Software Requirement Specification

Sri Lanka Unique Digital Identity Proof of Concept (SLUDI - PoC)

(Version 1.0)

Information Communication Technology Agency of Sri Lanka (ICTA)

DOCUMENT RELEASE NOTICE	
Document Title: Software Requirement Specification – Sri Lanka Unique Digital Identity – Proof of Concept (SLUDI PoC) Release (Number): 1.0 Date of Release: 11 February 2021	
Author(s): Sachin Anjana Kulasinghe	Date: 11 February 2021
Reviewer(s): Dasun Hegoda	Date: 1st March 2021
Approved by: Hiranya Samaresekara	Date:

REVISION HISTORY			
Document No:1.0		Document Title: Software Requirement Specification –SLUDI PoC	
Revision Number	Issue Date	Change Details	Approved by
1.0	11-02-2021	Initial document creation by Sachin	
1.1	01-03-2021	Document overall fine-tuning by Dasun	

Table of Contents

Contents

Table of Figures

No table of figures entries found.

List of Tables

Glossary

1 Introduction

The National Policy Framework (NPF) Vistas of Prosperity and Splendor is aimed at achieving a fourfold outcome of a productive citizenry, a contented family, a disciplined and just society and a prosperous nation. A Technology Based Society (Smart Nation) is one of the 10 key goals of the NPF. In that, setting up a Citizen Centric Digital Government has been identified as a strategy to achieve the government vision.

Governments worldwide are adopting the strategy of having a unique digital identity for citizens. It is envisioned that it could enable dramatic leaps in service quality and massive efficiency gains for governments, as well as drive financial and social inclusion by providing citizens access to citizen services and benefits of healthcare, education, and other government programs.

Therefore, the Government has given priority to a national level program for the establishment of a Unique Digital Identity Framework for Sri Lanka. The project is named Sri Lanka Unique Digital Identity (SLUDI).

For this purpose, a Programme Preparation Committee (PPC) has been appointed by HE the President. The Information and Communication Technology Agency of Sri Lanka (ICTA) has been appointed to function as the implementation/execution agency for the SLUDI project.

The objective of this document is to provide an overall understanding about the SLUDI project's Proof of Concept (PoC) including the specification of the scope of work and intended goals of the project.

1.1 Purpose

The SLUDI PoC project will be conducted as a feasibility study leading up to the main SLUDI project. The end goal of the project is to review systems that can be used by testing with mock scenarios.

1.2 Scope

The SLUDI PoC project will include the following aspects:

- Feasibility study of the proposed architecture of SLUDI
- Technical feasibility to implement SLUDI
    - Modular Open Source Identity Platform (MOSIP)
    - Biometric SDK
    - Automated Biometrics Identification System (ABIS)
    - Biometric Devices
- Functional feasibility study for the implementation of SLUDI
    - Pre-Registration Application
    - Registration Client Application
    - ABIS duplication
    - UDI Generation

1.3 User Characteristics

All user levels included in the system are mentioned below:

No.	Character	Description & Functions	Restrictions
01	PreReg Admin	Pre-registration of users to the system Approval of Pre-Reg applications entered to the system	Login is limited to the Pre-Reg application Can create a pre-registration application
02	PreReg Officer	Pre-registration of users to the system	Can create a pre-registration application only
03	RegCenter Admin	Registration of users to the system Approval of user registration submits	Login is limited to the Reg client application
04	RegCenter Officer	Registration of users to the system	Login is limited to the Reg client application
05	MOSSIP Admin	CRUD of all user roles Instance setup and management	-
06	Citizen	All applications entered to the system are citizen characters	-

Table 1: User Characteristic

1.4 Limitations

1.5 Assumptions and Dependencies

1.6 Definitions

1.7 Acronyms and Abbreviations

- NPF – National Policy Framework
- SLUDI – Sri Lanka Unique Digital Identity
- PPC - Programme Preparation Committee
- ICTA – Information Communication Technology Agency
- MOSIP – Modular Open Source Identity Platform
- ABIS – Automated Biometrics Identification System

2 Requirements

2.1 Use Cases

2.1.1 Use Case 01: Pre-Registration: Login

Use Case #/ID	01	**Description**	Pre-Registration: Login
Initiating Actor	PreReg Officer/ PreReg Admin	**Other Actors**	-
Use Case Overview			
The user logs into the system via a mobile number and an OTP			
Pre-conditions			
Each user must have a unique mobile number			
Business Rules			
- Mobile number contains numeric values only - Mobile number is mandatory field and should start with any country code example (+94) and rest nine characters should be numeric. Total character length is 12. - OTP validation			
Main Event List/Flow of Events			
Enter Mobile number *Receive OTP to mobile number* *Enter OTP* *Submit*			
Alternate Event List/Flow of Events			
Path 01 *Enter invalid or empty OPT* *Invalid OTP error message* *Reroute to re-enter OTP*			

2.1.2 Use Case 02: Pre-Registration: New Application

Use Case #/ID	02	**Description**	Pre-Registration: New Application
Initiating Actor	PreReg Officer/ PreReg Admin	**Other Actors**	Citizen

Use Case Overview

Pre-Registration process of an applicant to book an appointment for the final registration.

Pre-conditions

Login must be completed

Terms and conditions pop up must be accepted

Business Rules

- All data should be available in configured languages
- Full name should be in 0-120 length
- Date of birth should be in DD MM YYYY format
- Gender is mandatory field and should one of Male, Female, Other
- Residential status is mandatory field and should be one of Non-Foreigner or Foreigner.
- Address Line 1 to 3 are mandatory fields and length should 0-50 characters each.
- Province is a mandatory field and should not be editable. Picked from master data.
- District is a mandatory field and should not be editable. Picked from master data.
- City is mandatory field and should not be editable. Picked from master data.
- Postal code is a mandatory field and should not be editable. Picked from master data.
- Phone number is a mandatory field and should start with the country code (Ex:+94 for Sri Lankan numbers) and rest nine characters should be numeric. Total character length is 12.
- Email is a mandatory field and should contain only email addresses. Only “0-9”, “a-z”, “A-Z”. And in middle should contain “@” and “.”.
- Proof of Identity is a mandatory field, document should be in configured formats and the file size
- Proof of Address is an optional field, document should be in configured formats and the file size

Main Event List/Flow of Events

Enter demographic details

Upload scanned documents to show proof of identity and proof of address

Book appointment including date and time slot

Submit and view confirmation of appointment

Alternate Event List/Flow of Events

Path 01

Before submit appointment user click on send email/SMS

User get a pop up and enter email or mobile number(not the login email or mobile number)

User will receive pre-registration application to the email or SMS

Path 02

User able to cancel and delete appointments

Path 03

If user return home only entering demographic data, application will be in pending appointment

2.1.3 Use Case 03: Pre-Registration: Logout

Use Case #/ID	03	**Description**	Pre-Registration: Logout
Initiating Actor	PreReg Officer/ PreReg Admin	**Other Actors**	-
Use Case Overview			
Once tasks are completed the user logs out.			
Pre-conditions			
Should be logged into the system			
Business Rules			
- End the current session			
Main Event List/Flow of Events			
Select Logout option			
Alternate Event List/Flow of Events			
Path 01 *User inactive on pre-registration portal for the configured amount of time* *Log out user automatically*			

2.1.4 Use Case 04: Registration Client: Login

Use Case #/ID	04	**Description**	Registration Client: Login
Initiating Actor	RegCenter Officer/ RegCenter Admin	**Other Actors**	-
Use Case Overview			
The user connects to the system via an authenticated PC/Device.			
Pre-conditions			
User must have an authenticated devices registered in the system			
Business Rules			
- Validate Username and Password with system database - Username is a mandatory field - Password is a mandatory field - User should be mapped to the same registration center and device.			
Main Event List/Flow of Events			
Open Registration Client application *Login using given username and password*			

Alternate Event List/Flow of Events
Path 01 *Forgot Username* *Click Forgot username* *Path 02* *Forgot Password* *Click Reset Password* *Redirect to request password reset*

2.1.5 Use Case 05: Registration Client: New Registration

Use Case #/ID	05	**Description**	Registration Client: New Registration
Initiating Actor	RegCenter Officer/ RegCenter Admin	**Other Actors**	-
Use Case Overview			
Registration process of a new applicant or pre-registered citizen			
Pre-conditions			
Once user logs in data sync should be done			
Business Rules			

- If user locked, he needs to run data sync process before starting new registration
- Full Name is a mandatory field and length should 0-120 characters
- Gender is a mandatory field and should be one of Male, Female, Other
- DOB is a mandatory field and should this format DD/MM/YYYY
- Address Line 1 to 3 are mandatory fields and length should be 0-50 characters each.
- Residential status is a mandatory field and should one of Non-Foreigner or Foreigner.
- National Identity Number (Reference Identity Number) is a mandatory field and length should 10-12 characters.
    - If National Identity Number character length is 10, First nine characters should be (0-9) numbers and last character should be V or X.
    - If Reference Identity Number character length is 12, all 12 characters should be numbers.
- Province is a mandatory field and should not be editable. Picked from master data.
- District is a mandatory field and should not be editable. Picked from master data.
- City is a mandatory field and should not be editable. Picked from master data.
- Postal code is a mandatory field and should not be editable. Picked from master data.
- Phone number is a mandatory field and should start with the country code (Ex: +94 for Sri Lankan numbers) and rest nine characters should be numeric. Total character length is 12.
- Email is a mandatory field and should contain only email addresses. Only “0-9”, “a-z”, “A-Z”. And in middle should contain “@” and “.”.
- Proof of Identity is a mandatory field for new identities
- Proof of Date of Birth is a mandatory field
- Proof of Exception is an optional field
- Applicant biometric is a mandatory field for new identities and should not be editable. Values should be:
    1. Iris
    2. Finger print scan of right hand (four fingers excluding thumb)

3. Finger print scan of left hand (four fingers excluding thumb)
4. Finger print scan of both hands (Thumb fingers only)
5. Face image

- Continue button should enable only after all required fields are properly captured

Main Event List/Flow of Events

Select new registration option

Enter Pre-Registration ID to retrieve demographic details and uploaded documents from Pre-Registration data

Enter Reference ID Number

Continue to Document Upload section

Add required proof documents

Continue to Biometric Details section

Add biometric details

Continue to Registration Preview section

Review details and agree to consent conditions

Continue to Authentication section

Enter authorized user credentials

Continue to Registration Acknowledgement section

Review and submit application

Alternate Event List/Flow of Events

1. IF Pre-Registration ID is not available

Select new registration option

Enter Demographic details

Enter Reference ID Number

Continue to Document Upload section

Add required proof documents

Continue to Biometric Details section

Add biometric details

Continue to Registration Preview section

Review details and agree to consent condition

Continue to Authentication section

Enter authorized user credentials

Continue to Registration Acknowledgement section

Review and submit application

2.1.6 Use Case 06: Registration Client: New Registration Approval

Use Case #/ID	06	**Description**	Registration Client: New Registration Approval
Initiating Actor	RegCenter Admin	**Other Actors**	RegCenter Officer
Use Case Overview			
All new Registration Applications must be approved by the Center Admin user.			
Pre-conditions			
New Application must be completed and submitted			
Business Rules			
- Applications must be approved one at a time, to ensure review of each application. - If user reject the application reject reason is mandatory.			
Main Event List/Flow of Events			
Open Registration Client application *Login using given username and password* *Select Pending Approval option* *Select New Application* *Review and continue* *Enter Supervisor credentials* *End approval process*			
Alternate Event List/Flow of Events			
Path 01 *If Reject the application* *Select reject button.* *Enter reject reason.* *Enter authenticate button* *Enter Supervisor credentials* *End approval process*			

2.1.7 Use Case 07: Registration Client: Logout

Use Case #/ID	07	**Description**	Registration Client: Logout
Initiating Actor	RegCenter Admin/ RegCenter Officer	**Other Actors**	-
Use Case Overview			
Once tasks are completed the user logs out.			
Pre-conditions			
User should be logged in to the system			
Business Rules			
- Log out current session of the user - If user is not active on the system for a pre-defined amount of time; automatically log out user from the session			
Main Event List/Flow of Events			
Select log out option			
Alternate Event List/Flow of Events			
Path 01 *If user is in-active on the system for a pre-defined amount of time* *Automatically Log out user*			

2.1.8 Use Case 08: Registration Client: Demographic Deduplication

Use Case #/ID	08	**Description**	Registration Client: Demographic Deduplication
Initiating Actor	RegCenter Admin/ RegCenter Officer	**Other Actors**	-

Use Case Overview

Demographic Deduplication is the process of comparing and verifying if the entered demographic details of a new entry is already available in the system and notifying the user of the data duplication error.

Pre-conditions

New Registration process must be completed

Business Rules

-

Main Event List/Flow of Events

System receives a request to perform a Demographic Data Deduplication
System compares the demographic details in the new entry with existing data
If no match is found; the registration is allowed to pass to the next stage

Alternate Event List/Flow of Events

Path 01
System receives a request to perform a Data Deduplication
System compares the demographic details in the new entry with existing data
If a match is found; the system checks if the match is true on the following conditions:

- *The entry must be a successfully completed registration*
- *The UIN must be generated*

If true; the potential match's biometric details are also compared with existing biometric data
If a match is found; the registration is rejected

Path 02
System receives a request to perform a Data Deduplication
System compares the demographic details in the new entry with existing data
If a match is found; the system checks if the match is true on all the following conditions:

- *The entry must not be a rejected entry*
- *The entry must be a successfully completed registration*
- *The UIN must be generated*

If true; the potential match's biometric details are also compared with existing biometric data
If no match is found; the registration is allowed to pass to the next stage

2.1.9 Use Case 09: Registration Client: Biometric Deduplication

Use Case #/ID	09	**Description**	Registration Client: Biometric Deduplication
Initiating Actor	RegCenter Admin/ RegCenter Officer	**Other Actors**	-

Use Case Overview

Biometric Deduplication is the process of comparing and verifying if the entered biometric details of a new entry is already available in the system and notifying the user of the data duplication error.

