journaling Block (JLB).

Logging in through the SSO route always requires multi-factor authentication. Sessions established this way carry a lower identity assurance level than NDI sessions, so the set of services reachable through them is narrower.

SSO is the authentication gateway for Government Portal (MyBhutan Portal), when a user action requires an authenticated identity. After authentication the user reaches individual GA services, which lists the services they are eligible to access based on their identity and permissions.

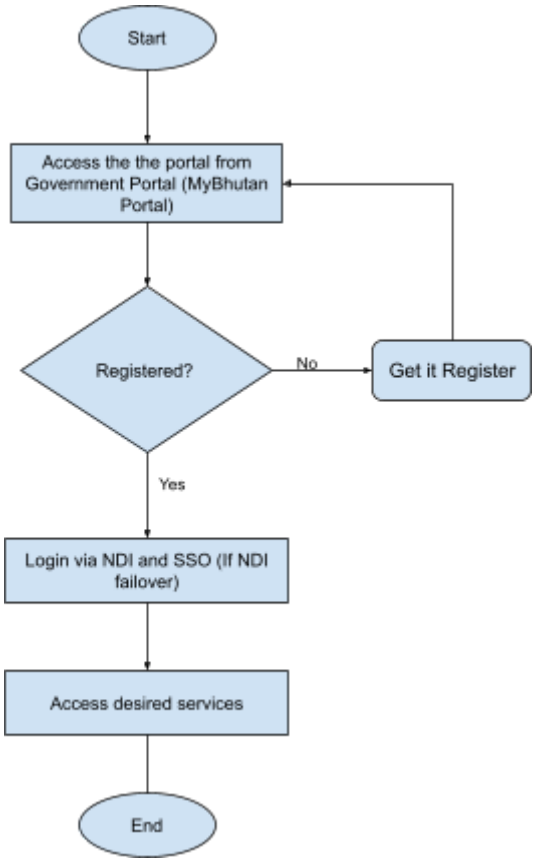


Figure 1: SSO architecture

How the two routes work

Both routes produce one user profile in the SSO database. The route used decides the credential, the checks, and the services the session can reach.

	NDI route	SSO route (fallback)

When used	Whenever NDI is available and the user holds an NDI credential	NDI is down and fails
Registration data	Details fetch from the NDI wallet.	Details fetch from the Agency (eg; DCRC, Tax,.), manual entry
Registration form	One form definition: same page, fields, validation rules and sequence on both routes. The SSO route adds Username, Password and Confirm Password.	
SSO username & password	Created by the backend at registration, saved to the SSO database, sent once to the user. Dormant while NDI is available.	Username pre-filled with the user's primary identifier; password set by the user on the form.
login	NDI authentication only. No SSO username or password prompt.	Username + password → MFA → post-authentication validation.

1.1.2 In Scope

Authentication routes and the NDI relationship

- Treatment of Bhutan NDI as the primary authentication route for every service that integrates with NDI, with SSO as the fallback.
- Consumption of a successful NDI authentication result and establishment of the SSO session from it, with no SSO username or password prompt, giving the user access to GA services, the Government Portal in one session.
- Continuous health checking of the NDI route, and selection of the routes offered on the login page on that basis. When NDI is down, the page offers the SSO username-and-password route and tells the user why.
- Availability of the SSO route when NDI is down, when NDI authentication fails for the user
- Deployment of SSO in a failure domain separate from NDI, with an independent credential store, session store, network path and health checking.

Registration through NDI (primary route)

- One registration form definition used on both the NDI and SSO routes, with the same page, fields, validation rules and sequence.
- Population of registration fields in this order:

    - claims held in the user's NDI wallet, including self-attested claims, retrieved with the user's consent;
    - remaining fields from the responsible agency's source of truth, DCRC Census System for citizens, Business Registry for businesses, Work Permit System for foreign workers, and other agency systems (such as DRC) as agreed during design;
    - manual entry of fields that no source holds.
- Email and SMS verification by OTP before account activation.
- Automatic creation of SSO credentials in the backend on successful NDI registration, without user action:
    - the username is set to the user's primary identifier (CID for citizens, permit number for foreign workers, business registration number for businesses);
    - a random password meeting the password policy is generated;
    - only the salted hash of the password is saved to the SSO database — the plain password is never stored or logged;
    - the username and password are sent once to the user's verified mobile and email through NTFB, with the message that they are for use only when Bhutan NDI is unavailable;
    - the credential stays dormant while NDI is available, and the user must change the password the first time it is used.
- Notification to the user each time the SSO credential is used.

Registration through SSO (fallback route)

- Self-service registration on the SSO route for a user who is not yet registered when NDI is down or fails. The registration page opens from the login page.
- Use of the same registration form as the NDI route, with Username, Password and Confirm Password added. Wallet retrieval is skipped; fields come from the agency source of truth, then manual entry.
- Registration of the user types: citizen by CID, service provider by business registration number, foreign worker by work permit.
- Marking of the resulting account as provisionally verified.
- Binding of a provisionally verified account to the user's NDI credential once NDI is available, duplicate detection on CID, permit number or registration number, and merge of duplicate accounts under one identity.

Login and session management

- Login on the SSO route in this sequence: username (email, CID, permit number or business registration number) and password → multi-factor authentication → post-authentication validation → session issued → access to eligible services.

- Mandatory multi-factor authentication on the SSO route for all user types, by SMS OTP, email OTP or TOTP.
- Post-authentication validation of account status, lockout state, session binding metadata and login anomalies before a session is issued.
- Constant-time credential comparison.
- Recording of the authentication route and resulting assurance level in the session, and enforcement of the narrower service set for sessions established through the SSO route.
- Step-up to NDI authentication when NDI is restored.
- Session establishment, token issuance, propagation to service providers, refresh, and timeout by user type.
- Single logout across all integrated services.
- Protocol support for OAuth 2.0 (Authorization Code with PKCE), OpenID Connect and SAML 2.0, token introspection, and onboarding and configuration of service providers.

Credential and account management

- Password policy, reset and recovery, password history and compromised-password checking.
- Password reset and account recovery by SMS or email OTP that works without NDI, so a user who has forgotten a dormant password can still sign in during an outage.
- Threat protection: brute-force lockout, credential stuffing detection, session fixation prevention and rate limiting.
- User profile management is limited to attributes the user entered manually; attributes from NDI or an agency source stay read-only.

Administration, audit and operations

- An administration portal covering user administration, service provider registration, active session monitoring, audit export and system configuration.
- Audit logging to JLB of authentication, registration, credential creation and use, fallback login, step-up, merge and administrative events.
- Integration with NTFB for notifications and OTP delivery, and with Unified Client Support (UCS) for account support tickets.
- Accessibility to WCAG 2.1 AA.
- Business continuity and disaster recovery for SSO, with a recovery objective stated against NDI outage scenarios.

1.1.3 Out of Scope

The following are explicitly excluded from the SSO Service scope:

- Issuance, custody and lifecycle management of the NDI credential and the NDI wallet. SSO consumes NDI authentication results and wallet claims; it does not issue, hold or revoke them.
- Biometric enrolment and biometric authentication, including fingerprint, facial and iris recognition. These remain NDI capabilities.
- Device management: device registration, fingerprinting, trust scoring and mobile device management. Session binding metadata recorded under S17 is not device management.
- Certificate and key-based authentication: PKI certificates, smart cards and hardware security keys beyond TOTP.
- Complex identity proofing: in-person verification at government offices, video verification, document upload with forensic checking, and manual verification workflows. SSO verifies identity through the NDI wallet and real-time integration with authoritative government sources only.
- Service-level authorization. Application permissions, role definitions and resource access policies remain with the individual services. SSO provides authentication and verified user identity.
- Federation with foreign or international identity systems.
- Verification of attributes beyond what the NDI wallet and the integrated government sources provide, such as employment history, educational credentials or property ownership. Data from integrated government sources is accepted as authoritative.
- Payment processing, payment gateway integration and digital wallet functionality for financial transactions.
- Service discovery and the service catalogue, including service metadata, application forms and eligibility determination, which belong to MyBhutan Portal.
- Delivery of the government services themselves.
- Support ticketing and complaint handling, which belong to the Unified Client Support (UCS) block.
- Diagnosis and repair of an NDI outage. SSO detects the outage, switches route, and restores NDI sessions on recovery.

1.2 Users

- Citizens authenticating by NDI, with an SSO credential held in reserve.
- Businesses and service provider organisations, including multiple users under one organisation.
- Foreign workers holding a work permit.
- Government services integrating with SSO as relying parties, including MyBhutan Portal.
- SSO administrators and GovTech operations staff.

1.3 Business Value

1.3.1 For Citizens

- Simplified Access to Government Services: Citizens log in once with SSO credentials and access all government services without repeated authentication. Eliminates need to remember multiple usernames and passwords across different services. Reduces friction in accessing essential services like healthcare, education, social welfare, and administrative services.
- Reduced Redundant Data Entry: Automatic population of personal information from Census System eliminates need to re-enter name, CID, address, and demographic details for each service. Saves time and reduces errors from manual data entry. Improves accuracy as data comes directly from authoritative government sources.
- Enhanced Security with Convenience: Strong password policies and optional multi-factor authentication protect citizen accounts from unauthorized access. Brute-force protection prevents account compromise. Impossible travel detection alerts citizens to suspicious login attempts. Citizens can manage their own passwords via self-service reset, reducing dependency on helpdesk.
- Consistent User Experience: Uniform login experience across all government digital services creates familiarity and reduces learning curve. Same credentials work everywhere - from MyBhutan Portal to service-specific applications. Single logout from any service logs out from all services, preventing unauthorized access from shared computers.

1.3.2 For Government Agencies

- Reduced Development & Maintenance Costs: Agencies no longer need to build and maintain separate authentication systems for each service. Eliminates duplicate effort in implementing password policies, MFA, audit logging, and security controls. Faster time-to-market for new services as authentication is ready-to-integrate infrastructure.
- Improved Security Posture: Enterprise-grade security controls (brute-force protection, credential stuffing detection, impossible travel detection) implemented once and benefit all services. Centralized security monitoring enables faster threat detection and response. Consistent password policies and MFA across all services eliminate weak security links. Immutable audit logging supports incident investigation and compliance audits.
- Verified User Identity: Integration with Census System, Tourism System, and Business Registry provides agencies with verified identity data. Reduces risk of fraudulent service access and identity theft. Agencies can trust SSO-authenticated users are who they claim to be. Eliminates the need for agencies to implement their own identity verification processes.
- Reduced Support Burden: Centralized password reset and account unlock workflows reduce helpdesk ticket volume. Self-service capabilities empower users to resolve common issues independently. A single support team handles authentication issues across

all services, enabling specialized expertise. Clear error messages and user guidance reduce support calls.