Pre-conditions

New Registration process must be completed

Business Rules

-

Main Event List/Flow of Events

System receives a request to perform a Biometric Data Deduplication

System compares the biometric data in the new entry with existing data

If no match is found; the registration is allowed to pass to the next stage

Alternate Event List/Flow of Events

Path 01

System receives a request to perform a Biometric Data Deduplication

System compares the biometric data in the new entry with existing data

If a match is found; the system checks if the match is true on any one of the following conditions:

- *The registration entry is not rejected and is still being processed*
- *The UIN has been generated*

If true; the registration is sent for Manual Adjudication for final decision to reject or not

Path 02

System receives a request to perform a Biometric Data Deduplication

System compares the biometric data in the new entry with existing data

If a match is found; the system checks if the match is true on any one of the following conditions:

- *The registration entry is not rejected and is still being processed*
- *The UIN has been generated*

If false; the registration is allowed to pass to the next stage

2.1.10 Use Case 10: Registration Client: UIN Generation

Use Case #/ID	10	**Description**	Registration Client: Unique Identification Number Generations
Initiating Actor	RegCenter Admin	**Other Actors**	-

Use Case Overview

Once a new registration entry completes the entire process and gets approved; a UIN is generated to uniquely identify the entry.

Pre-conditions

Demographic Deduplication process must be completed

Biometric Deduplication process must be completed

Business Rules

- UIN should not contain any alphanumeric characters
- UIN should not contain any repeating numbers for 2 or more than 2 digits
- UIN should not contain any sequential number for 3 or more than 3 digits
- UIN should not be generated sequentially
- UIN should not have repeated block of numbers for 2 or more than 2 digits
- The last digit in the number should be reserved for a checksum
- The number should not contain '0' or '1' as the first digit.
- First 5 digits should be different from the last 5 digits (example - 4345643456)
- First 5 digits should be different to the last 5 digits reversed (example - 4345665434)
- UIN should not be a cyclic figure (example - 4567890123, 6543210987)
- UIN should be different from the repetition of the first two digits 5 times (example - 3434343434)
- UIN should not contain three even adjacent digits (example - 3948613752)
- UIN should not contain admin defined restricted number

Main Event List/Flow of Events

System receives a request for UIN generation

System generates UIN for relevant registration entry

Alternate Event List/Flow of Events

-

2.2 Wireframes

2.2.1 Pre-Registration Application

1. Login Page

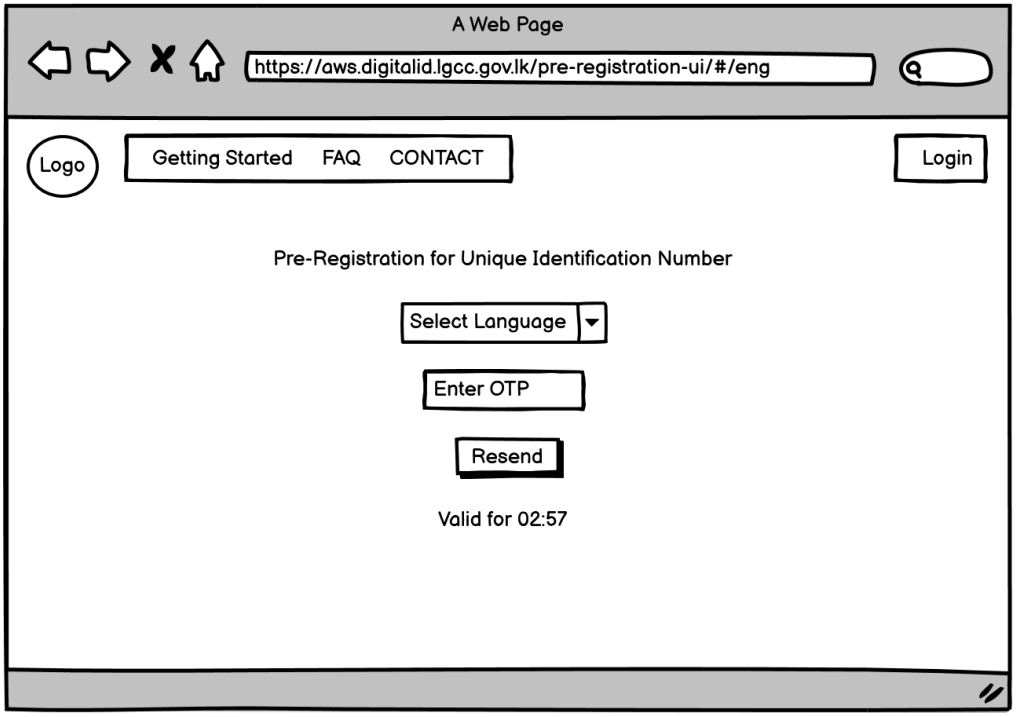

Figure 1: Pre registration - login page wireframe

2. Login Page Submit

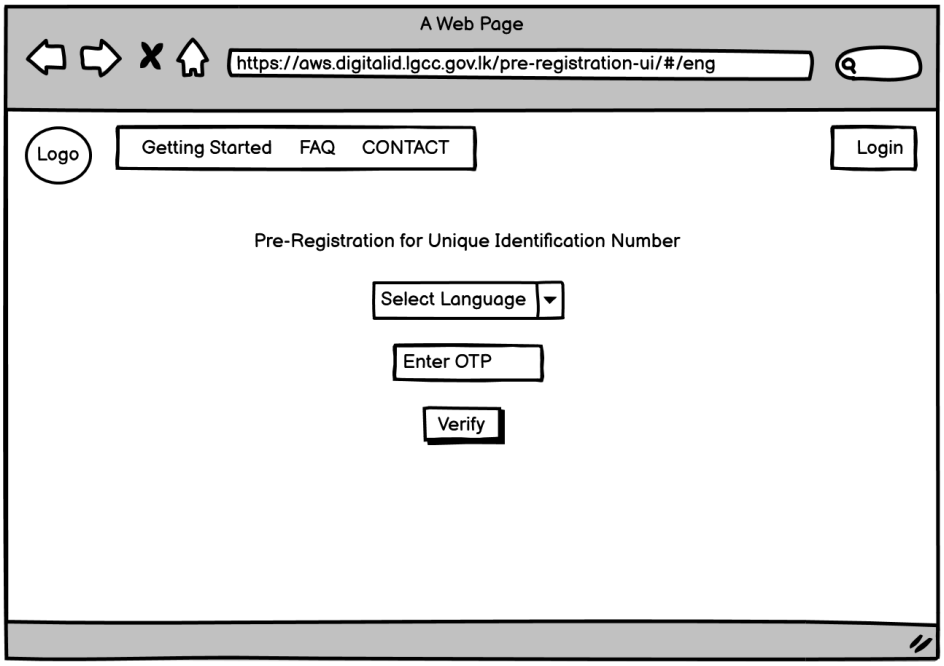

Figure 2: Pre registration - login page submit wireframe

3. Dashboard

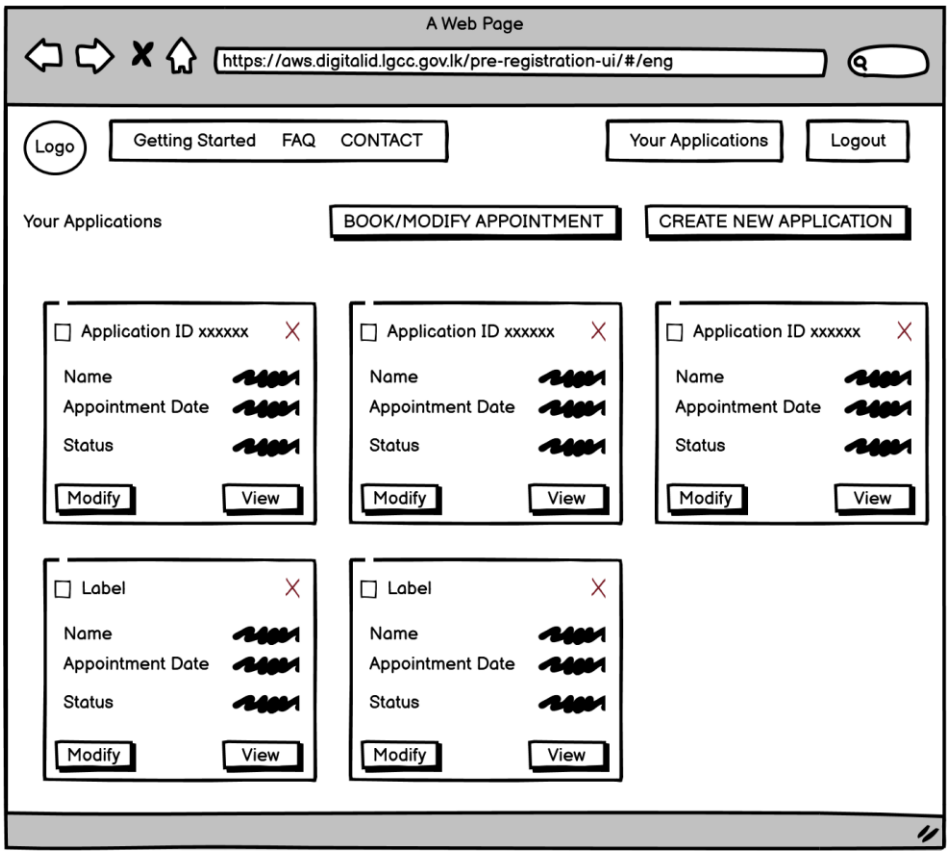

Figure 3: Pre registration - dashboard wireframe

4. Popup for Terms and Conditions

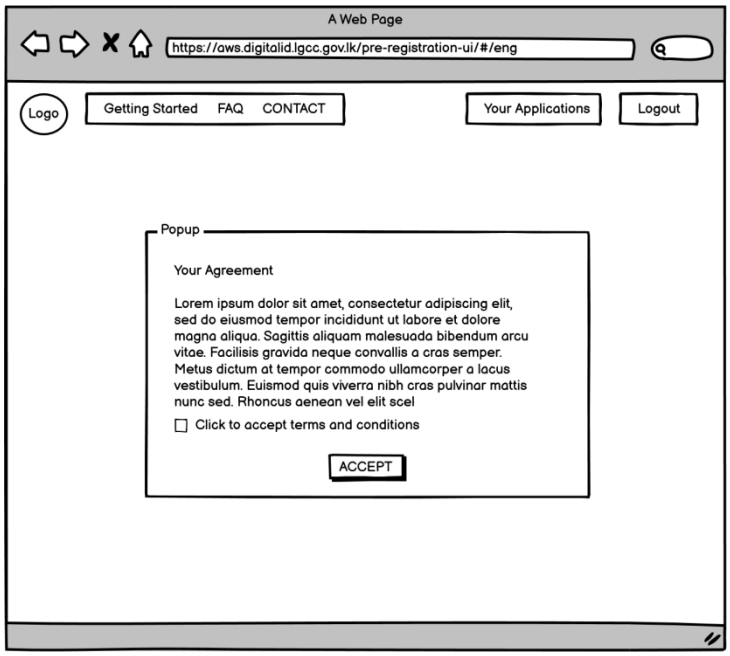

Figure 4: Pre registration - popup for terms and conditions wireframe

5. Details Form – Demographics

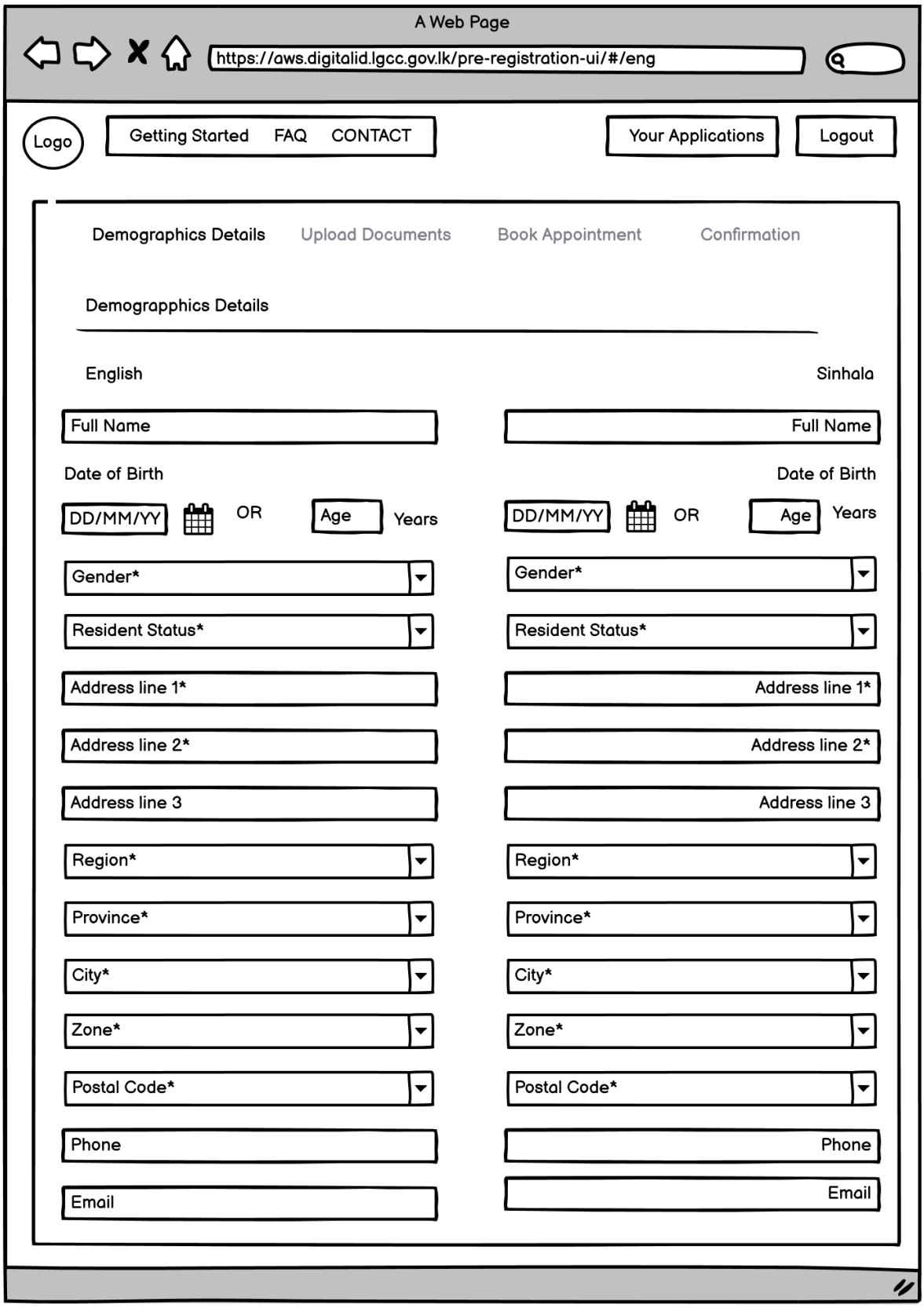

Figure 5: Pre registration - details form demographics wireframe

6. Details Form – Upload Documents

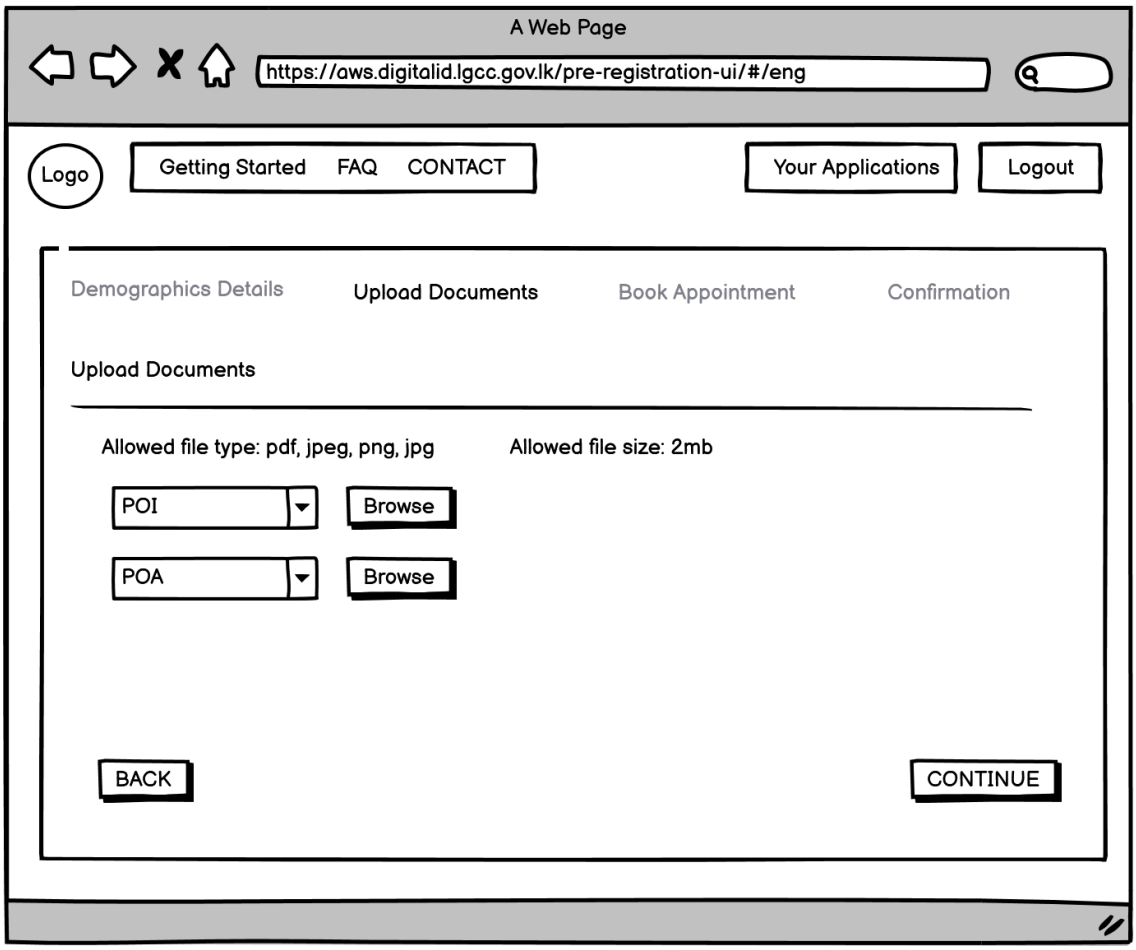

Figure 6: Pre registration - details form upload documents wireframe

7. Details Form – Personal Information

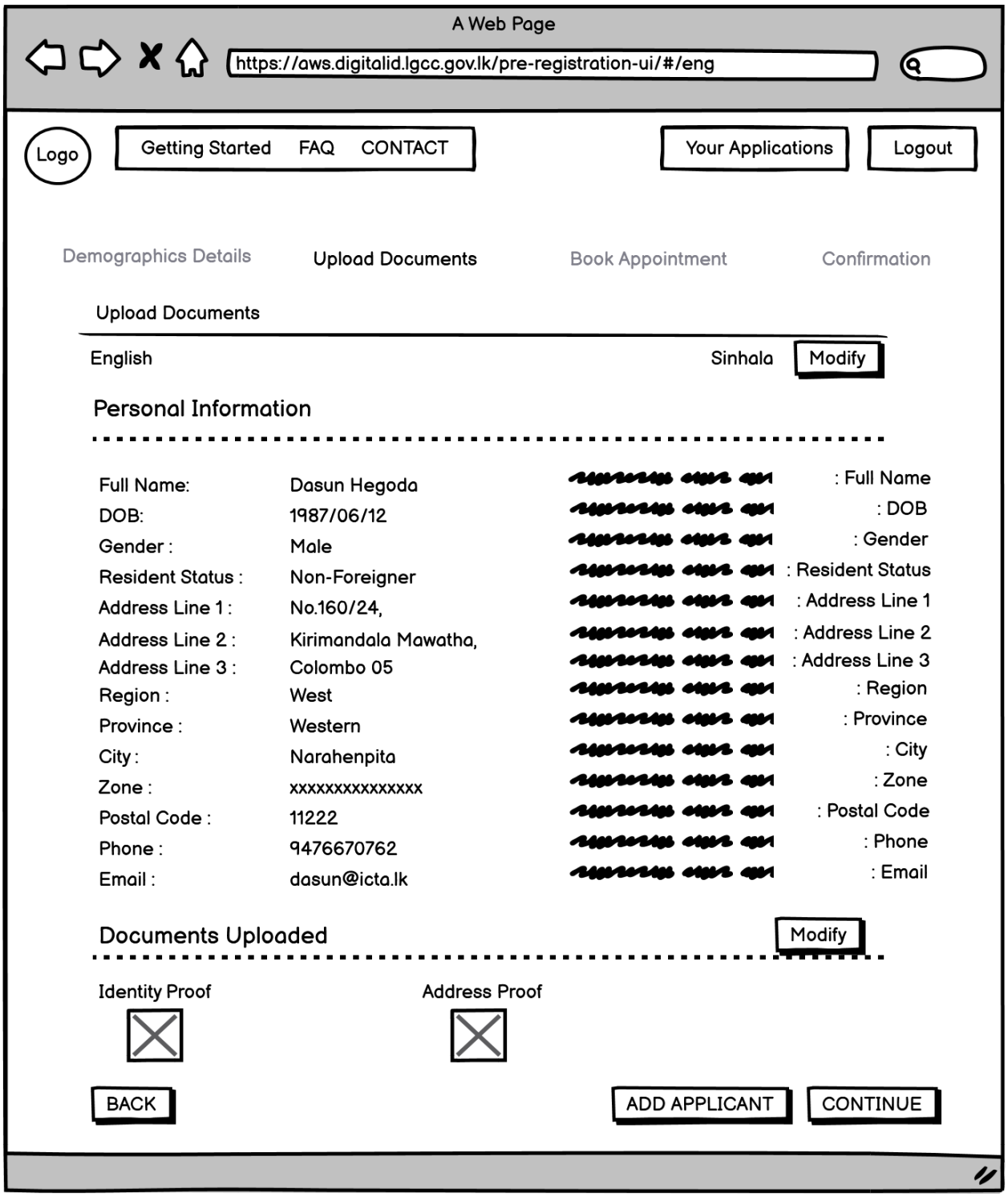

Figure 7: Pre registration - details form personal information

8. Details Form – Center Selection

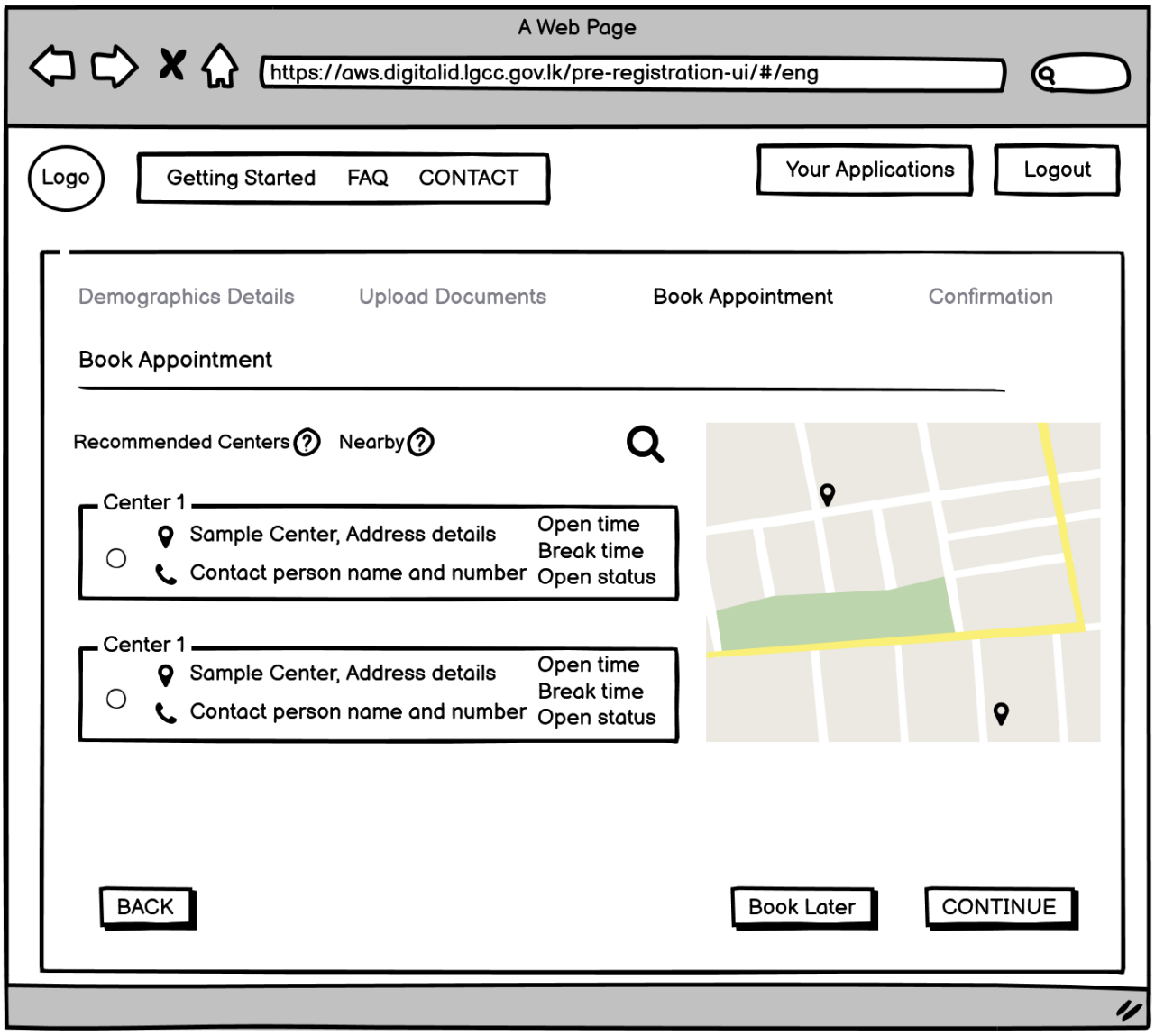

Figure 8: Pre registration - details form center selection

9. Details Form – Time Slot Selection

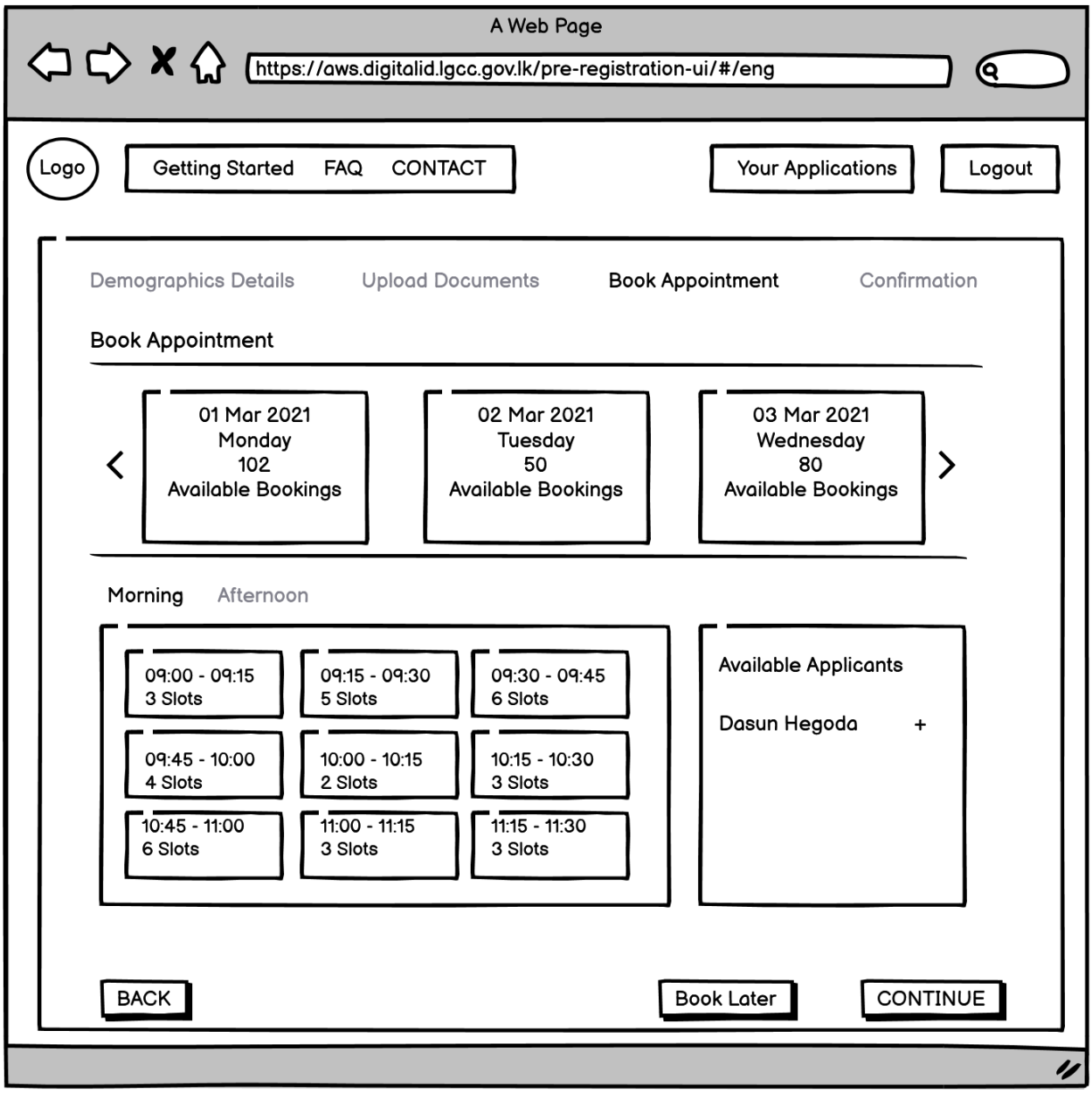

Figure 9: Pre registration - details form time slot selection

10. Details Form – Successful Booking Popup

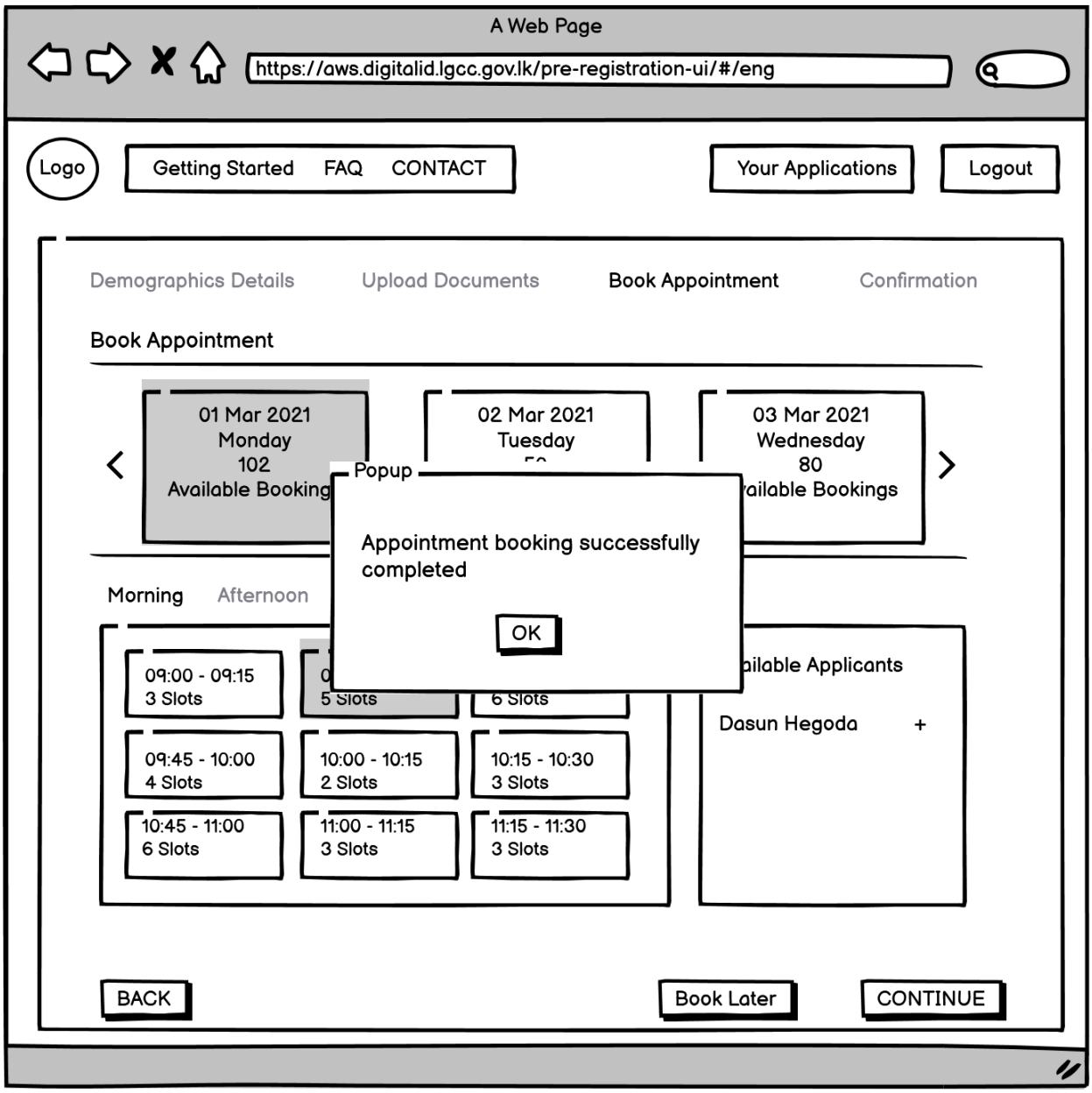

Figure 10: Pre registration - details form successful booking pop-up wireframe

11. Acknowledgement Page

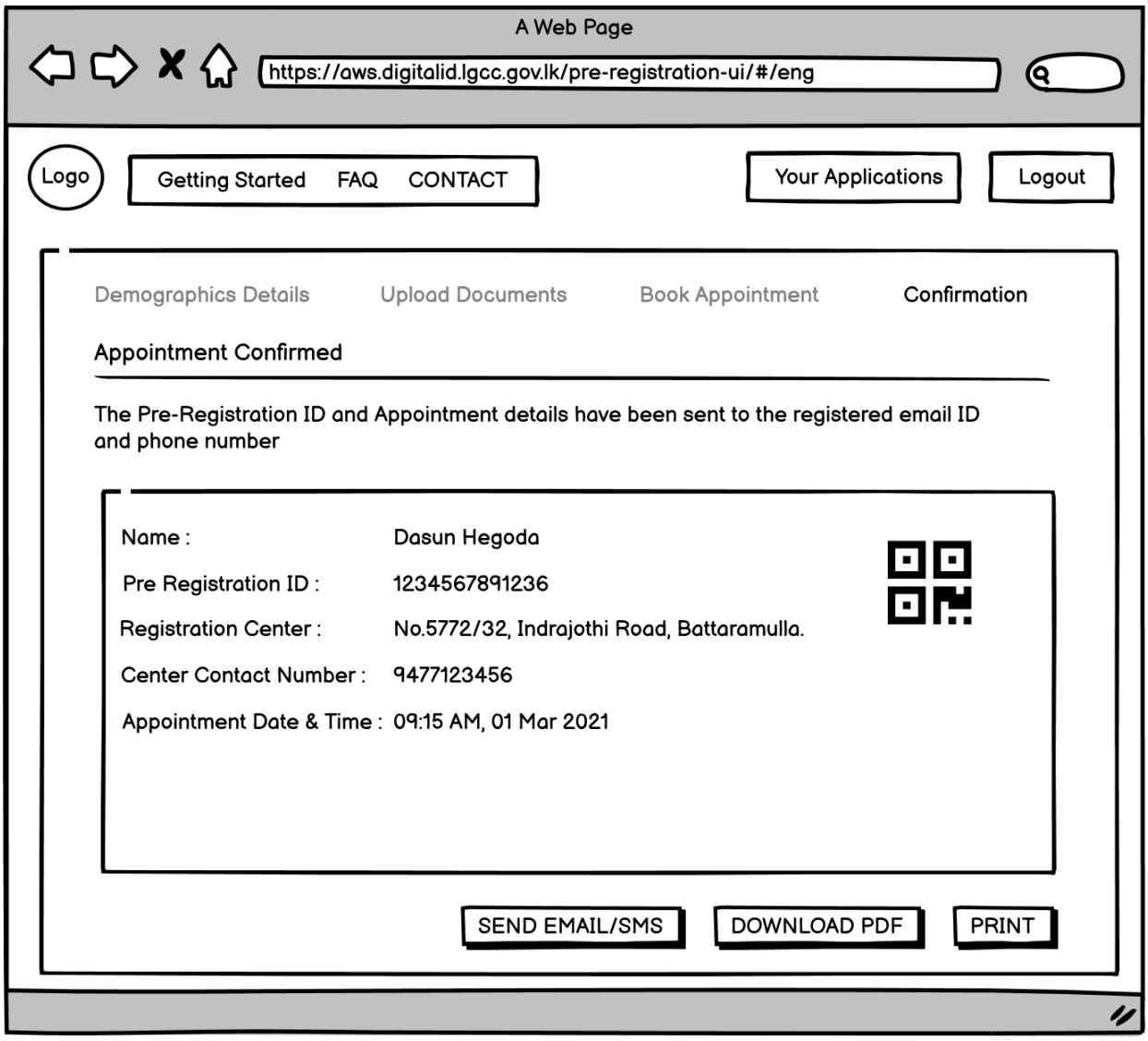

Figure 11: Pre registration - acknowledgement page wireframe

2.2.2 Registration Client Application

1. Dashboard

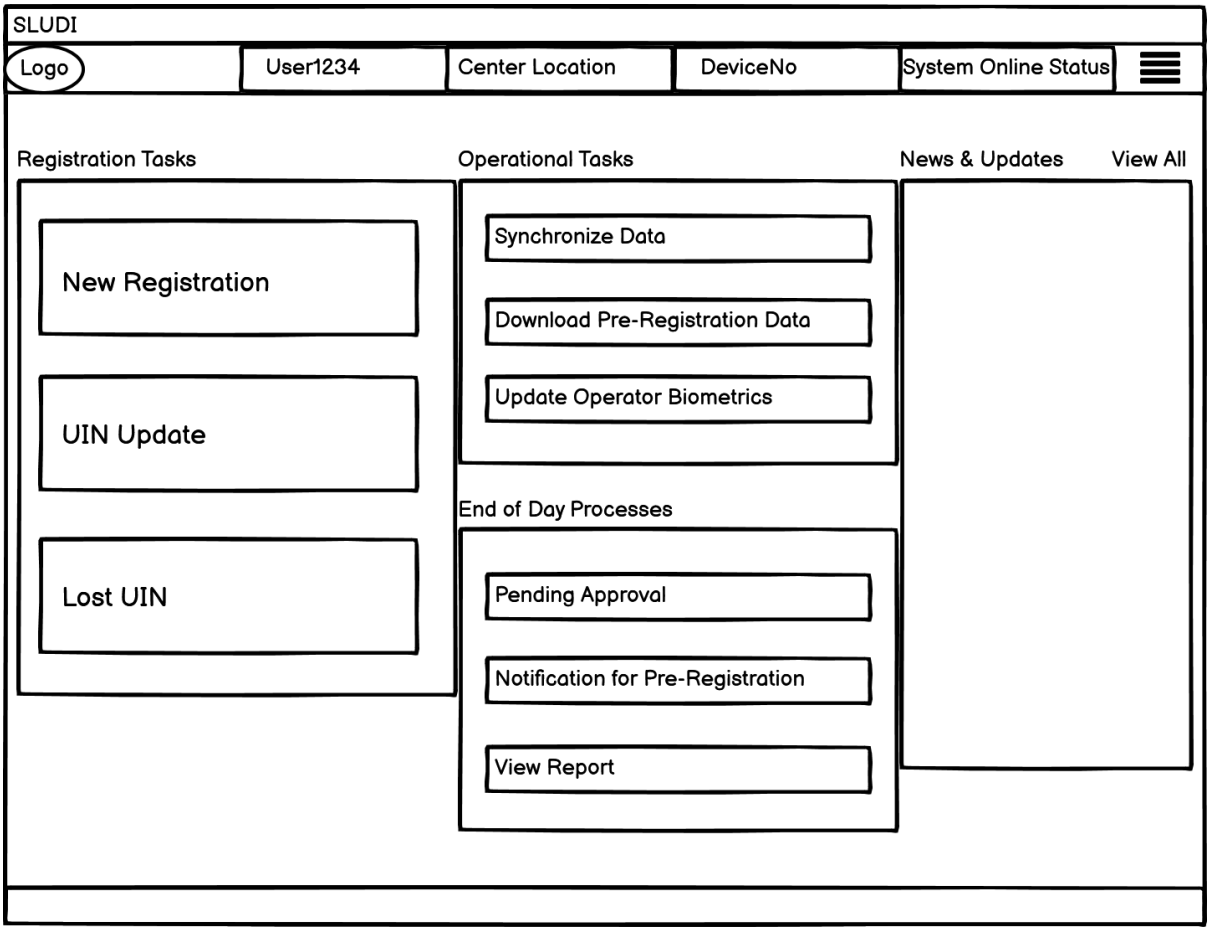

Figure 12: Registration - dashboard wireframe

2. New Registration - Demographic Details

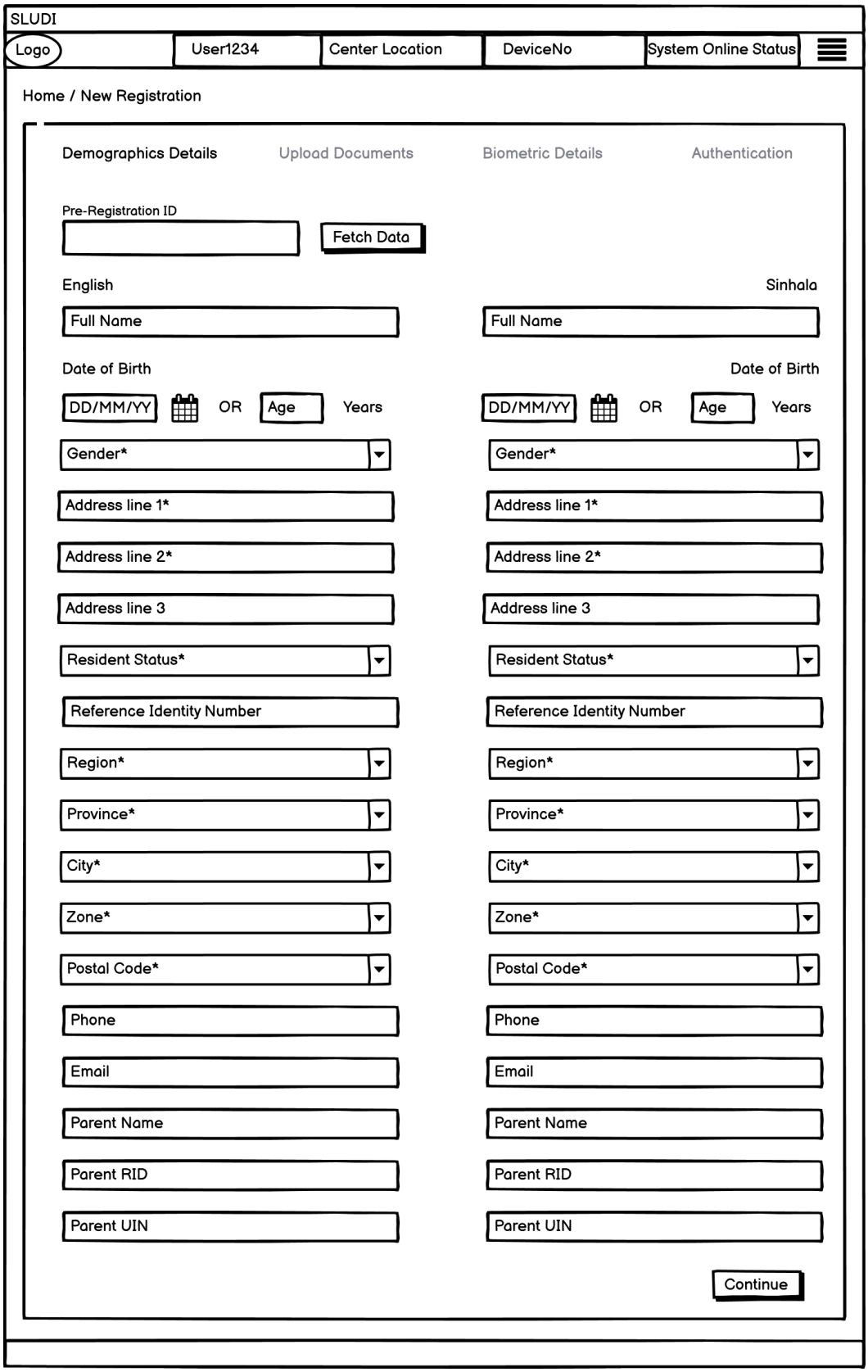

Figure 13: Registration - demographic details wireframe

3. New Registration - Upload Documents

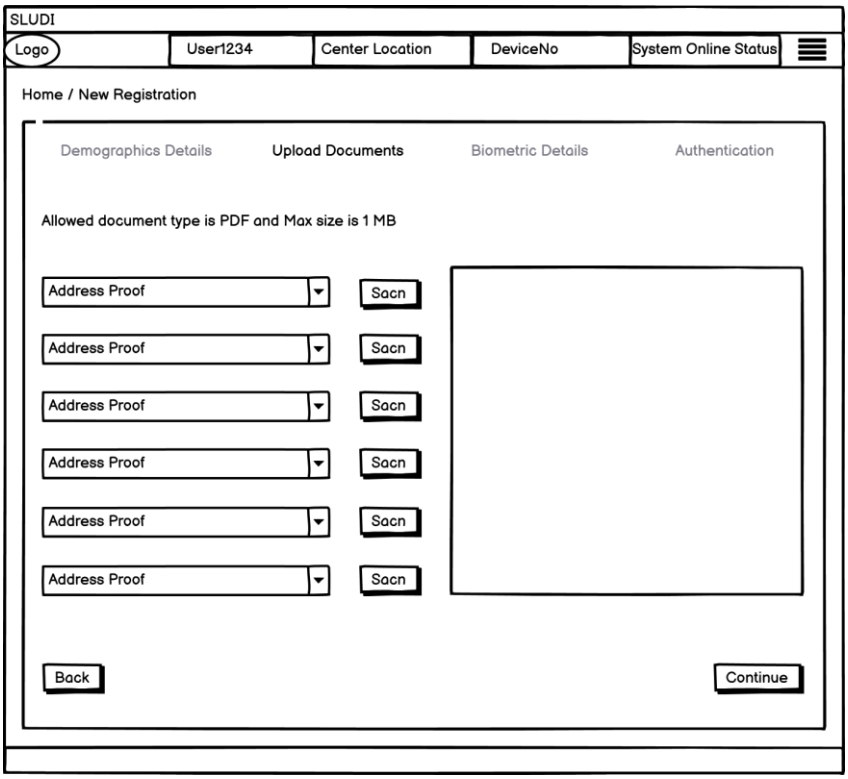

Figure 14: Registration – upload documents wireframe

4. New Registration - Upload Documents _ Scan Popup

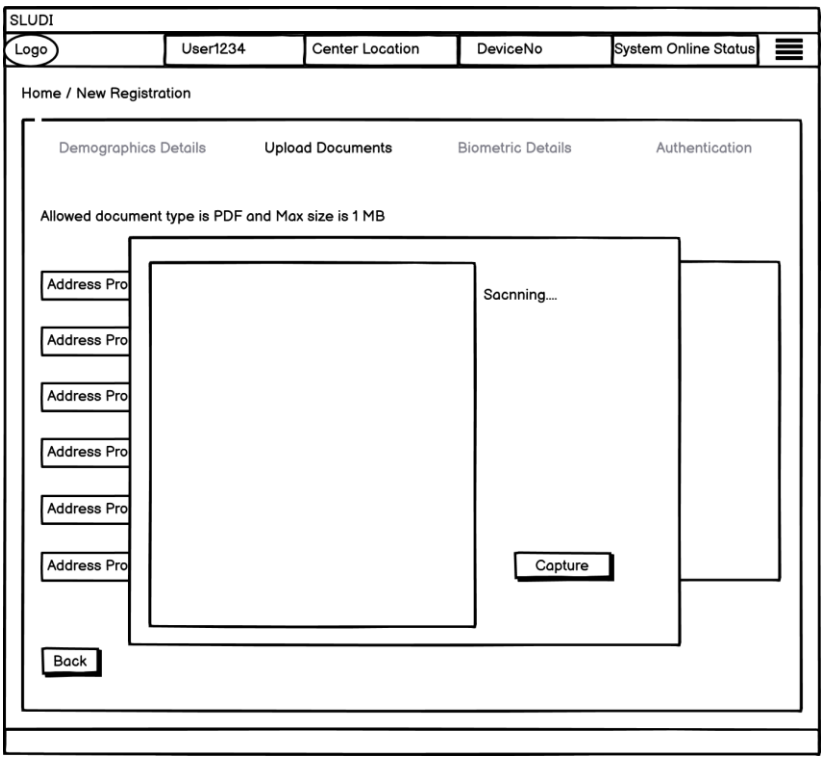

Figure 15: Registration – upload documents scan popup wireframe

5. New Registration - Upload Documents _ Scan Successful Popup

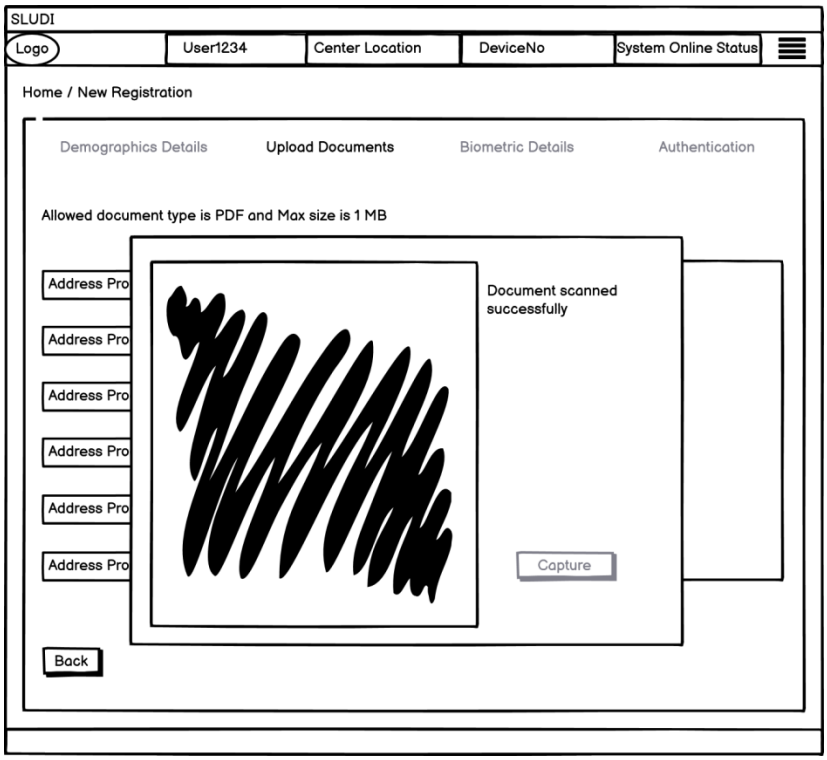

Figure 16: Registration – upload documents scan successful popup wireframe

6. New Registration - Biometric Details

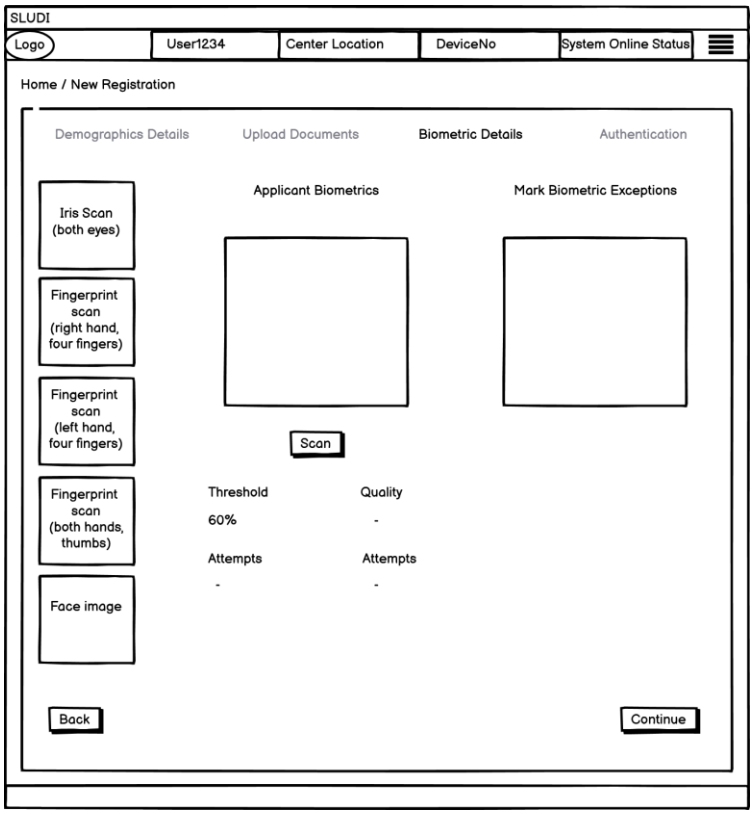

Figure 17: Registration – Biometric details wireframe

7. New Registration - Biometric Details _ Scan Popup

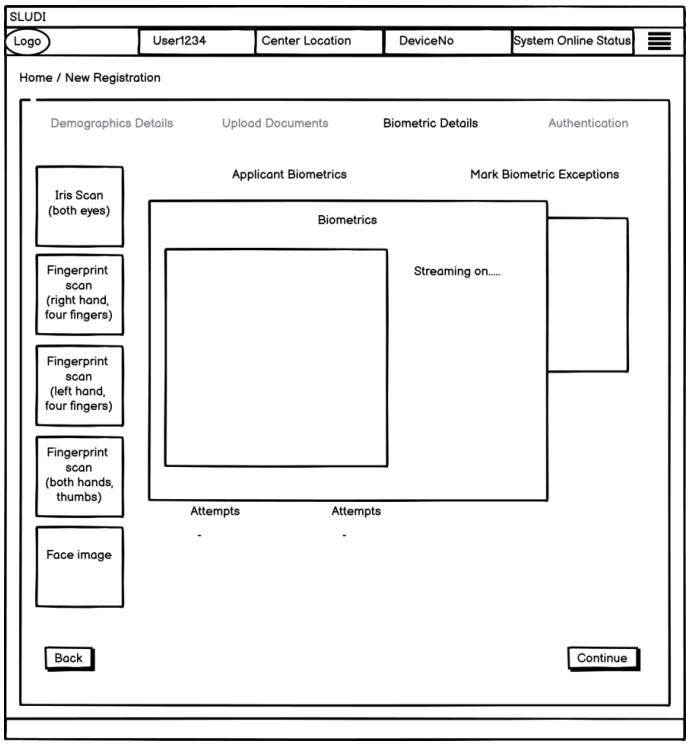