- Enhanced Data Quality: Auto-population from authoritative data sources eliminates duplicate data entry and associated errors. Agencies receive consistent, verified citizen/business data rather than self-declared information. Real-time synchronization with Census/Tourism/Business Registry ensures data remains current. Reduces data cleanup and reconciliation efforts.
- Seamless Cross-Service Integration: Standard OAuth 2.0 / OIDC / SAML 2.0 protocols enable easy integration with both new and legacy systems. User attributes available via standard claims in authentication token. Session management handled by SSO, eliminating inter-service session coordination complexity.

2. Single Sign-On Building Blocks Overview

2.1 SSO Overview

2.1.1 Digital Government Ecosystem

The SSO operates as the authentication gateway within the broader digital government ecosystem, serving as the unified authentication mechanism for all users accessing government digital services.

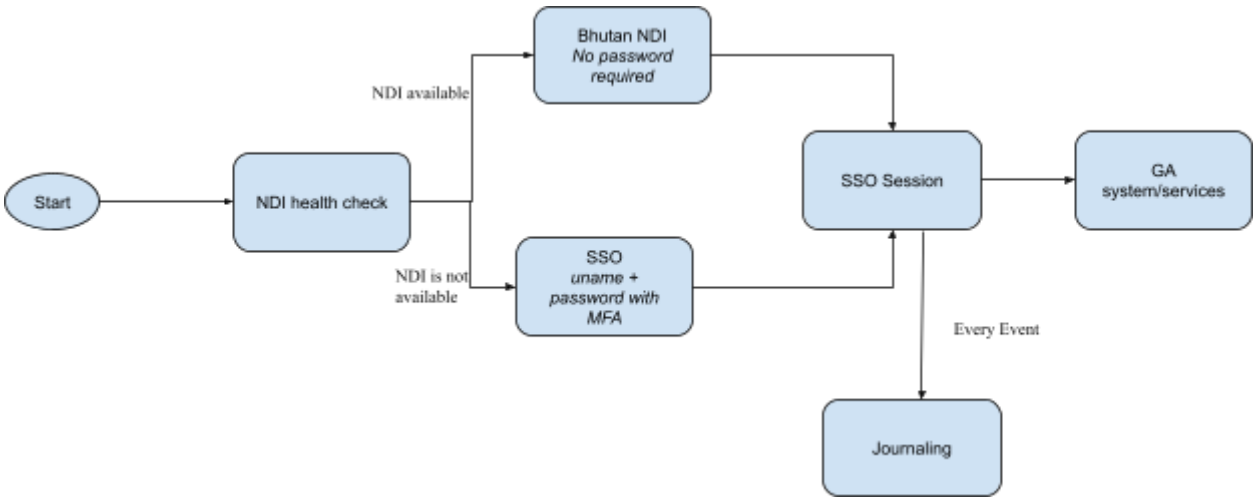


Figure 2 :Example Diagram of the Role of SSO

SSO Position in Ecosystem:

- Authentication Gateway: SSO serves as the central authentication point for citizens, businesses. All government services redirect unauthenticated users to SSO login pages.

- Identity Verification Hub: SSO integrates with authoritative government data sources (Census System, Business Registry) to verify user identity during registration, eliminating redundant verification across services.
- Session Authority: SSO manages authentication sessions across all integrated government services using standard protocols (OAuth 2.0, OIDC, SAML 2.0), enabling true single sign-on experience where users log in once and access all eligible services.
- Trust Anchor: Government services trust SSO-authenticated users because SSO has performed identity verification against authoritative sources. Services can focus on authorization decisions rather than re-implementing authentication.
- Audit Authority: All authentication events flow through SSO to Journaling Block (JLB), creating a comprehensive, centralized audit trail for security monitoring, compliance, and incident investigation.

2.2 SSO Roles and Responsibilities

Primary responsibility: authentication for all government digital services by consuming the Bhutan NDI authentication result while NDI is available, and by authenticating the user against its own credential when NDI is down.

SSO Receives:

- From Bhutan NDI: the authentication result for a user who signed in through NDI; wallet claims released by a user-authorised Proof Request at registration, including self-attested claims; the health status of the NDI route. SSO never receives or holds the NDI credential itself.
- From agency sources of truth: citizen data from the DCRC Census System (CID validation, name, date of birth, address, gender, dzongkhag); business data from the Business Registry (registration number validation, business name, owner, licence status); foreign worker data from the Work Permit System (permit validation, employer, validity).
- From users: registration submissions; login attempts with username and password on the fallback route; MFA responses (SMS OTP, email OTP, TOTP); password reset and account unlock requests; profile updates for user-entered fields; session status, extension and token refresh requests.
- From service providers: OAuth 2.0 and OIDC authorisation requests; SAML 2.0 authentication requests from legacy systems; token introspection requests; user info requests; single logout requests.

SSO Provides:

- A login page offering the available routes: Bhutan NDI while it is reachable, and the username-and-password route when it is not, with a message telling the user why the route changed.

- User-facing screens: registration (one form definition for both routes), MFA challenge, password reset, profile management.
- Credentials for the fallback route: a username and password created in the backend at NDI registration, sent to the user once through NTFB, and a notification each time that credential is used.
- Sessions and tokens: OAuth 2.0 authorisation codes and access tokens, OIDC ID tokens, SAML 2.0 assertions, refresh tokens, and session propagation across all integrated services.
- Verified user identity to services: user identifier, name, contact details, CID or permit or registration number, user type, verification status and language preference — together with the authentication route, the assurance level of the session and the provenance of each attribute. Revised
- Security protection: brute-force lockout, credential stuffing detection, account enumeration prevention, impossible travel detection, session fixation prevention, password policy enforcement and compromised-password checking.
- Audit and monitoring data: authentication, registration, credential, security, profile-change and administrative events to JLB; real-time metrics for SIEM.

SSO Manages:

- Route selection: continuous health checking of the NDI route, switching the login page between normal and fallback mode, and restoring the NDI route when it recovers.
- User account lifecycle: registration on both routes, email and mobile verification, activation, the provisionally verified state and its binding to an NDI credential, duplicate detection and merge, deactivation on permit expiry, reactivation, and deletion with data erasure.
- Credential lifecycle: generation of the fallback credential, hash-only storage, its dormant state while NDI is available, the forced change on first use, password history, reset and recovery that work without NDI.
- Session state: active sessions in the distributed cache, the authentication route and assurance level held in the session, step-up to NDI on recovery, service sessions per SSO session, timeout by user type, concurrent session limits and single logout.
- Security policy: password policy, MFA policy per user type and per route, failed-attempt tracking and lockout, rate limiting, and alert thresholds.
- Integration with identity sources: connections to NDI and the agency systems, caching, circuit breakers, retries and health monitoring for each.
- Service provider registry: onboarding, protocol and attribute-mapping configuration, and the service restrictions that apply to a fallback session.

Critical Boundaries:

- SSO provides authentication ONLY (not authorization): SSO authenticates user identity but does NOT determine which services users can access or what actions they can perform. Service-level authorization remains the responsibility of individual services.
- SSO does NOT modify identity source data: Census System, Tourism System, and Business Registry remain authoritative. SSO caches identity data for performance but cannot modify core identity attributes (name, CID, DOB). Users must update identity data at source systems.
- SSO does NOT handle payment processing: Financial transactions, payment gateways, digital wallets are separate payment infrastructure. SSO only provides authenticated identity for payment services.
- SSO does NOT manage service catalog: Service discovery, service metadata, eligibility determination are Government Portal (MyBhutan Portal) responsibilities. SSO redirects authenticated users to MyBhutan Portal which shows eligible services.
- SSO does NOT execute business workflows: Multi-step approval processes, task management, workflow orchestration are handled by workflow engines or individual services, not by SSO block.

2.3 Integration with Building Blocks

Building Blocks	Integration Purpose
Census System	Validate citizen CID during registration, fetch verified citizen data (name, DOB, address, gender, dzongkhag) as authoritative identity source
Zest System	Validate citizen EID during registration, fetch verified citizen data (Agency, Department) as authoritative identity source
Business Registry	Validate Business Registration Number, fetch business data (name, owner, type, license status), monitor license changes
Master Data Management Block (MDMB)	Master data that needs to be pulled from MDMB.
Journaling Block (JLB)	Immutable audit logging of all authentication events: login attempts, logout, password changes, profile updates, security alerts
Notification Block (NTFB)	Send email notifications (account creation, password reset, security alerts), SMS OTP for MFA, account lockout notifications
Government Portal(MyBhutan Portal)	Primary consumer - redirects users for login, validates tokens, displays eligible services, implements single logout
Feedback Block (FDBKB)	SSO authentication for authenticated feedback. Links feedback to verified identity. Supports anonymous mode.

Service-Specific Applications	Line-of-business apps (health, education, land, tax, licensing) use SSO for authentication. Services handle authorization.
Unified Client Support (UCS)	SSO admin console integrates with support system for account unlock, password reset assistance, user issue tracking
GA system	System that comes from Digital Service Transformation Division

3. Usage Scenarios

Refer to the use cases scenario in the annexure 8.

4. SSO Capabilities & Requirements

4.1 Functional Requirements

This section details the functional requirements for the Single Sign-On (SSO) module, organized by capability area. Each requirement includes a unique identifier (FR-X.Y format), priority classification using MoSCoW methodology (MUST/SHOULD/COULD), and specific acceptance criteria for validation and testing.

4.1.1 FR-1: Single Sign-On Core Requirements

These requirements define the fundamental Single Sign-On capabilities that enable users to authenticate once and gain access to multiple integrated government services without repeated login prompts.

ID	Requirement	Priority	Acceptance Criteria
FR-1.1	Implement centralized authentication for multiple applications	MUST	A single login grants access to all integrated services; the user authenticates once per session on either route; tokens propagate automatically to service providers; the user is redirected to the requested service after authentication; the session is maintained across all integrated applications; SP-initiated and IdP-initiated flows are both supported.
FR-1.2	Support cross-domain SSO across government services	MUST	SSO works across different domains and subdomains; session propagation is cookie-based or token-based; cross-origin communication is secured (CORS); domains are validated against a whitelist; cookies carry HttpOnly, Secure and SameSite=Strict; third-level domains are supported.

FR-1.3	Provide seamless service access without re-authentication	MUST	Connected services log the user in automatically while an SSO session exists; authentication is transparent; session validation responds in under 500 ms; application state is preserved during the SSO flow; no authentication prompt is shown to an authenticated user.
FR-1.4	Enable SSO session establishment and lifecycle management	MUST	A global SSO session is created on successful primary authentication, whether by NDI or by SSO credential; the session identifier is a UUID v4; the session is bound to the user identity and its metadata (user ID, IP address, user agent, timestamp, authentication route); sessions replicate across cluster nodes and synchronise within 1 second.
FR-1.5	Support SSO session validation for service providers	MUST	An active session is validated before service access; expiry and integrity are checked; session binding is verified; concurrent validation requests are handled; validation results are cached for 1 minute; validation responds in under 50 ms at the 95th percentile; a session validation API is available to SPs.
FR-1.6	Implement SSO session refresh and extension	MUST	Sessions extend on user activity using a sliding window; the refresh interval is configurable (default 5 minutes); refresh is transparent; the session timestamp and activity log are updated; session security is maintained through refresh; the user can extend a session manually.
FR-1.7	Enable service-to-service SSO propagation	MUST	(a) A service may obtain a token to call a downstream service on the user's behalf using OAuth 2.0 Token Exchange (RFC 8693). (b) The exchanged token is restricted to the specific downstream service (audience restriction). (c) It carries both the user's identity and the calling service's identity. (d) Its permissions are equal to or narrower than the original token's, never broader. (e) Its lifetime does not exceed the remaining SSO session lifetime. (f) The delegation chain is limited to [2] hops. (g) Service-to-service calls are authenticated with mutual TLS or signed client credentials. (h) Terminating the SSO session invalidates exchanged tokens within [X] seconds. (i) Every exchange is audit-logged with the user, calling service, target service and time.

FR-1.8	Provide single logout across integrated services	MUST	(a) Logging out from any integrated service or from the IdP terminates the global SSO session. (b) The IdP notifies all SPs that hold a session for that user, using [OIDC back-channel logout / SAML Single Logout]. (c) After logout, opening any integrated service requires a fresh authentication. (d) Session termination is effective on all cluster nodes within 1 second (FR-1.4.4(c)). (e) SPs that fail to acknowledge logout are recorded and retried [3] times; failures are logged and alerted.

4.1.2 FR-2: User Type Management Requirements

These requirements define support for different user types (Citizens, Service Providers) with type-specific authentication policies, session management, and access controls tailored to each category's security and usability needs.

ID	Requirement	Priority	Acceptance Criteria
FR-2.1	Support Citizen user type with National ID authentication	MUST	CID-based registration and authentication; full access to citizen-facing services on an NDI session; session timeout 30 minutes idle (configurable); MFA mandatory on the SSO route (FR-11.11) and carried by NDI on the NDI route; password, email OTP, SMS OTP and authenticator app supported; profile management, email and mobile number management.
FR-2.3	Support Service Provider user type for business entities	MUST	Business entity registration with business registration number or Organization ID (OID); mandatory MFA on both routes; session timeout 60 minutes idle; multiple users under one organisation with hierarchy support; password, email OTP and authenticator app; role-based access within the organisation; business verification workflow.
FR-2.4	Implement user type-specific authentication policies	MUST	Password policy, session timeout, login attempt limits, lockout, password reset and re-authentication rules are configurable per user type; (e.g session timeouts are Citizen 30 min, Tourist 15 min, Service Provider 60 min, Administrator 30 min) MFA is mandatory for every user type on the SSO route and for Service Providers on both

FR-2.5	Support user type identification and enforcement	MUST	User types are Citizen,Business, Service Provider and Foreign Worker; the type is selected at registration, shown in the UI and session information, and carried in the ID and access tokens; restrictions are enforced at the service provider; the type cannot be changed after registration; assignments are audit-logged and validated on every authentication.

4.1.3 FR-3: Authentication Methods Requirements

These requirements define the various authentication methods supported by the SSO system, including primary authentication (username/password), multi-factor authentication options (OTP, TOTP).

ID	Requirement	Priority	Acceptance Criteria
FR-3.1	Support username and password authentication	MUST	Passwords are validated against the stored hash using bcrypt (cost factor ≥ 12) or Argon2id; minimum length 12 characters with configurable complexity (uppercase, lowercase, number, special character); failed attempts are tracked per user with progressive delays; lockout follows the ladder in FR-10.1; unlock by OTP or administrator; passwords are checked against known breach lists.
FR-3.2	Support Email OTP authentication for all user types	MUST	6-digit OTP generated with cryptographic randomness; delivered through NTFB within configurable time (e.g., 30 seconds; validity 5 minutes; maximum 3 generations per hour per email address; resend cooldown 1 minute, the OTP is invalidated after use; failed attempts are capped at 3; the expiry time is displayed to the user.)
FR-3.3	Support SMS OTP authentication for Citizens	MUST	6-digit numeric OTP sent through Bhutan telecom providers within configurable time (e.g., 30 seconds; validity 5 minutes; maximum 3 requests per hour per mobile number; Bhutan number format validation; fallback to email OTP if SMS delivery fails after 2 minutes; delivery status and cost tracked; international numbers supported for citizens abroad.)

FR-3.4	Support TOTP/Authenticator App (mandatory for Service Providers)	MUST	TOTP to RFC 6238; QR code enrolment; common authenticator apps supported; 30-second time step; 6-digit codes; clock skew tolerance of ±1 step; 10 single-use backup codes generated at enrolment with a regeneration option; multiple devices per user; removal requires current authentication.

4.1.4 FR-4: Single Logout (SLO) Requirements

These requirements define Single Logout capabilities ensuring that when a user logs out from one service, they are automatically logged out from all connected services, maintaining security and preventing unauthorized access.

ID	Requirement	Priority	Acceptance Criteria
FR-4.1	Implement Single Logout across all integrated services	MUST	Logout terminates all active service sessions and notifies every participating SP; the process completes within 3 seconds at the 95th percentile; all access, refresh and ID tokens are invalidated; session cookies are cleared across domains; the user reaches a logout confirmation page; partial logout is handled when an SP is unavailable; all logout events are logged.
FR-4.2	Support SAML 2.0 Single Logout Protocol	MUST	SAML 2.0 SLO profile; front-channel (HTTP-Redirect and HTTP-POST) and back-channel (SOAP) bindings; LogoutRequest and LogoutResponse handling; SP-initiated and IdP-initiated flows; graceful handling of failures with a 3-second timeout per SP; messages are signed.
FR-4.3	Support OIDC Logout (RP-Initiated and Back-Channel)	MUST	OIDC RP-Initiated Logout 1.0 support; Implement end_session_endpoint; id_token_hint parameter validation; post_logout_redirect_uri support and validation; state parameter handling; OIDC Back-Channel Logout 1.0 support; logout_token JWT generation and signing; Deliver logout notifications to all RPs with registered backchannel_logout_uri
FR-4.4	Provide logout notification to all active service sessions	MUST	All active service sessions are tracked per SSO session; notifications are sent asynchronously; failed notifications retry up to 3 times with exponential backoff; propagation status is logged per SP; logout continues when an SP fails; a status summary is shown to the user; the audit trail is retained.

FR-4.5	Handle session timeout and automatic logout	MUST	Timeouts should be configurable (e.g., Citizen 30 min, Service Provider 60 min, Administrator 30 min, each configurable; an idle warning appears 2 minutes before expiry with a countdown and an extension option; timeout triggers full SLO; session data is cleared and the user is returned to the login page with a timeout message; timeout events are logged.)

4.1.5 FR-5: SSO Protocol Support Requirements

These requirements define support for industry-standard SSO protocols (SAML 2.0, OpenID Connect, OAuth 2.0) enabling interoperability with various government services and third-party applications.

ID	Requirement	Priority	Acceptance Criteria
FR-5.1	Support SAML 2.0 as Identity Provider (IdP)	MUST	SAML 2.0 Web Browser SSO Profile; SP-initiated SSO (AuthnRequest from SP); IdP-initiated SSO (unsolicited response); HTTP-POST and HTTP-Redirect bindings; Signed SAML assertions (RSA-SHA256 minimum); Signed SAML responses; Encrypted assertions (optional); AttributeStatement support with configurable attributes; Support NameID formats (persistent, transient, email); SAML metadata endpoint for IdP; Subject confirmation method (bearer); Audience restriction enforcement
FR-5.2	Support OpenID Connect (OIDC) as OpenID Provider	MUST	OIDC Core 1.0; Authorization Code Flow with PKCE for all client types, including single-page applications; Implicit Flow is not supported; Hybrid Flow only where a specific SP requires it and is approved; standard and custom claims, including authentication route and assurance level; UserInfo endpoint; ID tokens signed RS256; discovery and JWKS endpoints; scope, nonce and state validation.
FR-5.3	Support OAuth 2.0 for API authorization	MUST	OAuth 2.0 RFC 6749 compliance; Authorization Code Grant with PKCE; Client Credentials Grant (for service accounts); Refresh Token Grant; Scope-based authorization; Access token generation (JWT format); Token introspection endpoint (RFC 7662); Token revocation endpoint (RFC 7009); Client authentication methods (client_secret_basic, client_secret_post,

			private_key_jwt); Proof Key for Code Exchange (PKCE) RFC 7636

4.1.6 FR-6: SSO Session Management Requirements

These requirements define session lifecycle management including session creation, validation, refresh, tracking, and termination across the SSO infrastructure.

ID	Requirement	Priority	Acceptance Criteria
FR-6.1	Create and manage global SSO sessions	MUST	Generate unique session identifier (UUID v4 format); Store comprehensive session metadata (user ID, username, user type, IP address, user agent, device fingerprint, authentication timestamp, last activity timestamp, authentication method, authentication strength); Configurable session duration per user type; Session data stored in distributed cache (Redis cluster); Session replication across nodes for high availability; Secure session cookie attributes (HttpOnly, Secure, SameSite=Strict); Optional IP address binding for session validation; Session data encryption at rest
FR-6.2	Support session validation and refresh	MUST	Validate active SSO session on each SP access request; Check session expiry and integrity; Verify IP address binding (if enabled); Automatic session extension on user activity (sliding window); Configurable refresh interval (default 5 minutes before expiry); Session validation response time <50ms (95%); Cache session validation results (1 minute TTL); Silent session refresh without user interaction; Update session activity timestamp on validation; Handle session validation failures gracefully
FR-6.3	Track active service sessions per SSO session	MUST	Maintain registry of all services accessed during SSO session; Record service access timestamp; Track service provider details (entity ID, service name); Support concurrent access to multiple services; Session registry stored in distributed cache; Enable session listing via user dashboard; Allow selective service session termination; Record service access patterns for analytics; Expire service session entries on SSO logout

FR-6.4	Support multiple concurrent SSO sessions per user	MUST	Multiple sessions from different devices are allowed, each with its own session ID and binding metadata; all active sessions are listed in the dashboard with device type, browser, location and last activity; sessions can be terminated remotely; the concurrent session limit is configurable (default 3); the user is alerted on a login from a new device or location.
FR-6.5	Implement Remember Me functionality	SHOULD	Extended session duration for Remember Me (default 30 days); Separate persistent cookie for Remember Me token; Secure token generation (cryptographically random); Encrypted token storage; Remember Me token tied to specific device; Revocable Remember Me tokens; Re-authentication required for sensitive operations even with Remember Me; Device-based Remember Me (per device enrollment); Remember Me option during login; Clear explanation of Remember Me implications to user

4.1.7 FR-7: Token Management for SSO Requirements

These requirements define JWT token generation, validation, refresh, introspection, revocation, and security controls ensuring secure token-based authentication across SSO infrastructure.