Figure 18: Registration – biometric details scan popup wireframe

8. New Registration - Biometric Details _ Scan Successful Popup

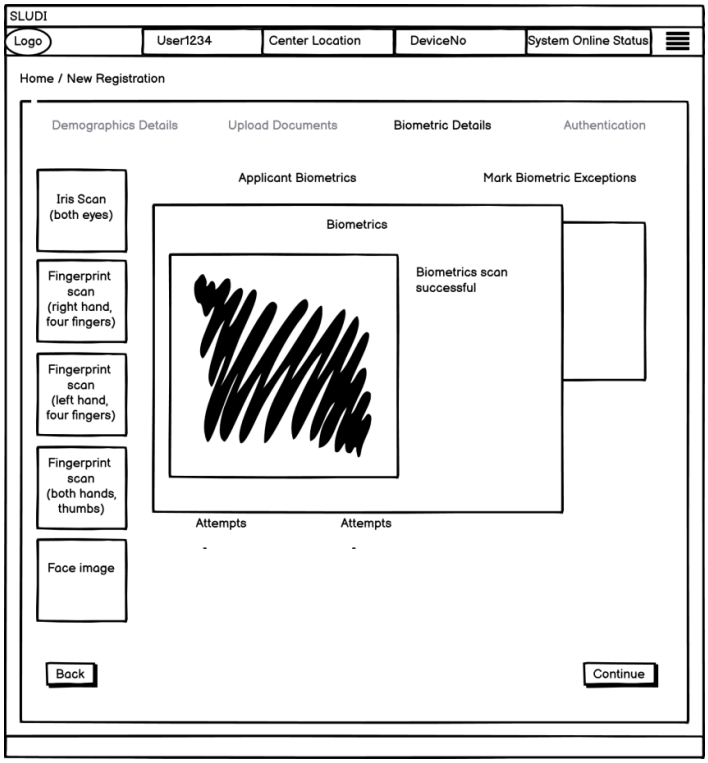

Figure 19: Registration – biometric details scan successful popup wireframe

9. New Registration - Registration Preview

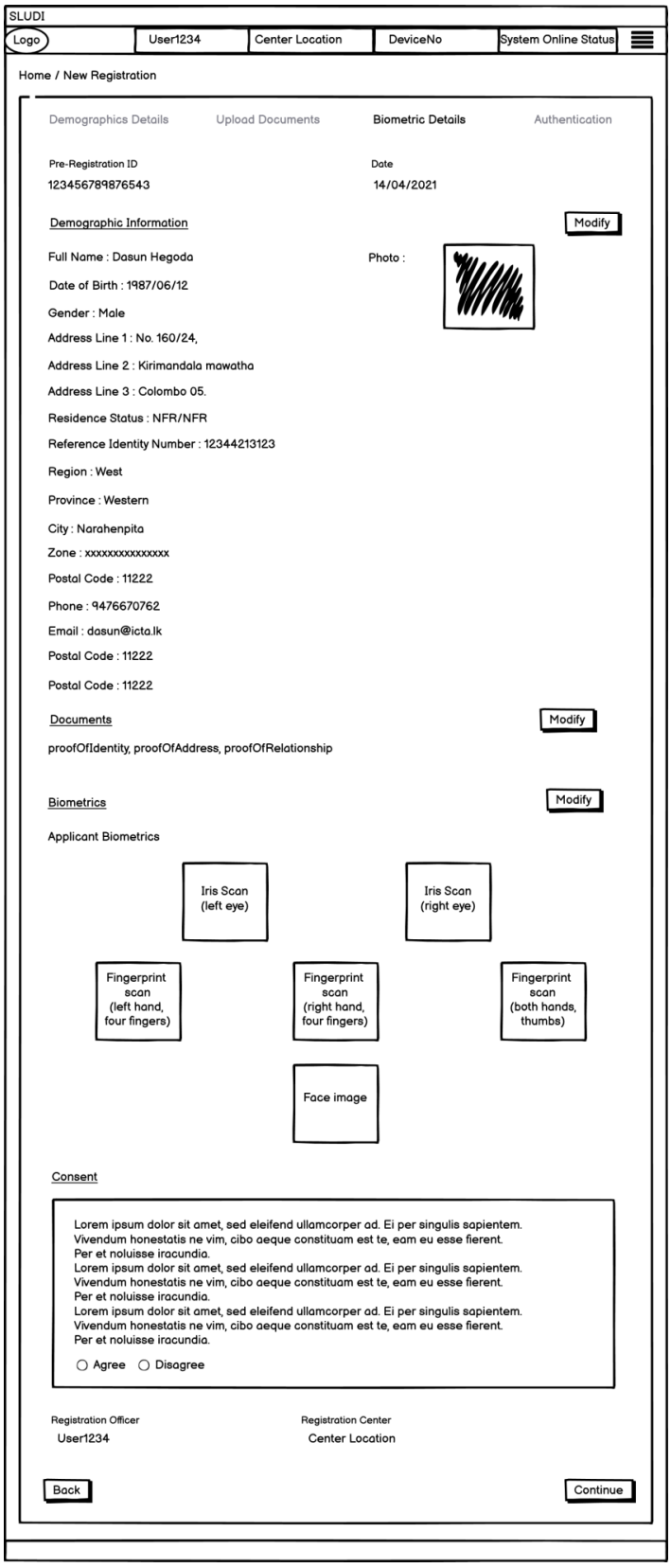

Figure 20: Registration – registration preview wireframe

10. New Registration – Authentication

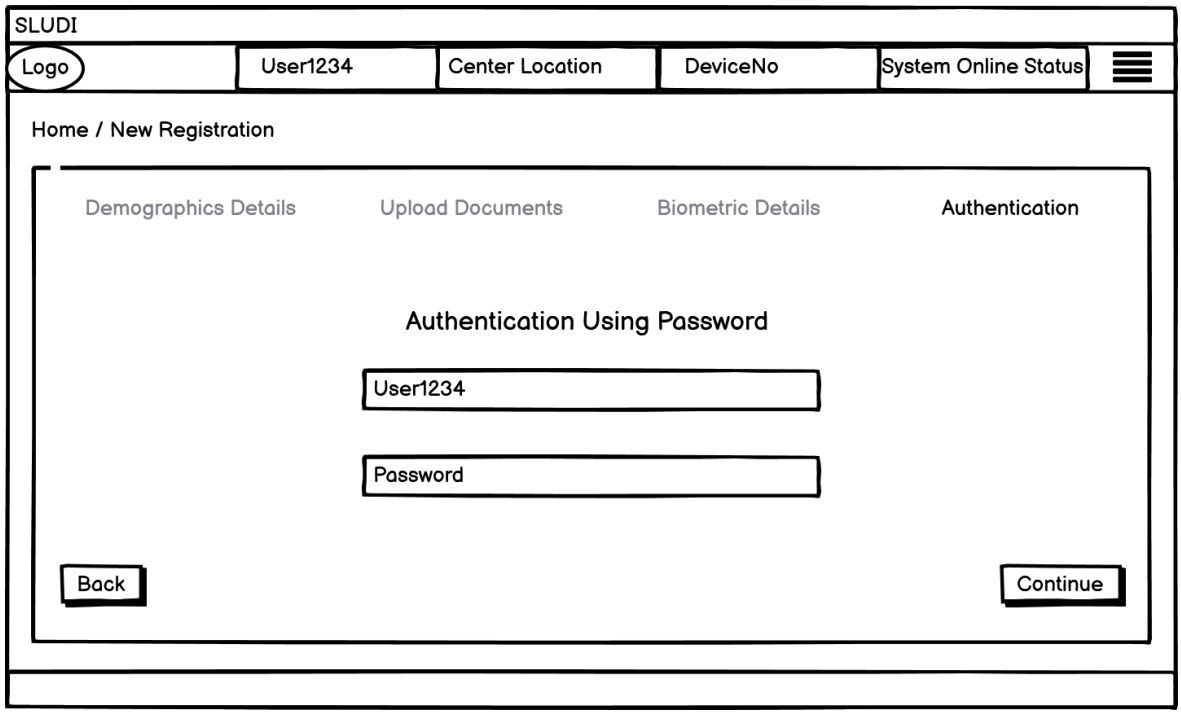

Figure 21: Registration – authentication wireframe

11. Registration Acknowledgement

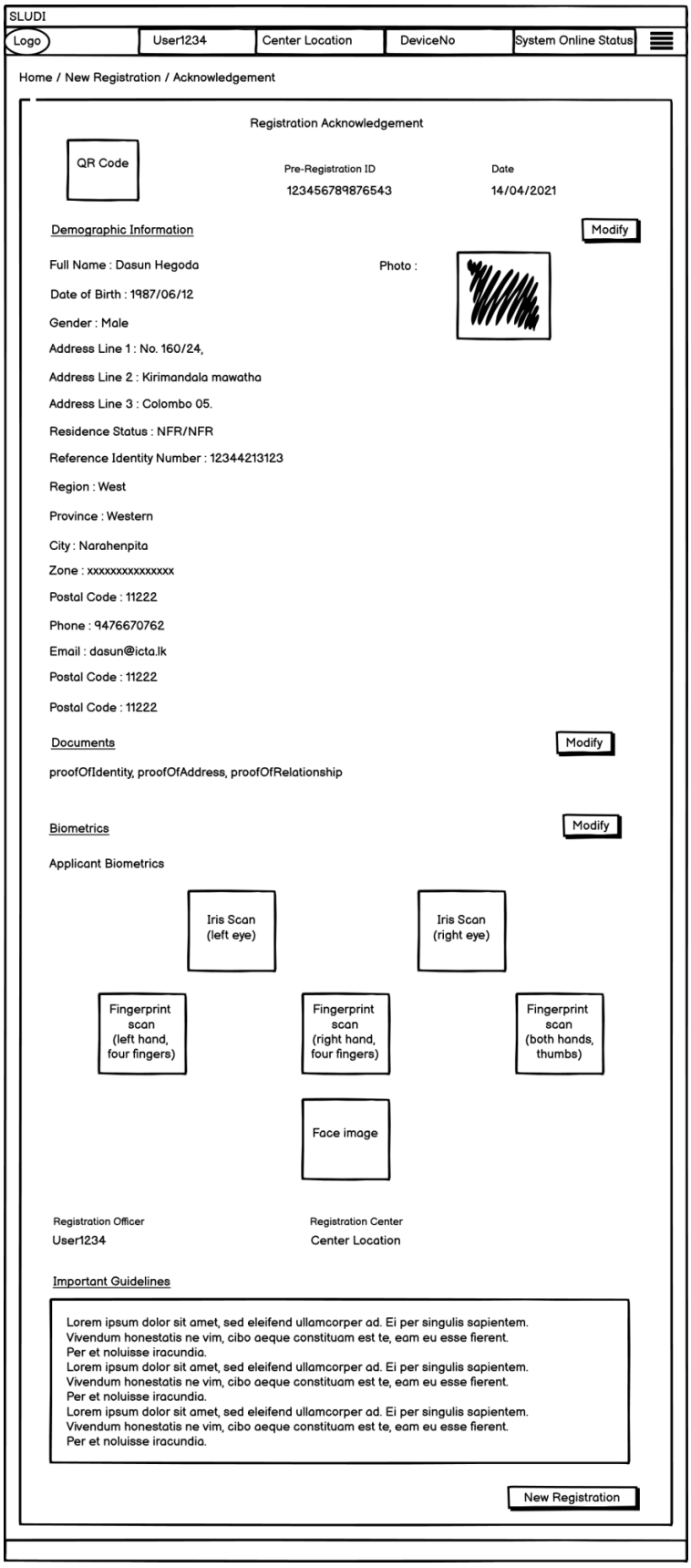

Figure 22: Registration – registration acknowledgement wireframe

12. Pending Approval

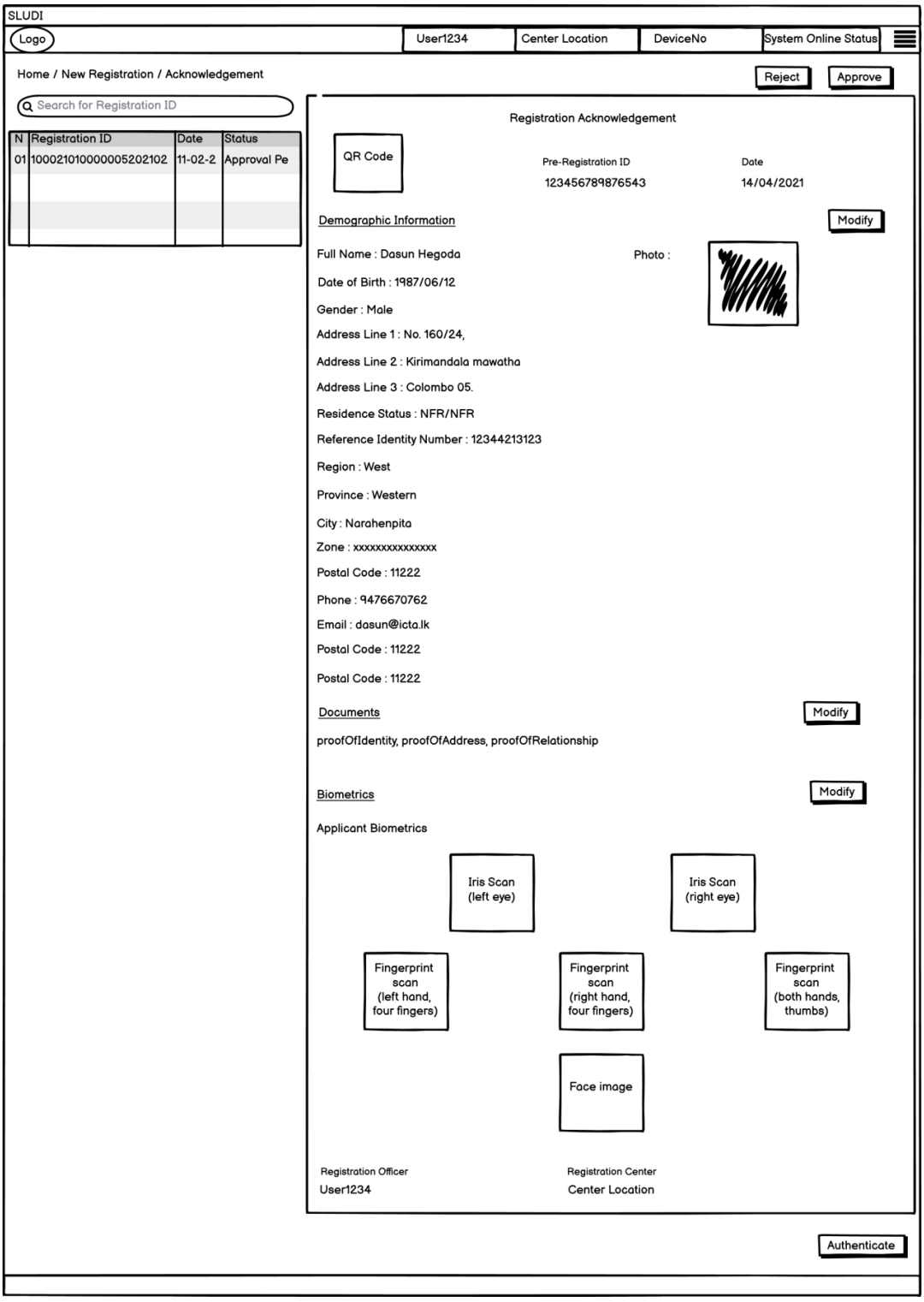

Figure 23: Registration – pending approval wireframe

13. Pending Approval - Supervisor Authenticate Popup

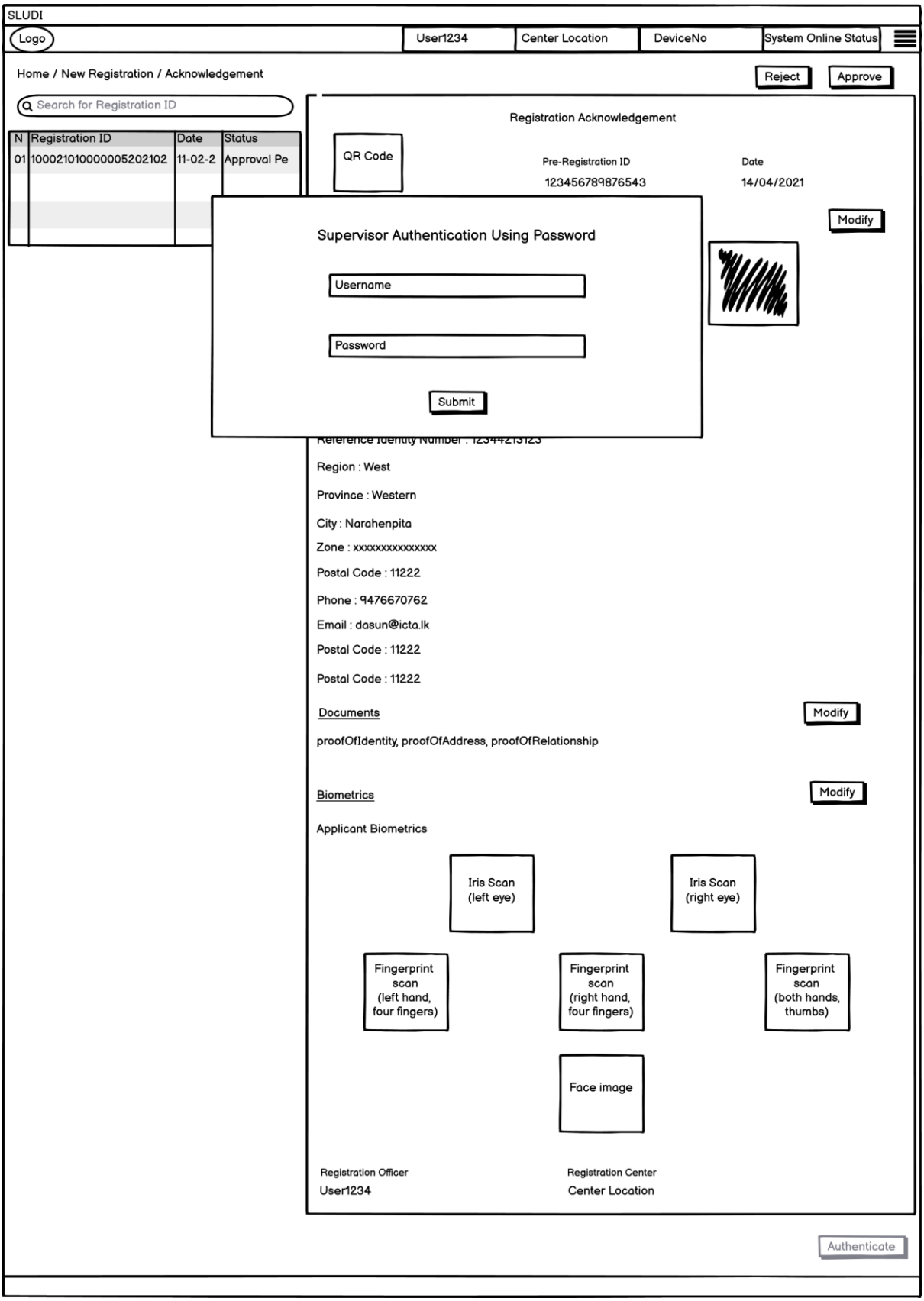

Figure 24: Registration – pending approval supervisor authenticate popup wireframe

3 Non-Functional Requirements

3.1 Trust Privacy and Security

The establishment and operation of the UDI POC system requires putting in place an elaborate set of safeguards that fall under the heading of trust, privacy, and security. Collectively, these are intended to ensure that the system operates within the boundaries of the law, does not violate people's rights, and is protected from abuse, risks, and vulnerabilities, so that it can earn the confidence of those who rely on it.

3.1.1 Trust

Paramount for the success of UDI POC is, earning the trust of all stakeholders that relies on it. This includes the citizens whose identity is managed by the UDI and the public and private sector entities who rely on UDI to authenticate and provide KYC data to carry out their operation. Hence it is of utmost importance UDI to pay due attention to build and retain the trust; this section details the important factors that the program needs to address.

No.	Trust Element	Key Consideration
1.	Registration Integrity	This is a crucial element in the chain of trust. The registration process should ensure that only legitimate identities are able to enroll. Required Measures: • Assurance of captured data integrity at the enrollment centers and during transmission to prevent alternations, substitutions, or other manipulations. • When using biometrics, controlling captured image quality as measured metrics such as NIST NFIQ for fingerprints or ICAO face image quality 19794–5. If image quality is not kept high, fraud perpetrators could attempt evasion by intentionally providing bad-quality samples, since match accuracy is directly related to quality. • Matching accuracy of ABIS, if used, in the backend system should be high enough that (together with deterrence) it can lead to practically zero duplicate enrollments.