ID	Requirement	Priority	Acceptance Criteria
FR-7.1	Generate JWT tokens for SAML and OIDC flows	MUST	JWT to RFC 7519 signed RS256 with RSA keys of 2048 bits or more; standard claims (iss, sub, aud, exp, iat, nbf, jti); custom claims for user attributes and for authentication route, assurance level and NDI status; configurable expiry (default ID token 15 minutes, access token 1 hour); token size under 2 KB; kid in the header; audience validation; acr and amr claims included.
FR-7.2	Support token refresh for extended sessions	MUST	Issue refresh tokens with authorization code flow; Refresh token validity 7 days (configurable up to 30 days); Refresh token rotation on use (one-time use); Revoke old refresh token when new one issued; Refresh token family tracking for security; Rate limiting on token refresh endpoint (10 requests per minute per client); Client authentication required for refresh; Return new access token and refresh token pair; Maintain refresh token lineage for audit; Detect refresh token reuse attacks

FR-7.3	Implement token introspection endpoint	MUST	RFC 7662 compliance; signature validated against JWKS; expiry and nbf checked; response carries active status and metadata, including the authentication route and assurance level; client authentication required; responds in under 100 ms at the 95th percentile; access and refresh tokens both supported; blacklist checked; rate-limited per client.
FR-7.4	Implement token revocation endpoint	MUST	OAuth 2.0 Token Revocation RFC 7009 compliance; Immediate token invalidation on revocation; Add revoked token to blacklist; Revoke entire refresh token family on revocation; Client authentication required; Support access token and refresh token revocation; Broadcast revocation to all cluster nodes; Audit log of all token revocations; Idempotent revocation (no error if already revoked); Handle revocation of expired tokens gracefully
FR-7.5	Support cryptographic key rotation for token signing	MUST	Automated key rotation every 90 days; Generate new RSA key pair (2048-bit minimum); Overlapping key validity period (7-day grace period); Publish multiple active keys via JWKS endpoint; Support simultaneous use of old and new keys during transition; Include kid (key ID) in JWKS and JWT header; Gradual key rollover without service disruption; Archive old keys for 30 days for signature verification; Manual key rotation trigger for security incidents; Key generation audit logging
FR-7.6	Maintain token blacklist for revoked tokens	MUST	(e.g. Redis)-based blacklist for high performance; Store revoked token JTI (JWT ID); Automatic blacklist entry expiry based on token exp claim; Check blacklist on every token validation; Cluster-wide blacklist synchronization (<1 second); Blacklist lookup response time <10ms; Support bulk token revocation; Persistent storage backup for blacklist (database); Blacklist cleanup for expired entries; Monitor blacklist size and performance

4.1.8 FR-8: Service Provider Integration Requirements

These requirements define the registration, configuration, testing, and monitoring capabilities for integrating service providers with the SSO system.

ID	Requirement	Priority	Acceptance Criteria

FR-8.1	Provide Service Provider registration and management interface	MUST	Admin UI for SP registration workflow; SAML SP metadata upload (XML file) with parsing; Manual OIDC client registration form; Configure SP entity ID, ACS URL, logout URLs; Set SP-specific attribute mapping; Configure user type restrictions per SP (Citizens only, exclude Tourists, etc.); Enable/disable SP integration toggle; SP registration approval workflow; Validation of SP metadata against schema; Test SP configuration before activation; SP documentation upload; Contact information management
FR-8.2	Support SAML metadata exchange and management	MUST	Expose IdP SAML metadata endpoint (/saml/metadata); Well-formed XML conforming to SAML 2.0 metadata schema; Accept SP metadata upload with validation; Automatic metadata parsing and entity extraction; Periodic SP metadata refresh (configurable interval, default 24 hours); Metadata signature verification (if signed); Entity descriptor validation; Support multiple assertion consumer service URLs; Support multiple single logout service URLs; Cache metadata for performance
FR-8.3	Support OIDC dynamic client registration	SHOULD	OAuth 2.0 Dynamic Client Registration Protocol RFC 7591; Automatic client_id generation (UUID); Automatic client_secret generation (cryptographically secure); Support client metadata (redirect_uris, grant_types, response_types, scopes, token_endpoint_auth_method); Client update endpoint; Client deletion endpoint (soft delete); Initial access token for registration endpoint; Rate limiting on registration (10 requests/hour per IP); Client metadata validation; Store client registration timestamp and metadata
FR-8.4	Configure attribute mapping per Service Provider	MUST	Map internal user attributes to SP-specific attribute names; Support attribute transformation rules (format conversion, concatenation, substring); Conditional attribute release based on user type or consent; Default attribute bundles (basic profile: name+email, full profile: all attributes); Custom attribute definitions per SP; Attribute format conversion (string, integer, boolean, array); Attribute filtering

			and masking; Test attribute release in sandbox mode; Attribute mapping versioning; Attribute mapping templates for common SPs
FR-8.5	Support SP-specific authentication and session policies	SHOULD	Configure required authentication strength per SP (LoA 1, 2, 3); Force MFA for high-security services; Set session duration override per SP; Restrict access to specific user types; IP whitelist/blacklist per SP; Time-based access restrictions (business hours only, 9AM-5PM); Geographic restrictions (Bhutan only, exclude specific countries); Re-authentication interval for sensitive SPs; Step-up authentication for privileged operations
FR-8.6	Provide SP integration testing and validation tools	SHOULD	Test SAML authentication flows (SP-initiated, IdP-initiated); Generate sample SAML assertions with test user; Test OIDC authentication flows (authorization code, implicit); Generate sample ID tokens and access tokens; Validate SP metadata and configuration; Test attribute release and verify attribute values; Simulate SSO and SLO flows end-to-end; Debug console with detailed request/response logs; Export test results and logs; Test environment separate from production
FR-8.7	Monitor and report on SP integration health	MUST	Track authentication success rate per SP (daily, weekly, monthly); Track authentication failure rate and error codes; Monitor authentication response times per SP; Detect SP availability issues (connection timeouts, errors); Alert on integration failures (>5% error rate or >10 consecutive failures); Dashboard showing SP status indicators (green/yellow/red); Historical integration metrics (30 days retention); SP usage analytics (authentication volume, active users); Weekly integration health reports to administrators

4.1.9 FR-9: SSO User Experience Requirements

These requirements ensure intuitive, accessible, and seamless user experience across all authentication touchpoints including login, consent, session management, and account recovery.

ID	Requirement	Priority	Acceptance Criteria
FR-9.1	Provide unified and accessible login interface	MUST	Single login page URL for all user types and SPs; User type selection interface (Citizens/Tourists/Service Providers); Responsive design (mobile 320px+, tablet, desktop); WCAG 2.1 Level AA accessibility compliance; Clear and actionable error messages; Progressive disclosure of authentication options; Remember username functionality; Show/hide password toggle; Keyboard navigation support; Screen reader compatibility; High contrast mode support
FR-9.2	Support seamless service redirection after authentication	MUST	Preserve original service URL (SAML RelayState, OIDC state parameter); Automatic redirect after successful authentication; Handle deep links and preserve query parameters; Maintain application state during SSO flow; Redirect completion within 2 seconds; Clear progress indicator during redirect; Handle redirect failures gracefully with error message; Support post-authentication landing page configuration per SP; Validate redirect URLs against whitelist
FR-9.3	Display consent screen for attribute sharing	MUST	Clear consent screen on first-time service access; Service provider name and logo display; List of specific attributes being shared with SP; Explanation of why attributes are needed; Option to accept or deny (with explanation of denial consequences); Remember consent decision for subsequent logins to same SP; Revoke consent option in user profile settings; Audit trail of all consent decisions; GDPR compliance for consent management; Consent expiry and re-prompting (annual); Progressive consent (request additional attributes later)
FR-9.4	Provide session timeout warning and extension	MUST	Display warning 2 minutes before session timeout; Modal dialog with countdown timer; One-click session extension button; Show remaining session time; Non-intrusive notification (not blocking user work); Work across all service provider applications; Preserve unsaved user work during extension; Configurable warning threshold per user type; Log session extension events; Limit number of extensions (default 3 per session)

FR-9.5	Support comprehensive account recovery workflows	MUST	Forgot password flow via email OTP or SMS OTP; Password reset link validity 1 hour; Security questions for additional identity verification (optional); Account unlock via OTP for locked accounts; Help desk escalation option with ticket generation; Clear step-by-step instructions; Track recovery attempts per user; Lockout after excessive recovery attempts (5 attempts per hour); Recovery success/failure notifications; Multi-language support for recovery flows; Accessibility compliance in recovery flows
FR-9.6	Provide user dashboard for session and account management	SHOULD	List all active SSO sessions with details (device type, browser, IP address, location, login timestamp, last activity); Show recently accessed services (last 30 days); One-click session termination per session; Terminate all sessions button; Security alerts for suspicious logins (new device, new location); Activity log with filtering (last 90 days); Download activity report (CSV, PDF); Link to profile management; MFA management interface; Password change interface
FR-9.7	Ensure full accessibility compliance	MUST	WCAG 2.1 Level AA full compliance; Screen reader support with ARIA labels and landmarks; Full keyboard navigation (Tab, Shift+Tab, Enter, Space, Esc); Focus indicators visible on all interactive elements; Skip navigation links; High contrast mode (4.5:1 minimum ratio); Adjustable font sizes (support browser zoom up to 200%); Alternative text for all images and icons; Form labels and error associations; No time limits on critical actions; Accessible error identification and suggestions; Accessible CAPTCHA alternatives; Regular accessibility testing

4.1.10 FR-10: SSO Security Requirements

These requirements define comprehensive security controls protecting against common attacks, ensuring data protection, and maintaining security audit trails.