2.	Trusted Credential	The digital credential as well as the physical proxy should be virtually impossible to fabricate outside the NIA process. Required Measures: • Mature and consistent information security, digital signature, certificate management, and encryption practices that leave no loopholes.

		• Minimum security requirements for any medium that will carry the credential, such as smartcards or mobile phones.
3.	Identity Assurance	Relying parties need to be assured that the person conducting a transaction is who he claims to be and not someone who stole a legitimate identity. Required Measures: Strong authentication: multifactor or biometric 1:1 match.
4.	Combating Malfeasance (Human Factors)	Preventing the issuance of true-false identity, where a human operator could issue a genuine document for a false identity due to bribe or coercion. Required Measures: • Supervised procedures and technology to limit the ability of enrollment agents to fabricate fake enrollment data (often by presenting the wrong sequence of fingers, or by mixing and matching fingers from multiple people, including their own as they reconstitute the 10-print). • Internal controls at the DRP/UDI to ensure that no single operator is capable of surreptitiously modifying or enrolling identity records without supervisor approval. • A higher standard for screening of new hires and ongoing monitoring of agents.
5.	Data Protection and Security	The public should be assured that their data at the UDI is protected against unauthorized access, including external (hacking), internal (rogue employee), as well as organized mission creep. Required Measures: • Information security measures that emphasize strong data rights management. • Physical security measures to protect data centers. • Identity data segregation. • Enforced internal policy and procedures for access. • Public policy on data use. More details on Security measures are provided in Section 5.1.3
6.	Trust Model	Underlying the UDI program, there is a technology for trusted communication. This includes enabling authentication for access to online services, digital signature for commitment and non-repudiation, and encryption to secure transmission of transactions. Not only technical measures have to be in place, but also clearly defined responsibilities and

		liabilities of the authority providing this trust (e.g., CA) should be set in a Legal Act.

Table 2: Non-functional requirements – trust section

3.1.2 Privacy

Data privacy is challenging since it attempts to use data while protecting an individual's privacy preferences and personally identifiable information. Privacy is the ability of an individual, group, or individuals or entity to free itself from being observed information about them with due consent.