ID	Requirement	Priority	Acceptance Criteria

FR-10.1	Implement rate limiting and brute force protection	MUST	Rate limit login attempts (5 per minute per IP address); Progressive account lockout (5 failed attempts = 30 min lockout, 10 failed = 24 hours); CAPTCHA challenge after 3 failed login attempts; IP-based rate limiting and blocking; Distributed rate limiting across cluster nodes; Alert security team on brute force patterns (>100 failed attempts per hour); Whitelist trusted IP ranges; Monitor and block credential stuffing attacks; Track failed authentication attempts globally; Automatic IP unblock after timeout
FR-10.2	Protect against CSRF attacks in authentication flows	MUST	CSRF tokens for all state-changing operations; State parameter validation in OAuth 2.0/OIDC flows (must match); Nonce parameter in OIDC ID tokens; Validate HTTP origin and referer headers; SameSite cookie attribute (Strict for session cookies); Double submit cookie pattern for AJAX requests; CSRF token rotation after authentication; Short-lived CSRF tokens (15 minutes); Synchronizer token pattern implementation; Log CSRF validation failures
FR-10.3	Prevent session fixation and hijacking attacks	MUST	Regenerate session ID immediately after successful authentication; Secure session cookie attributes (HttpOnly, Secure, SameSite=Strict); Optional IP address binding for session validation; User agent validation on session reuse; Detect and alert on session anomalies (IP change, location change); Force logout on security events; Session hijacking detection algorithms; Mutual TLS for high-security sessions; Monitor concurrent session usage patterns; Log all session security events
FR-10.4	Implement secure password storage and handling	MUST	bcrypt password hashing with salt (minimum cost factor 12); Argon2id algorithm support as alternative; No reversible encryption of passwords; Password pepper stored separately from database; Constant-time password verification (prevent timing attacks); Password history (prevent reuse of last 5 passwords); Hash passwords immediately upon receipt; Never log passwords; Secure password reset token generation; Password complexity validation before hashing

FR-10.5	Implement security headers and content security policies	MUST	Content-Security-Policy header with restrictive directives; X-Frame-Options: DENY (prevent clickjacking); X-Content-Type-Options: nosniff; Strict-Transport-Security with long max-age (31536000 seconds); X-XSS-Protection: 1; mode=block; Referrer-Policy: no-referrer; Permissions-Policy for sensitive features; Remove Server header; Remove X-Powered-By header; Cache-Control headers for sensitive pages
FR-10.6	Implement comprehensive input validation and sanitization	MUST	Validate all inputs against whitelist patterns; Reject inputs exceeding maximum length limits; Sanitize HTML and JavaScript in user inputs; SQL injection prevention using parameterized queries; LDAP injection prevention; XML/SAML injection prevention (secure XML parsing); URL validation and encoding; Email format validation; Phone number format validation; Reject null bytes and control characters; Validate file uploads (type, size, content); Log validation failures
FR-10.7	Implement security event logging and monitoring	MUST	Log all authentication events (success, failure, method); Log authorization decisions and failures; Log privilege escalation attempts; Log sensitive operations (password reset, MFA changes, profile updates); Real-time security event monitoring; Alert on anomalous patterns (failed logins spike, unusual access patterns); Integration with SIEM systems via syslog; Structured logging format (JSON); Include correlation ID for request tracing; Log retention 90 days (configurable); Secure log storage with integrity protection; Log access audit trail
FR-10.8	Enforce TLS/SSL encryption for all communications	MUST	TLS 1.2 minimum, TLS 1.3 preferred; Strong cipher suites only (AES-GCM, ChaCha20-Poly1305); Perfect Forward Secrecy (ECDHE key exchange); Valid SSL certificates from trusted Certificate Authority; Certificate pinning for critical connections; HSTS enabled with long max-age; OCSP stapling for certificate validation; Automated certificate renewal (Let's Encrypt or equivalent); Monitor certificate expiry (alert 30 days before); TLS for all backend service communications

FR-10.9	Support security scanning and penetration testing	MUST	Quarterly automated vulnerability scans; Annual third-party penetration testing; OWASP Top 10 compliance testing; Automated dependency vulnerability scanning (e.g. Snyk, Dependabot); Security patch management process (critical patches within 7 days); Vulnerability disclosure program with responsible disclosure policy; Security bug bounty program (optional); Pre-production security review for major changes; Security testing in CI/CD pipeline; Document and track security findings

4.1.11 FR-11:Fallback Registration and Authentication Requirements

These requirements define how SSO works with Bhutan NDI: NDI as the primary route, the credentials SSO holds in reserve, and the fallback registration and login used when NDI is down.

ID	Requirement	Priority	Acceptance Criteria
FR-11.1	Designate Bhutan NDI as the primary path for citizens, with SSO as fallback	MUST	For any consuming application integrated with NDI, registration and login route through NDI first; the SSO credential route is offered only when NDI is down, or when NDI authentication fails. The NDI route never prompts for an SSO username or password.
FR-11.2	Establish the SSO session from an NDI authentication result	MUST	On a successful NDI authentication, SSO creates its own session and issues tokens to the requesting service without any credential prompt; the session records authentication route = NDI and the NDI assurance level; within that session the user reaches GA services, and MyBhutan Portal; the event is logged to JLB.
FR-11.3	Check NDI health and select the routes offered	MUST	The NDI route is health-checked at a configurable interval (default 30 seconds) and on each login page load; the login page offers routes on that basis; in fallback mode a banner states that NDI is unavailable; the NDI route returns automatically within one interval of

			recovery; every mode change is logged; an administrator can force fallback mode.
FR-11.4	Retrieve registration data in stages: wallet, then agency source, then manual	MUST	Attributes are retrieved first by a user-authorised Proof Request to the NDI wallet, including self-attested claims; attributes not released are queried from the responsible agency source (DCRC Census System by CID, Tourism System by permit, Business Registry by registration number, Work Permit System by permit); anything still missing is entered manually; each attribute is stored with its provenance (wallet-verified, source-verified, self-declared); auto-populated fields display read-only.
FR-11.5	Use one registration form definition on both routes	MUST	The NDI and SSO routes present the same page, fields, validation rules and sequence; the SSO route adds Username, Create Password and Confirm Password; the username is pre-filled with the user's primary identifier and checked for uniqueness before submission.
FR-11.6	Deliver the fallback credential once and notify the user when it is used	MUST	NTFB sends the username and password once to the user's verified mobile and email, stating they are for use only when Bhutan NDI is unavailable; the password is never resent in plain text (recovery goes through reset); the user is notified each time the credential is used; delivery status is tracked; the user must change the password the first time it is used.
FR-11.7	Allow self-service SSO registration when NDI is unavailable	MUST	The login page offers registration while NDI is down; the form of FR-11.5 is used with the wallet step skipped; fields come from the agency source, then manual entry; email and mobile OTP verification is still required before activation; the account is created as provisionally verified.

FR-11.8	Support uninterrupted fallback login for NDI-registered users	MUST	A previously NDI-registered user signs in with CID or username and the SSO password during an outage; the session resolves to the same profile as the NDI-based account, keeping access, history and permissions consistent; the username field also accepts email, permit number and business registration number.
FR-11.9	Require MFA on the SSO route for every user type	MUST	Login on the SSO route always requires a second factor, SMS OTP, email OTP or TOTP, with no bypass for any user type; users without a mobile number use email OTP or TOTP; backup codes are accepted; a failed or abandoned MFA challenge issues no session; each attempt is logged.
FR-11.10	Validate the account after credential and MFA checks, before issuing a session	MUST	Before a session is issued the system checks account status, lockout state, credential expiry, session binding metadata and login anomalies; a failed check denies the session with a generic message and a specific audit entry; password comparison is constant-time.
FR-11.11	Record the route and assurance level, and restrict fallback sessions	MUST	The session and its tokens carry the authentication route, assurance level and NDI status; the services and actions unavailable to a fallback session are configurable per service provider; a blocked action returns a clear message telling the user to sign in with NDI once it is restored; enforcement is server-side.
FR-11.12	Step up to NDI authentication when NDI is restored	MUST	When NDI recovers, a fallback session is offered step-up authentication; on success the assurance level is raised within the same session without a new sign-in; the restrictions of FR-11.13 are lifted immediately; the step-up is logged to JLB.
FR-11.13	Provide password reset and account recovery that do not depend on NDI	MUST	Reset and unlock work entirely through SMS or email OTP while NDI is down, with no step in the path calling NDI; rate limits and audit logging apply as in §4.1.5; the user is notified after any credential change.

FR-11.14	Restrict profile editing to manually-entered fields	MUST	Fields populated from the NDI wallet or an agency source remain read-only; only user-entered fields are editable; server-side validation rejects edits to source-populated fields; users are told where to correct source data.

4.2 Non-Functional Requirements

This section defines the non-functional requirements that specify quality attributes, performance targets, security standards, and operational characteristics of the SSO system.

4.2.1 NFR-1: Performance Requirements

ID	Requirement	Target Metric
NFR-1.1	SSO authentication response time	Complete authentication in <2 seconds (95%), <3 seconds (99%)
NFR-1.2	Token validation performance	Token validation <100ms (95%), <200ms (99%)
NFR-1.3	Session validation performance	Session lookup and validation <50ms (95%)
NFR-1.4	Concurrent user capacity	Support 10,000 concurrent authenticated sessions; 100 authentication requests/second
NFR-1.5	Database query performance	Database queries <100ms (95%); Connection pool utilization <80%
NFR-1.6	Single Logout completion	Logout shall complete within ≤5 seconds for 95% of requests across integrated Service Providers, with partial-logout handling

4.2.2 NFR-2: Availability and Reliability Requirements

ID	Requirement	Target Metric
NFR-2.1	System uptime	99.9% uptime (8.76 hours downtime per year); Measured monthly
NFR-2.2	Planned maintenance windows	Max 4 hours/month; Scheduled during off-peak hours (midnight-4AM)
NFR-2.3	Mean Time To Recovery (MTTR)	Critical failures recovered within 1 hour; Non-critical within 4 hours
NFR-2.4	Failover capability	Automatic failover to secondary datacenter <30 seconds; Zero data loss

NFR-2.5	Backup and recovery	Daily automated backups; Recovery Point Objective (RPO) <24 hours; Recovery Time Objective (RTO) <4 hours

4.2.3 NFR-3: Scalability Requirements

ID	Requirement	Target Metric
NFR-3.1	Horizontal scaling	Scale to 50,000 users; Add nodes without downtime; Linear performance scaling
NFR-3.2	Auto-scaling capability	Auto-scale based on CPU (>70%) and memory (>80%) thresholds; Scale up <5 minutes
NFR-3.3	Service provider scaling	Support 100+ integrated service providers; Add new SPs without performance degradation
NFR-3.4	Database scalability	Support read replicas; Database sharding ready; Handle 1M+ user records
NFR-3.5	Session storage scaling	Redis cluster with 3+ nodes; Support 100,000+ concurrent sessions
NFR-3.6	Concurrent session / user scale	Support 10,000 concurrent authenticated sessions baseline, scaling to 50,000 users and 100,000+ sessions

4.2.4 NFR-4: Security and Compliance Requirements

ID	Requirement	Target Metric
NFR-4.1	Data encryption at rest	AES-256 encryption for all stored data; Database encryption enabled
NFR-4.2	Data encryption in transit	Minimum TLS 1.2 and TLS 1.3 is preferred for all communications; Perfect Forward Secrecy enabled
NFR-4.3	Security compliance	OWASP Top 10 compliance; ISO 27001 alignment; SOC 2 Type II readiness
NFR-4.4	Vulnerability management	Quarterly security scans; Critical patches within 7 days; Annual penetration testing
NFR-4.5	Audit logging	100% authentication events logged; 90-day log retention; Tamper-proof logs
NFR-4.6	Key rotation	RSA 2048-bit minimum, rotation at least every 90 days with 7-day overlapping validity via JWKS

4.2.5 NFR-5: Usability Requirements

ID	Requirement	Target Metric

NFR-5.1	User interface responsiveness	UI renders <1 second; Interactions respond <200ms
NFR-5.2	Browser compatibility	Support latest version Chrome, Firefox, Safari, Edge
NFR-5.3	Mobile compatibility	Responsive design for screens 320px+; Touch-optimized controls
NFR-5.4	Accessibility compliance	WCAG 2.1 Level AA; Keyboard navigation; Screen reader compatible
NFR-5.5	Internationalization	Support Dzongkha and English; RTL language ready; UTF-8 encoding

6. Data, Security and Compliance (Indicative)

6.1 Data Model (Indicative)

The SSO system manages multiple data entities stored across (e.g. PostgreSQL relational data), (e.g. Redis cache and sessions), and integrated with external systems. The data model is designed for high performance, security, and compliance with data protection regulations.

All the following table structures are examples only to provide an understanding of the data structure. It will vary depending on the details analysis, SRS and implementation stage.

6.1.1 User Data (E.g. PostgreSQL)

Table: users

Field Name	Data Type	Description	Constraints
user_id	UUID	Primary key, unique user identifier	PRIMARY KEY, NOT NULL
username	VARCHAR(100)	Unique username for login	UNIQUE, NOT NULL
email	VARCHAR(255)	User email address	UNIQUE, NOT NULL, INDEXED
email_verified	BOOLEAN	Email verification status	DEFAULT FALSE
phone_number	VARCHAR(20)	Mobile number (E.164 format)	NULLABLE, INDEXED
phone_verified	BOOLEAN	Phone verification status	DEFAULT FALSE
password_hash	VARCHAR(255)	bcrypt hashed password	NOT NULL
user_type	ENUM	Citizen, Tourist, Service_Provider	NOT NULL
cid	VARCHAR(50)	Citizen ID (for Citizens)	NULLABLE, UNIQUE

passport_number	VARCHAR(50)	Passport number (for Tourists)	NULLABLE
organization_id	VARCHAR(50)	OID (for Service Providers)	NULLABLE
first_name	VARCHAR(100)	User first name	NOT NULL
last_name	VARCHAR(100)	User last name	NOT NULL
language_preference	VARCHAR(10)	dz (Dzongkha) or en (English)	DEFAULT 'en'
status	ENUM	Active, Locked, Deactivated, Deleted	DEFAULT 'Active'
failed_login_attempts	INTEGER	Counter for failed login attempts	DEFAULT 0
locked_until	TIMESTAMP	Account unlock timestamp	NULLABLE
last_login	TIMESTAMP	Last successful login timestamp	NULLABLE
created_at	TIMESTAMP	Account creation timestamp	NOT NULL
updated_at	TIMESTAMP	Last update timestamp	NOT NULL
deleted_at	TIMESTAMP	Soft delete timestamp	NULLABLE

6.1.2 Multi-Factor Authentication Data (E.g. PostgreSQL)

Table: user_mfa

Field Name	Data Type	Description	Constraints
mfa_id	UUID	Primary key	PRIMARY KEY
user_id	UUID	Foreign key to users table	FOREIGN KEY, NOT NULL
mfa_type	ENUM	TOTP, Email_OTP, SMS_OTP	NOT NULL
mfa_secret	VARCHAR(255)	Encrypted TOTP secret	ENCRYPTED, NULLABLE
backup_codes	TEXT[]	Array of hashed backup codes	NULLABLE
is_enabled	BOOLEAN	MFA method enabled status	DEFAULT TRUE
enrolled_at	TIMESTAMP	MFA enrollment timestamp	NOT NULL
last_used_at	TIMESTAMP	Last successful MFA use	NULLABLE

6.1.3 Session Data (E.g. Redis)

Key Pattern: session:{session_id}

Data Structure: JSON

Field Name	Data Type	Description
session_id	String (UUID)	Unique session identifier
user_id	String (UUID)	Reference to user
username	String	Cached username
user_type	String	Citizen/Tourist/Service_Provider
ip_address	String	User IP address
user_agent	String	Browser user agent string
device_fingerprint	String	Device identifier hash
authentication_method	String	Password, OTP, MFA
authentication_strength	String	LoA 1, 2, or 3
created_at	Timestamp	Session creation time
last_activity	Timestamp	Last user activity time
expires_at	Timestamp	Session expiry time
service_sessions	Array	List of accessed SPs

TTL: User type specific (Citizen: 30min, Tourist: 15min, SP: 60min)

6.1.4 Token Metadata (E.g. PostgreSQL)

Table: tokens

Field Name	Data Type	Description	Constraints
token_id	UUID	Primary key	PRIMARY KEY
jti	VARCHAR(100)	JWT ID from token	UNIQUE, INDEXED
user_id	UUID	Foreign key to users	FOREIGN KEY, NOT NULL
token_type	ENUM	Access, Refresh, ID_Token	NOT NULL
client_id	VARCHAR(255)	Service provider client ID	NOT NULL
scope	TEXT	OAuth scopes	NULLABLE
issued_at	TIMESTAMP	Token issue timestamp	NOT NULL
expires_at	TIMESTAMP	Token expiry timestamp	NOT NULL
revoked	BOOLEAN	Token revocation status	DEFAULT FALSE
revoked_at	TIMESTAMP	Revocation timestamp	NULLABLE
refresh_token_family	VARCHAR(100)	Token family for rotation	NULLABLE

6.1.5 Service Provider Data (E.g. PostgreSQL)

Table: service_providers

Field Name	Data Type	Description	Constraints

sp_id	UUID	Primary key	PRIMARY KEY
entity_id	VARCHAR(500)	SAML Entity ID or OIDC Client ID	UNIQUE, NOT NULL
sp_name	VARCHAR(255)	Service provider name	NOT NULL
protocol	ENUM	SAML, OIDC, OAuth2	NOT NULL
metadata_url	TEXT	SAML metadata URL	NULLABLE
acs_url	TEXT	Assertion Consumer Service URL	NULLABLE
logout_url	TEXT	Single Logout URL	NULLABLE
redirect_uris	TEXT[]	OIDC redirect URIs	NULLABLE
client_secret_hash	VARCHAR(255)	Hashed client secret	NULLABLE
attribute_mapping	JSONB	Attribute mapping rules	NULLABLE
user_type_restrictions	TEXT[]	Allowed user types	NULLABLE
is_enabled	BOOLEAN	SP activation status	DEFAULT TRUE
registered_at	TIMESTAMP	Registration timestamp	NOT NULL
last_used_at	TIMESTAMP	Last authentication timestamp	NULLABLE

6.1.6 Audit Log Data (E.g. PostgreSQL + JLB)

Table: audit_logs

Field Name	Data Type	Description	Constraints
log_id	UUID	Primary key	PRIMARY KEY
timestamp	TIMESTAMP	Event timestamp	NOT NULL, INDEXED
event_type	VARCHAR(100)	Authentication, Authorization, Admin	NOT NULL, INDEXED
event_action	VARCHAR(100)	Login, Logout, Register, etc.	NOT NULL
user_id	UUID	User performing action	NULLABLE
username	VARCHAR(100)	Cached username	NULLABLE
ip_address	VARCHAR(50)	Source IP address	NOT NULL
user_agent	TEXT	Browser/client info	NULLABLE
result	ENUM	Success, Failure	NOT NULL
error_code	VARCHAR(50)	Error code if failure	NULLABLE
details	JSONB	Additional event details	NULLABLE
correlation_id	VARCHAR(100)	Request correlation ID	INDEXED

Note: Audit logs are also streamed to Journaling Block (JLB) for immutable storage and compliance.

6.2 Data Security (indicative)

6.2.1 Encryption Standards

Data at Rest:

- PostgreSQL: Transparent Data Encryption (TDE) with AES-256
- Redis: Encryption at filesystem level using LUKS
- Backup Storage: Encrypted backups with AES-256
- Sensitive Fields: Application-level encryption for passwords, MFA secrets, tokens

Data in Transit:

- External Traffic: TLS 1.3 only (fallback to TLS 1.2)
- Internal Service-to-Service: Mutual TLS (mTLS)
- Database Connections: TLS for all database connections
- Kafka: TLS encryption and SASL authentication
- Redis: TLS for all Redis connections

Sensitive Data Handling:

- Passwords: bcrypt hashing (cost factor 12) or Argon2id
- MFA Secrets: Encrypted with AES-256-GCM before storage
- Tokens: Signed with RS256, short-lived
- Session Data: Encrypted in Redis
- Backup Codes: Hashed with bcrypt

6.2.2 Key Management

Key Hierarchy:

- Root Key: Managed in Hardware Security Module (HSM) or G-Cloud KMS
- Data Encryption Keys (DEK): Per service, rotated every 90 days
- JWT Signing Keys: RSA 2048-bit, rotated every 90 days
- Session Encryption Keys: AES-256, rotated every 180 days

Key Rotation:

- Automated rotation schedule maintained
- Overlapping validity period (7 days grace)
- Zero-downtime key rotation
- Re-encryption of data with new keys within 30 days
- Old keys archived for 30 days for backward compatibility

6.3 Data Security Controls

6.3.1 Authentication and Authorization

Authentication:

- User Authentication: Multi-method (password, OTP, TOTP)
- Admin Portal: Mandatory MFA for all administrative access
- API Access: OAuth 2.0 client credentials or API keys
- Service-to-Service: mTLS with client certificates

Authorization (RBAC):

Role	Permissions
Super Admin	Full system access, user management, SP management, system configuration, audit log access
User Admin	User search, view user details, reset passwords, unlock accounts, view user audit logs
SP Admin	Service provider registration, configuration, attribute mapping, SP monitoring
Security Admin	View audit logs, security monitoring, token revocation, session management
Read-Only Admin	View-only access to dashboards, reports, and configurations

6.3.2 API Security

- Authentication: OAuth 2.0 Bearer tokens or API keys
- Rate Limiting: Per client (100 requests/minute)
- Input Validation: JSON schema validation on all inputs
- CORS: Restricted to whitelisted domains
- API Versioning: Version in URL path (/v1/)
- Request Signing: HMAC-SHA256 for sensitive operations
- Response Filtering: No sensitive data in error messages

6.3.3 Data Privacy

- Data Minimization: Collect only necessary data
- Purpose Limitation: Use data only for authentication purposes
- Consent Management: Explicit consent for optional data collection
- Right to Access: Users can view their data via dashboard
- Right to Erasure: Users can delete their accounts
- Data Portability: Export user data in JSON format

- Privacy by Design: Privacy controls built into system

6.4 Compliance Requirements

6.4.1 Data Protection Compliance

- Bhutan ICT Act: Compliance with national ICT regulations
- GDPR Principles: Apply GDPR principles where applicable
- Data Protection Impact Assessment (DPIA): Conducted and documented
- Data Breach Notification: Procedures for breach detection and reporting
- Data Processing Agreement: With all third-party processors

6.4.2 Security Standards Compliance

- OWASP Top 10: Protection against all OWASP Top 10 vulnerabilities
- ISO 27001: Alignment with ISO 27001 information security controls
- SOC 2 Type II: Readiness for SOC 2 Type II audit
- PCI DSS: Not applicable (no payment card data)

6.4.3 Accessibility Standards Compliance

- WCAG 2.1 Level AA: Full compliance with Web Content Accessibility Guidelines
- Section 508: Compliance with U.S. Section 508 standards
- Keyboard Navigation: Complete keyboard accessibility
- Screen Reader Support: Tested with NVDA, JAWS, VoiceOver

6.4.4 API and Interoperability Standards

- SAML 2.0: Full SAML 2.0 specification compliance
- OpenID Connect Core 1.0: Full OIDC specification compliance
- OAuth 2.0: RFC 6749 compliance
- JWT: RFC 7519 compliance
- OpenAPI 3.0: API documentation in OpenAPI 3.0 format
- REST API Best Practices: Following industry REST standards

7. Appendices

7.1 Glossary of Terms

Term	Definition
SSO	Single Sign-On - Authentication method allowing users to access multiple applications with one set of credentials
SLO	Single Logout - Capability to log out from all connected services simultaneously
SAML 2.0	Security Assertion Markup Language - XML-based standard for exchanging authentication and authorization data
OIDC	OpenID Connect - Identity layer built on top of OAuth 2.0 for authentication
OAuth 2.0	Open standard for access delegation, commonly used for token-based authentication
JWT	JSON Web Token - Compact, URL-safe means of representing claims between two parties
IdP	Identity Provider - System that creates, maintains, and manages identity information
SP	Service Provider - Application or service that relies on IdP for authentication
MFA	Multi-Factor Authentication - Authentication method requiring two or more verification factors
TOTP	Time-based One-Time Password - Temporary password generated using current time as factor
OTP	One-Time Password - Password valid for only one login session or transaction
CID	Citizen ID - National identification number for Bhutanese citizens
OID	Organization ID - Unique identifier for business entities and organizations
PKCE	Proof Key for Code Exchange - Security extension for OAuth 2.0 authorization code flow
JWKS	JSON Web Key Set - Set of public keys used to verify JWT signatures
TLS	Transport Layer Security - Cryptographic protocol for secure communication
mTLS	Mutual TLS - Two-way authentication where both client and server verify each other
ACS	Assertion Consumer Service - SAML endpoint that receives and processes authentication assertions
AuthnRequest	SAML authentication request sent from SP to IdP
RBAC	Role-Based Access Control - Access control method based on user roles
DPI	Digital Public Infrastructure - Foundational digital systems for government services

IDCB	Identity Conversion Block - DPI component for identity resolution and transformation
NTFB	Notification Block - DPI component for multi-channel notifications
EVTB	Government Event Bus - DPI component for event-driven integration
JLB	Journaling Block - DPI component for immutable audit logging
WCAG	Web Content Accessibility Guidelines - Standards for web accessibility
CORS	Cross-Origin Resource Sharing - Security mechanism for cross-domain requests
CSRF	Cross-Site Request Forgery - Type of attack exploiting user authentication
HSM	Hardware Security Module - Physical device for managing cryptographic keys

8. Annexure: Example Scenario for SSO

- Persona: Sonam Wangmo, 32-year-old citizen, first-time user of government digital services.
- Context: Sonam has a Bhutan NDI credential in her wallet and has never used a government service online. Bhutan NDI is available, so she registers through it. SSO creates her backup credential in the background for use during a future NDI outage.
- Step 1 — Initiate registration
    - User → opens a browser → navigates to gov.bt/portal
    - SSO → checks the NDI route: {"status":"UP"}
    - SSO → displays the login page for normal mode:
- Sign in to government services
    - [Continue with Bhutan NDI]
    - New user? Register here
    - Having trouble with Bhutan NDI? Get help

      The username and password route is not shown while Bhutan NDI is available (FR-11.1, FR-11.3).

    - User → clicks 'Register here'
- Step 2 — Select user type
    - SSO → displays "Who are you?": Bhutanese Citizen (with CID) · Tourist (with Tourism Permit) · Business (with Business Registration Number or OID) · Foreign Worker (with Work Permit)
    - User → selects 'Bhutanese Citizen'
- Step 3 — Verify identity through the NDI wallet
    - SSO → sends a Proof Request to Bhutan NDI for CID, full name, date of birth and gender
    - User → opens the NDI wallet → reviews what is being asked → approves
    - NDI → returns the released claims:

      {

      "cid": "11234567890",

      "name": "Sonam Wangmo",

      "dob": "1992-05-15",

      "gender": "Female",

      "provenance": "wallet-verified"

      }

SSO → address and dzongkhag were not released → queries the DCRC Census System by CID over NDE:

{

“address": "Changzamtog, Thimphu",

"dzongkhag": "Thimphu",

"provenance": "source-verified"

}

SSO → displays: "Identity verified. Welcome, Sonam Wangmo."

- Step 4 — Complete registration details

  Complete your registration

  Verified identity (read-only)

  - Full Name: Sonam Wangmo — from your NDI wallet
  - CID: 11234567890 — from your NDI wallet
  - Date of Birth: 15/05/1992 — from your NDI wallet
  - Gender: Female — from your NDI wallet
  - Address: Changzamtog, Thimphu — from the Census System

  Contact details (will be verified)

  - Email Address: _____
  - Mobile Number: +975 _____

  You do not choose a password here. Sign-in details for use if Bhutan NDI is ever unavailable will be created and sent to you once your account is active.

  - User → enters sonam.wangmo@gmail.com and +975 17123456, keeps English → clicks 'Register'
  - Each field is stored with its provenance, and the read-only fields cannot be edited later (FR-11.4, FR-11.16)
- Step 5 — Email verification
  - SSO → creates the account with status pending_verification
  - SSO → generates a 6-digit OTP valid 5 minutes → requests delivery from NTFB over NDE

    - SSO → displays the verification page with the code entry and a resend option (1-minute cooldown)
    - User → enters the code → email verified
- Step 6 — Mobile verification
    - SSO → sends an SMS OTP through NTFB, valid 5 minutes
    - User → enters the code → mobile verified
    - SSO → sets the account status to active, verification level verified, registration route NDI
    - SSO → publishes the registration event to JLB:

      {

       "event_type": "user_registered",

       "user_id": "USR_001",

       "cid": "11234567890",

       "registration_route": "NDI",

       "sources": ["ndi_wallet", "census_system"],

       "timestamp": "2026-09-22T10:30:00Z"

      }

- Step 7 — Backup credential created in the backend New
    - SSO → sets the username to her CID, 11234567890
    - SSO → generates a random password meeting the policy, stores only its salted hash, and marks the credential dormant (FR-11.6)
    - SSO → asks NTFB to send it once, by SMS and email:

      "Your account is active. If Bhutan NDI is ever unavailable, sign in

       with username 11234567890 and password Kz7#mVp2qRt9.

       You will be asked to change this password the first time you use it.

       Never share it. It is not needed for normal Bhutan NDI sign-in."

    - SSO → logs fallback_credential_issued to JLB. The password itself is never written to the log or stored in plain text (FR-11.7, FR-10.4)
    - SSO → displays: "Registration complete. Your account is active." → [Continue]
- Step 8 — First login with Bhutan NDI
    - User → clicks 'Continue' → SSO login page → [Continue with Bhutan NDI]

- SSO → NDI authentication (QR scan or deep link to the wallet); no username or password is requested
- NDI → returns a successful authentication result
- SSO → creates the session and issues an ID token:


```
{
 "sub": "USR_001",
 "name": "Sonam Wangmo",
 "email": "sonam.wangmo@gmail.com",
 "cid": "11234567890",
 "user_type": "citizen",
 "verification_status": "verified",
 "auth_route": "ndi",
 "acr": "ndi-high",
 "amr": ["ndi"],
 "language": "en",
 "exp": 1758540600
}
```


- SSO → session created with a 30-minute idle timeout (FR-2.4)
- SSO → logs the login to JLB
- SSO → redirects back to MyBhutan Portal with an authorization code, not a token:

  https://systems.gov.bt/callback?code=SplxlOB...&state=af0ifjsldkj

Key SSO Capabilities Demonstrated:

1. Identity verification via Census System integration with real-time CID validation
2. Auto-population of verified citizen data from authoritative source
3. Email verification via OTP sent through Notification Service
4. Mobile verification via SMS OTP
5. Password policy enforcement (12 char minimum, complexity)
6. JWT token generation with user claims for service integration
7. Comprehensive audit logging to Journaling Block (JLB) for all events

8. Session management with Redis distributed cache

Success Criteria:

1. Registration completed within 5 minutes
2. CID verified in real-time (<2 seconds)
3. Email and mobile verified successfully
4. User data accurate (from Census System)
5. First login successful with correct token claims
6. All events logged to JLB for audit trail
7. User satisfaction score ≥4/5

Scenario 2: Business User Login with Password Reset

Persona: Karma Tshering, 40-year-old business owner, registered restaurant owner, forgets password

Context: Karma registered his restaurant business account 2 months ago but forgot his password. He needs to log in to renew his business license and access tax filing services.

User Journey:

Step 1: Failed Login Attempt

- User → Navigates to SSO login page
- User → Enters username: karma_restaurant
- User → Enters password: [wrong password]
- User → Clicks 'Login'
- SSO → Validates credentials → Failed (Attempt 1/5)
- SSO → Displays error: "Invalid username or password. Attempts remaining: 4"
- User → Tries again with different password → Failed (Attempt 2/5)
- User → Realizes password forgotten → Clicks 'Forgot Password?'