UDI generates sensitive data during enrollment and when it is used to enable the actions of its holder (audit trail of transactions). More precisely, eID evokes privacy concerns primarily for the following reasons:

1. Enrollment Data: the UDI registration process requires the collection of significant amounts of personally identifying information (PII) for validation and vetting,
2. The Central Database: not only does a UDI system capture PII during enrollment, but it also consolidates that data into central repositories to guard against duplicative registration and to deliver identity services.
3. UDI Number allows data correlation: the use of the Unique Identity Number as an administrative tool to manage identity evokes privacy concerns since it enables the linking of disparate information about an individual across databases, which a priori are not linked.
4. Digital Audit Trail: Over time, if UDI is successful, it would become pervasive; it would enable a dominant number of the population's daily actions.

Protecting user data privacy is a key requirement for UDI and is of utmost importance for the overall success of the program. Hence the program needs to consider the measures outlined below to avoid any privacy concerns.

No.	Trust Element	Key Consideration
1.	Legislation	The systems should be in compliance with GDPR and the Data Protection Act of Sri Lanka. Several obligations have been imposed by this legislation on those who collect and process personal data ("Controllers" and "Processors") and whole new set of rights have been given to citizens under this new legislation, which are known as "Rights of data subjects". • UDI specific Legal Acts: Implement where necessary UDI specific legal acts to reiterate or introduce new bodies of legislation that explicitly provide privacy protection to people.
2.	Access and Data Protection	The protection of identity data and limiting its use, using technical measures: • Data rights access management. • Anti-data retention measures (e.g., retention of audit trail data only for the period required by law for

		non-repudiation). • Use limitations.
3.	Notice	• Individuals' right to have noticed regarding the data gathered about themselves and the right to know how and for what purpose it will be used. This may be required by law, or it may be good practice for all eID processes (enrollment, use). • Clear, meaningful, and prominent notice when collecting identifying data (iconic plus information link).
4.	Consent/Choice	The individual's right to consent to the collection and use of their personal data.