Step 2: Initiate Password Reset

- SSO → Displays password reset page:
  - "Reset Your Password"
  - Enter your email or username:_____
- User → Enters: karma_restaurant
- User → Clicks 'Send Reset Link'
- SSO → Looks up user account → Found (email: karma.tshering@gmail.com, phone: +97517987654)
- SSO → Generates password reset token (6-hour validity)

- SSO → Calls Notification Service to send reset link via email
- SSO → Displays: "Password reset link sent to karma.t***@gmail.com"

Step 3: Verify Identity via SMS OTP

- SSO → Generates SMS OTP: 456789
- SSO → Sends SMS to +97517987654
- SSO → Displays OTP verification page:
    - "Verify Your Identity"
    - We've sent a code to your mobile ending in ***7654
    - Enter code: __ __ __ __ __ __
- User → Receives SMS → Enters OTP: 456789
- SSO → Validates OTP → **Verified**

Step 4-6: [Set new password, login with new credentials, access MyBhutan Portal successfully]

- Key SSO Security Capabilities Demonstrated:
    - Failed login attempt tracking (5 attempts before lockout)
    - Self-service password reset workflow
    - Identity verification via SMS OTP before password reset
    - Time-limited reset tokens (6-hour expiry)
    - Secure password reset preventing account enumeration
    - Comprehensive audit logging of password reset events
    - Notification of password change to user email for security awareness

Scenario 3: Existing NDI-Registered Citizen Login During Bhutan NDI Outage

Persona: Sonam Wangmo, 32-year-old citizen, existing SSO and Bhutan NDI registered user
Context: Sonam has already registered her account previously using Bhutan NDI. Her verified identity and profile are already stored in the SSO database. Today, she wants to access government services online, but the Bhutan NDI platform is temporarily unavailable. The SSO platform provides secure fallback authentication using locally stored credentials and OTP verification.

User Journey:

Step 1: Access Government Portal

- User → Opens web browser → Navigates to mybhutan.gov.bt/portal
- MyBhutan Portal → Detects user not authenticated → Redirects to SSO login page

- SSO → Performs Bhutan NDI health check: GET /ndi/health
- NDI Gateway → Returns:

```
{
"status": "DOWN",
"message": "NDI authentication service unavailable"
}
```

- SSO → Displays login page with options:
    - Login with Bhutan NDI (Temporarily Unavailable)
    - Login with Username & Password
    - Forgot Password?
- SSO → Displays notification banner:

"Bhutan NDI services are temporarily unavailable. Please use fallback secure login."

Step 2: User Selects Fallback Login

- User → Clicks "Login with Username & Password"
- SSO → Displays secure login form:
    - Username / CID: _____
    - Password: _____
    - [Login]

Security Notice:

- OTP verification will be required for secure access
- User → Enters:
    - Username: sonam_wangmo
    - Password: MySecure@Pass123
- User → Clicks "Login"

Step 3: Validate Existing SSO User

- SSO → Searches local SSO Identity Database
- SSO → Retrieves user profile:

```
{
"user_id": "USR_001",
"username": "sonam_wangmo",
"name": "Sonam Wangmo",
"cid": "11234567890",
```

"ndi_registered": true,
"account_status": "active",
"mobile_verified": true,
"email_verified": true
}

- SSO → Validates password hash → Success
- SSO → Determines:
  - User already verified via Bhutan NDI previously
  - NDI currently unavailable
  - Step-up OTP verification required

Step 4: OTP Verification

- SSO → Generates SMS OTP: 674219
- SSO → Calls Notification Block: POST /notifications/send

{
"recipient": "+97517123456",
"channel": "SMS",
"message": "Your SSO verification code is 674219. Valid for 5 minutes."
}

- Notification Block → Sends SMS OTP
- SSO → Displays OTP verification page:
  - "Verify Your Identity"
  - Enter the 6-digit code sent to your mobile number
  - Code: _ _ _ _ _ _
  - Code expires in: 5:00 minutes
  - [Resend OTP]
- User → Receives SMS → Enters OTP: 674219
- SSO → Validates OTP → Success

Step 5: Risk and Security Evaluation

- SSO → Performs adaptive authentication checks:
  - Device recognition
  - Login history validation
  - IP reputation check
  - Geolocation consistency
  - Failed login monitoring
- SSO → Risk engine returns:

```
{
"risk_level": "LOW",
"action": "ALLOW"
}
```

- SSO → Allows authenticated session creation

Step 6: Token Generation and Session Creation

- SSO → Generates JWT token with claims:

```
{

"user_id": "USR_001",
"username": "sonam_wangmo",
"name": "Sonam Wangmo",
"cid": "11234567890",
"user_type": "citizen",
"ndi_registered": true,
"authentication_method": "fallback_password_sms_otp",
"ndi_status": "DOWN",
"mfa_verified": true,
"session_trust_level": "MEDIUM",
"exp": "2025-12-29T12:30:00Z"
}
```

- SSO → Creates session in Redis (1-hour timeout)
- SSO → Logs authentication event to JLB:

```
{
"event_type": "fallback_login_success",
"user_id": "USR_001",
"authentication_method": "password_sms_otp",
"ndi_registered": true,
"ndi_status": "DOWN",
"timestamp": "2025-12-29T10:45:00Z"
}
```

- SSO → Redirects to MyBhutan Portal with token:

```
https://systems.gov.bt?token=[JWT]
```

Step 7: Access Citizen Portal

- MyBhutan Portal → Receives token → Validates with SSO: POST /oauth/introspect
- SSO → Returns:

```
{
 "active": true,
 "user_id": "USR_001",
 "authentication_method": "fallback_password_sms_otp",
 "session_trust_level": "MEDIUM"
}
```

- MyBhutan Portal → Grants access → Displays citizen dashboard:
  - "Welcome, Sonam Wangmo!"
- Available Services:
  - Health Services
  - Education Services
  - Tax Services
  - License Renewal
  - Application Tracking
- Restricted Services During NDI Outage:
  - Digital signature services
  - High-value financial transactions
  - Sensitive profile updates
- MyBhutan Portal → Displays banner:

"You are logged in using fallback authentication because Bhutan NDI services are temporarily unavailable."

Key SSO Capabilities Demonstrated:

- Existing NDI-linked user support
- Local SSO credential validation
- Fallback authentication during NDI outage
- SMS OTP-based MFA
- Adaptive risk-based authentication
- JWT token generation with fallback claims
- Redis-based session management
- Conditional access restrictions
- Audit logging to JLB
- Session trust-level management
- Seamless NDI recovery handling

Success Criteria:

- Existing user login completed successfully
- OTP delivered within 30 seconds
- Essential government services remain accessible
- Sensitive services remain protected
- All authentication events logged to JLB
- No unauthorized access during fallback mode
- Session upgraded automatically once NDI restored
- Minimal disruption to citizen services

Scenario 4: Admin Account Unlock and Security Review

Persona: Pema Dorji, SSO User Administrator at GovTech Bhutan
Context: A citizen reports that her SSO account is locked after multiple failed login attempts. At the same time, the SSO Security Dashboard shows repeated failed logins from an unfamiliar IP address. The administrator must verify the user, review the security event, unlock the account if legitimate, and ensure all actions are logged.

User Journey

Step 1: Admin Login

- Admin → Opens SSO Admin Portal
- SSO → Displays admin login page
- Admin → Enters username and password
- SSO → Requires mandatory MFA for admin access
- Admin → Enters TOTP / OTP code
- SSO → Validates credentials and MFA
- SSO → Grants access based on admin role: User Admin / Security Admin

Step 2: Review Security Dashboard

- Admin → Opens **Security Dashboard**
- SSO → Displays real-time metrics:
- Active users
- Concurrent sessions
- Login success/failure rate
- Locked accounts
- Failed login trends
- Suspicious IP addresses
- Account lockout alerts

- Admin → Notices alert:
  "Multiple failed login attempts detected for user: sonam_wangmo"
- The SSO document defines the dashboard as showing authentication metrics, active sessions, locked accounts, failed login trends, suspicious patterns, and system health.

Step 3: Search and Verify User

- Admin → Opens **User Management Console**
- Admin → Searches by username / email / CID:

  Sonam_wangmo

- SSO → Displays user record:

```
{
 "username": "sonam_wangmo",
 "user_type": "citizen",
 "verification_status": "verified",
 "account_status": "locked",
 "failed_login_attempts": 5,
 "last_login": "2025-12-28T09:15:00Z",
 "locked_until": "2025-12-29T11:00:00Z"
}
```

- Admin → Reviews profile, registration date, last login, active sessions, and audit history.

Step 4: Review Audit Trail

- Admin → Opens user audit trail
- SSO → Shows recent events:

```
[
    {
     "event_type": "login_failed",
     "reason": "invalid_password",
     "ip_address": "203.xxx.xxx.10",
     "timestamp": "2025-12-29T10:05:00Z"
    },
    {
     "event_type": "account_locked",
     "reason": "5_failed_login_attempts",
     "timestamp": "2025-12-29T10:07:00Z"
    }
```

]

- Admin → Confirms whether the failed attempts came from the user's known location/device.
- The SSO requirements state that authentication events, account lockouts, security alerts, admin actions, account unlocks, and manual password resets must be logged and sent to JLB for audit/compliance.

Step 5: Verify User Identity

- Admin → Contacts user through registered phone/email or linked UCS ticket
- User → Confirms identity details:
    - CID
    - Registered email
    - Registered mobile number
    - Last successful login date
- Admin → Confirms the request is legitimate

Step 6: Unlock Account

- Admin → Clicks **Unlock Account**
- SSO → Requires justification:

User identity verified through registered mobile number and CID.
Account locked due to repeated failed login attempts.
Unlock approved after user confirmation.

- Admin → Submits unlock request
- SSO → Updates account status:

```
{
 "account_status": "active",
 "failed_login_attempts": 0,
 "locked_until": null
}
```

- SSO → Logs admin unlock event to JLB
- SSO → Sends notification to user:
    - "Your SSO account has been unlocked. If this was not requested by you, contact support immediately."

Step 7: Optional Password Reset

- If the user cannot remember the password:
- Admin → Selects **Manual Password Reset**
- SSO → Requires dual approval
- Second Admin → Reviews and approves reset request
- SSO → Generates temporary reset link or temporary password
- User → Sets a new password on first login
- SSO → Invalidates old sessions and logs password reset event

The document specifies that manual password reset requires dual approval and must include audit trail with administrator identity.

Step 8: Close Support Case

- Admin → Adds resolution note:

Account unlocked after identity verification. No active suspicious session found.
Users advised to change password and enable MFA.

- SSO/UCS → Closes support ticket
- SSO → Final audit event recorded

Key SSO Capabilities Demonstrated

1. Admin login with mandatory MFA
2. Role-based access control for User Admin and Security Admin
3. User search by username, email, CID, or phone
4. Account lockout investigation
5. Security dashboard review
6. Audit trail review
7. Manual account unlock with justification
8. Optional manual password reset with dual approval
9. User notification after admin action
10. JLB audit logging for compliance

Success Criteria

1. Admin accesses portal only after MFA
2. Locked user account is found within 1 minute
3. User identity is verified before account unlock
4. Unlock action requires justification
5. Password reset requires dual approval when used
6. All admin actions are logged to JLB

7. User receives unlock/reset notification
8. No unauthorized account access occurs after unlock