5.	Privacy by Design	These include privacy-enhancing technologies and measures such as: • Data minimization and proportionality: capture data in proportion to risk. • Identity data segmentation and segregation: e.g., store identifiers separately from PII. • Do-not-track (DNT). • Right to be forgotten. • Right to view. • Pseudonymous, or anonymous transaction management (Trusted Agents).
6.	Privacy Policy and Support Framework and Enforcement	Implementation of program-specific (UDI program-wide), as well as specific applications privacy policy to create awareness and implant the importance of privacy. An independent body that reports directly to the legislative body (parliament) and acts as an advocate for privacy rights, with powers that include: • Investigate complaints, conduct audits, and publicly report on the privacy practices of public and private sector organizations. • Educate the public regarding privacy.

		• Pursue legal actions for violations, where supported by law. Meaningful legal instruments and mechanisms that provide sanctions for noncompliance. Enforcement is not necessarily limited to the scope of action of the Privacy Commissioner's Office.

Table 3: Non-functional requirements – privacy section

3.1.3 Security

At a basic level, an eID program is an information system that is supposed to secure online human interactions. As such, in addition to the measures needed to build trust and respect privacy, as discussed above, the information system requires sound information security safeguards that mitigate against the risk of breach and other operational vulnerabilities, spanning areas of legislation, governance, technology, and operational control.

At a basic level, an eID program is an information system that is supposed to secure online human interactions. As such, in addition to the measures needed to build trust and respect privacy, as discussed above, the information system requires sound information security safeguards that mitigates against the risk of breach and other operational vulnerabilities, spanning areas of legislation, governance, technology, and operational control.

User authentication and authorization

An administrative web application needs to be developed to manage users and permissions.

Confidentiality and Integrity

All developed web applications should ensure "confidentiality" and "integrity" whenever required by adhering to transport and message-level security standards. (i.e., HTTPS, WS-Security)

Authentication

The web application should be able to verify users.

Users will be authenticated based on an identifier/secret pairing (An username/password combination). The authentication service has decoupled using JWT tokens, and there is no persistent session between server and client. User access and executes services with JWT token.

Authorization

The web application should be able to verify that it allowed users to have access to resources.

Role-Based Access Control (RBAC) will be used to ensure the operation of the solution will be restricted and tightly controlled users with relevant permission levels. Domain logic rules that apply to specific functional scenarios will also adhere. Even though there are roles, it only restricts users' login to different consoles. Authorization happens based on the JWT claims.

Non-repudiation

All Web applications should ensure non-repudiation by having standard audit-trails and provisions to have digital signatures.

OWASP Guidelines

Open web application security project guidelines (OWASP) will be followed to protect from typical web attacks. The scope of testing will be limited to the most common web attack vectors, as identified by OWASP.

Auditing

The operations listed below will be audited as a means of tracing actions/manipulation of data within the solution:

No.	Operations	Audit Storage	Mandatory Log Entry	Remarks
1.	Data Capture & Maintenance	Diagnostics Database	Yes	
2.	Creation of Entry or Item	Diagnostics Database	Partial	Can be done selectively, where performance may be affected.
3.	Modification of an Item	Diagnostics Database	Partial	Can be done selectively, where performance may be affected.
4.	Deletion of an Item	Diagnostics Database	Partial	Can be done selectively, where performance may be affected.
5.	Control or Status Change	Diagnostics Database	Yes	
6.	Process Execution	Diagnostics Database	Yes	
7.	Data Synchronization	Diagnostics Database	Yes	
8.	Print (only selected items)	Diagnostics Database	Yes	
9.	Retrieval	Diagnostics Database	Yes	This should be done selectively. Auditing on retrieval may impact performance.

10.	Monitoring	Logs and Diagnostics Database	Partial	Can be done selectively.

Table 4: Security – auditing

Data is inclusive of (but not exclusive to) the executing thread identifier, timestamp, client IP address, client user-agent, server (internal) IP address must be stored per audit entry, where relevant.

Encryption

Transport-level encryption is mandated across system/environment boundaries; hence, HTTPS will be used for external communications. Confidential data will be encrypted where relevant, using encryption keys applicable to the context of the data (i.e., application-level, user-level, session-level).

NOTE: encryption will render encrypted data fields non-searchable.

Hashing

Passwords will not be stored in a recoverable format, but will be 'salted' based on a randomized seed and hashed for storage so that not even administrators can view the raw password itself. All variables related to this process will be provisioned via the context of the data being secured (i.e., application-level, user-level, session-level).

Digital Certification

Public Key Infrastructure (PKI) using digital certificates provided by a trusted Certification Authority (CA) can be used for non-repudiation. This mechanism may also be used to identify the solution to third parties when consuming external services.

3.2 Audit facilities

Wherever applicable, an audit trail of all activities must be maintained. On service or operation being initiated, the system should log the event, creating a basic 'audit log entry.' It should not be possible for the operation to be executed without the log entry being made.

The information recorded in the audit trail depends on the type of activity which takes place. Each service would be responsible for logging detailed information. The different types of operations are

- Data Capture & Maintenance
- Creation of an entry/item
- Modification an item
- Deletion
- Control (or status change)
- Process execution
- Data synchronization
- Print (only selected item)
- Retrieval
- Monitor

Detail logging may be enabled or disabled for each type of operation, and/or for each business object. It should be possible to configure which attributes of a data item should be traced at the detail level. Tracing of some attributes may be considered mandatory, and they should not be turned off.

3.3 Availability/Reliability

3.3.1 Redundancy & Failover

Redundancy is the fault-tolerance technique used to increase the availability of the application where a secondary node of hardware/software takes over when the primary node fails. The redundancy and failover method will be defined in the design phase based on service type and requirements. The system should be reliable, with high-quality performance and minimum or no down-time.

3.3.2 Failure Detection

This should be designed in a manner to attempt recovery where and when it is possible. And if recovery is impossible, to fail gracefully - by ensuring transaction semantics (typically via rollback), making the required diagnostics/audit entries, and performing clean-up activities like closing connections, etc.

3.3.3 Fault Tolerance

This illustrates that the failure of the system (be it due to hardware, software, or networking issues) will result in visitors to sites being not able to visit the site. Thus it is recommended that a manual process be retained on standby (at least for critical processes).

3.3.4 Performance Testing

Please find the below index as a guide to determine the benchmark values for the Application under the test.

Approach to Optimization in Development

The performance of the solution should be enhanced by cashing master/reference data to minimize database access. Indexes should be created in the database to enable the rapid retrieval of data.

The following performance criteria are provided as a guideline only. If the actual performance is falling below the stipulated figures, the consultant is to justify the reasons. However, the performance level must be accepted by the technical evaluation committee appointed by the ICTA. The bandwidth is assumed at 1mbps (shared) with 1,000 concurrent users (50% load factor) in total.

Item	Performance
Screen Navigation: field-to-field	< 5 milliseconds
Screen Navigation: screen-to-screen	< 3 seconds
Screen Refresh	< 3 seconds
Screen list box, combo box	< 2 seconds
Screen grid – 25 rows, 10 columns	<3 seconds
Report preview – (all reports) – initial page view (if asynchronous)	< 40 seconds in most instances. It is understood that complicated / large volume reports may require a longer period

Simple inquiry – single table, 5 fields, 3 conditions – without screen rendering	< 4 seconds for 100,000 rows
Complex inquiry– multiple joined table (5), 10 fields, 3 conditions – without screen rendering	< 6 seconds for 100,000 rows
Server-side validations / computations	< 10 milliseconds
Client-side validations / computations	< 1 millisecond
Batch processing (if any) per 100 records	< 120 seconds
Login, authentication, and verification	< 3 seconds
Daily backups (@Dept.) – max duration	1 hour (on-line preferred)
Total Restore (@Dept.) – max duration	4 hours

Table 5: Non-functional requirements – availability/reliability – performance testing

Performance Test Process Outputs

- Performance Test Scripts
- Performance Test Results

3.4 Usability

The web application should be extremely usable; even a greenhorn user should be able to handle the system and incorporate all the functionality of the system in a simple and user-friendly interface. The web application should be internationalized and localized if needed. The web application should be responsive, where it should be viewable on any computing device.

One of the main focus of the solution design will be to enhance the productivity of the end-users by following User Experience best practices. This will range from workflow design (minimizing the time taken to complete a task) to the design of screens (which will make using the application a pleasant experience).

3.5 Interoperability

The web application should be able to view in standard compatible web browsers.

3.6 Availability

The web application should be performed as follows,

- 99.99% available unless the web application is designed with expected downtime for activities such as database upgrades and backups.
- Hence to have high availability, the web application must have low downtime and low recovery time.

3.7 Robustness

The web application should be able to handle error conditions gracefully without failure. This includes tolerance of invalid data, software defects, and unexpected operating conditions.

- Failure Detection

- Once deployed, there should be appropriate tools to discover anomalies and failures of the system

- Fault Tolerance
  - Web application developers should anticipate exceptional conditions and develop the system to cope with them. The web application must be able to use reversion to fall back to a safe mode, meaning, the application should continue its intended functions, possibly at a reduced level, rather than failing completely.

3.8 Maintainability

The code of a web application should be properly documented with appropriate comments and no complex codes (highly cohesive and loosely coupled) to do modifications such as corrections, improvements, or adaption.

3.9 Compliance with standards

The code of web application should be standardized by following web standards like W3C and ECMA – European Computer Manufacturers Association, to save time, augment the extensibility of the code, increase web traffic and improve the accessibility and load time of your application.

3.10 Reusability

The web application should use existing assets in some form with the software product development process. Assets are products and by-products of the software development life cycle and include code, software components, test suites, design, and documentation.

Standard coding practices and code documentation will be maintained in order to build quality reusable software and achieve the most gain from reuse.

It is recommended that reuse takes place via the consumption of the service layer. As necessary, the functionality of the solution can be reused at the binary level.

3.11 Internationalization

The web application should be able to be accessed in Sinhalese, English, and Tamil. The web application should be able to view in a usable manner in all three languages in any computing device.

3.12 API Management

The services layer of the solution will function as an endpoint for integration consumers, by default, as a RESTful Application Programming Interface (API), using the JSON data format.

3.12.1 API Standards and Best Practices

All API standards and best practices should be adhered to the code.

3.12.2 API Documentation

Swagger documentation should be provided.

3.12.3 API Security

The web application should use the appropriate API security protocol mentioned below.

- OAuth2
    - No need to use cryptographic algorithms to create, generate, and validate signatures as all the encryption handled by TLS.
    - Recommend for less sensitive data applications
- JWT (JSON Web Tokens)

3.13 Scalability

Suggested web applications should be both scalable and resilient. A well-designed application should be able to scale seamlessly as demand increases and decreases. It should be resilient enough to withstand the loss of one or more hardware resources.

The design of the solution will support both vertical and horizontal scaling, with vertical scaling (also known as 'scaling up') being the addition of more resources to existing deployment units (e.g., increasing processor power of existing servers). Horizontal scaling ('scaling out') being the addition expanded by adding processing, main memory, storage, or network interfaces to a node to satisfy more requests per system.

The solution should be initially deployed in a scaled-out (clustered) configuration, with the minimal required deployment units. While vertical scaling can be used as a short-term measure to handle the increasing load, it is recommended that the more sustainable measure of horizontal scaling be moved to as quickly as possible.

All requests to the servers in the solution should pass through a proxy web server, operating in failover mode in an Active-Passive configuration.

3.14 Portability

Generalized abstraction between the application logic and system interfaces will be built for the usability of the solution in different environments.

3.15Patch Management

Patch management helps to acquire, testing, and installing multiple patches.

- This involves updating the relevant system, OS, Firmware patches after qualifying the same in the Test / Pre- Production environment before moving to production. Notify all storage users of an impact on their applications and assist them in testing their applications with new patches or upgrades.
- Security and Vulnerability patches should be accorded a higher priority than other patches.

3.16 Legal and Licensing

The web application should comply with the national law of Sri Lanka.

3.17Maintainability and Extensibility

The web application should be designed and developed in a way that it can cater to future business needs. The attributes will be enhanced by the use of techniques such as Dependency Injection. System build assets of rest APIs and Integrations points are added to most of the high-level applications. API has been documented using swagger to support maintainability.

From an engineering practice perspective, static analysis tools will be used to ensure maintainable code is being developed, while regular code reviews will further ensure the quality of the source code.

3.18 Testability

The web application should be designed and developed in a way that testability is high, meaning, the ease of testing a piece of code or functionality, or a provision added in software so that test plans and scripts can be systematically executed. In simple terms, the software should be tested easily with the most famous five testing categories,

- Unit test
- Integration test
- System test
- Safety test
- Experience test

Refer to Aden's (2016) view on semantic testing for more information.

The Test-driven development (TDD) approach should be used for unit tests to ensure minimal efforts on the implementation and facilitate correctness. Inversion of control (IoC) will be used to assist the development of such tests. Code coverage must be maintained at 95% or higher to achieve a higher degree of testability.

A performance test will be performed to determine system parameters in terms of responsiveness and stability under various workloads. The test will provide an approximation of how many transactions per second can be supported. The scalability, reliability, and resource usage of the solution will be measured during the test. This is highly recommended as this process ensures meeting the expected service levels in production by optimizing indicators such as network response time, server query processing time, CPU memory consumption, etc.

Furthermore, schedule constraints allowing functional browser-based automated tests will be developed to test user interaction points. The web application should be working according to the given criteria in the latest version and five versions before in web browsers such as Mozilla Firefox, Google Chrome, Opera, and Apple Safari and the latest version and two versions before in Internet Explorer.

3.19 Configurability

The solution should be made configurable where possible, to enable modification of system behavior, post-deployment. This will be managed carefully (i.e., implemented only where required) to minimize any impact on the performance of the system. All the services build to comply with the 12-factor app development framework, so the configurability is inbuilt with the system. The system can be deployed in any cloud platform with minimum changes due to that.

3.20 Monitoring/Instrumentation

Monitoring should be implemented at all levels of the application and its infrastructure.

3.21 Accuracy/Correctness

3.21.1 Transactions

The correctness of data – in terms of ACID properties (Atomic, Consistent, Integrity, and Durability) - will be ensured by the use of a transaction framework built into the programming frameworks used.

All write operations (Create, Update, Delete), barring those exempted by specific functional requirements, should exhibit serializable behavior; read operations, where relevant (e.g., for generating list views) may use a lower level of serializability, such as Read Committed.

3.21.2 Concurrency

To maximize throughput, and optimistic concurrency model should be utilized, except where functional requirements dictate a pessimistic model, such as locking.

The system should be designed to support the microservice architecture with an eventually consistent method. Concurrency is handled by providing event-based communication and orchestration of services based on events. Based on specific functional requirements, a higher granularity of concurrency checking (even up to field level) should be supported, though with an impact on performance and maintainability.

3.22 Controls and Governance

The following mechanism should be implemented but not limited to.

3.22.1 Operational Governance

These involve internal policies and procedures for the operation. Further should align with the ISO/IEC 38500:2008.

- Information security policies
- Privacy policy and notices
- Human resources policies
- IT governance policy
- Business continuity management and disaster recovery
- Data retention policies
- Communication to and acknowledgment by employees of policies

3.22.2 Audit and Compliance

Rigorous audits for the entire system, which would be conducted on a regular basis both internally and by trusted independent entities. The goal is to demonstrate the compliance of the UDI system with applicable laws and regulations, as well as internal policies, and that it operates effectively as designed and presented to the public.

3.22.3 Security and Privacy

- Physical access control and security procedures to the UDI issuance site to protect against unauthorized use.
- Role-based system and logical access control to prevent system abuse.
- Segregation of operational authority to combat malfeasance.
- Secure audit logs to enhance investigative power in case of an incident and to provide deterrence.
- Privacy controls.

4 Annexure

5 Sign off

Name:

Designation:

Signature:

Name:

Designation:

Signature: