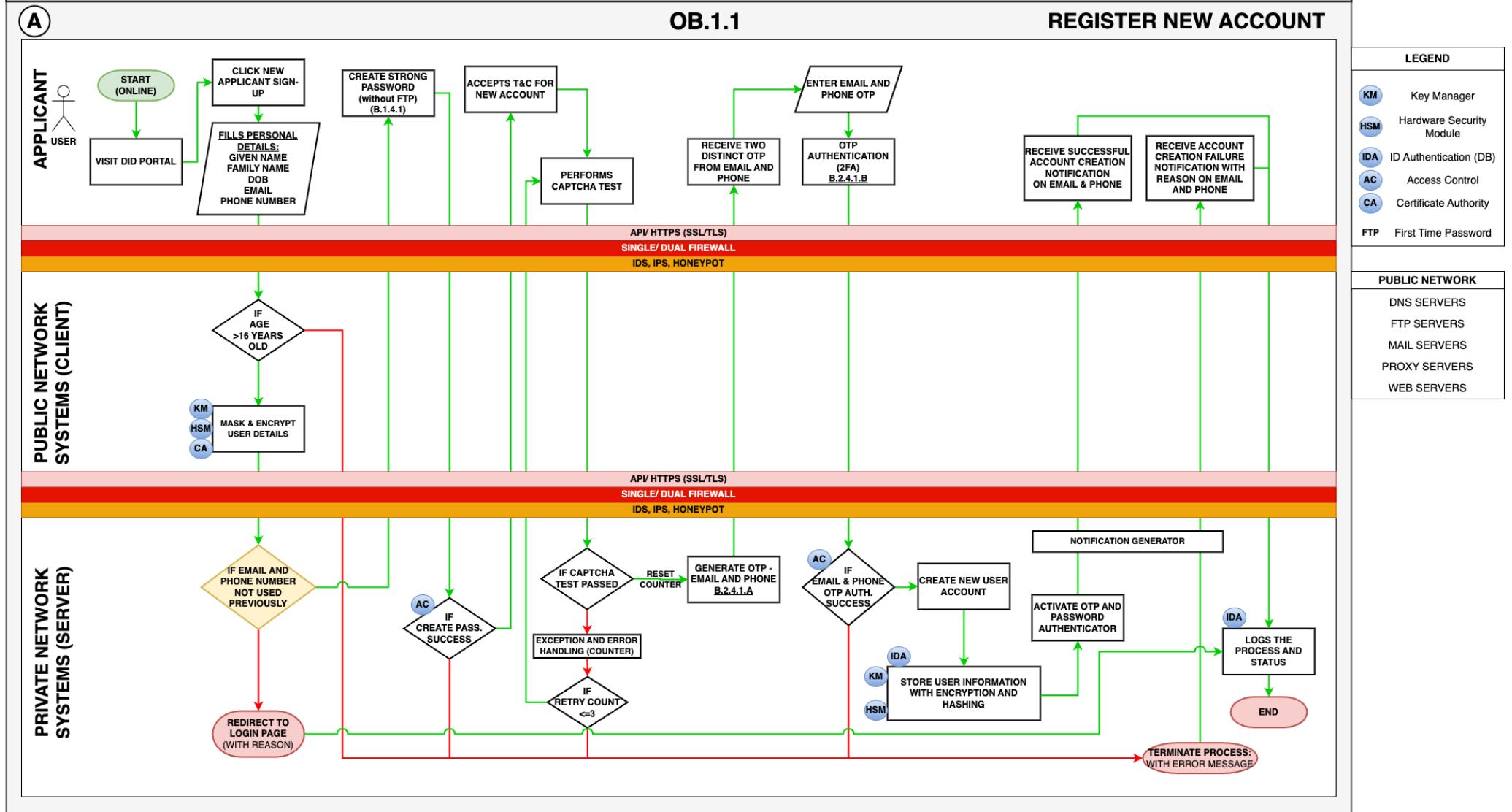
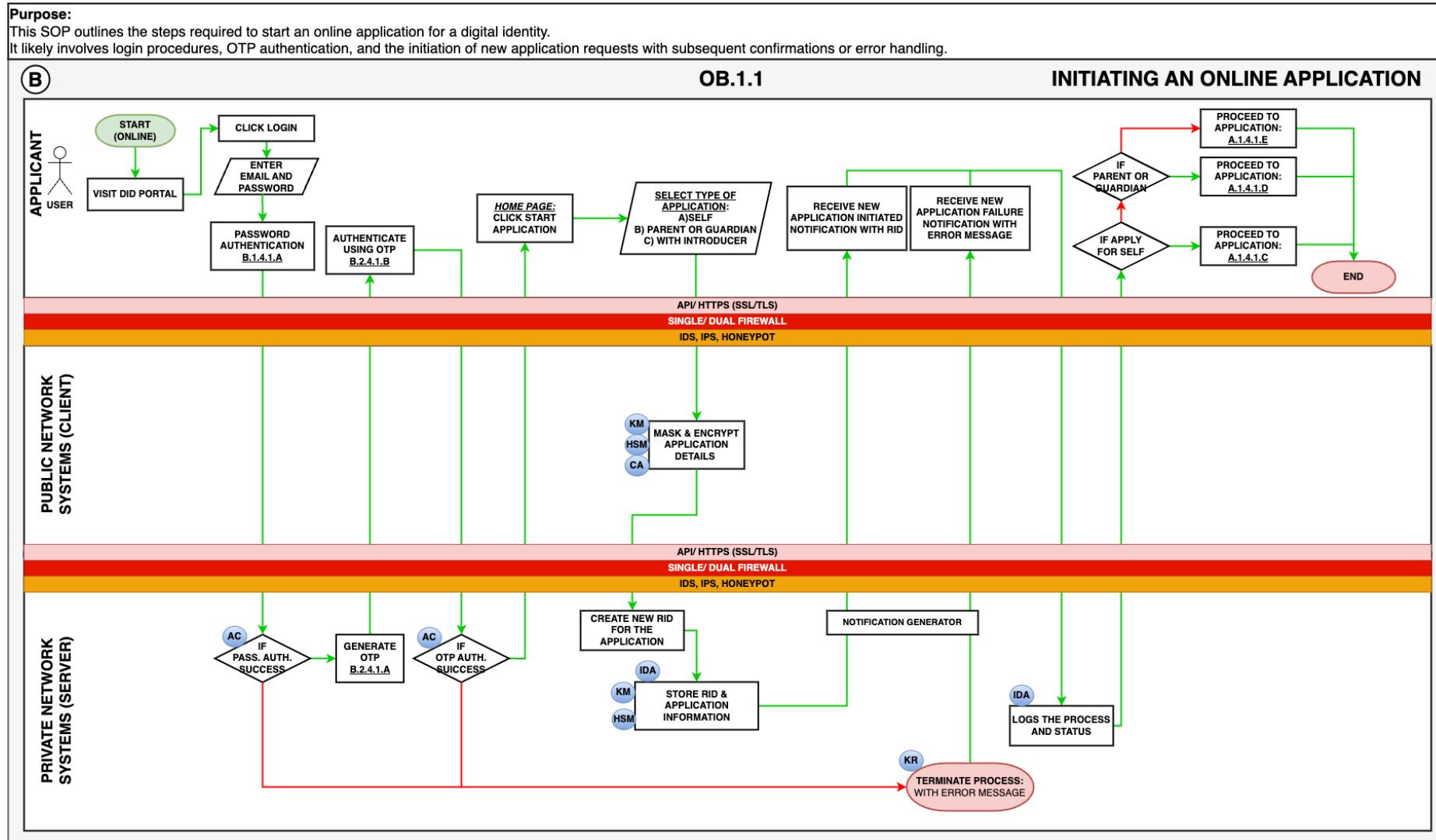


Purpose:

The SOP is designed to guide applicants through the process of registering a new account within the digital identity system.

This would typically include creating login credentials, passing security checks, and receiving confirmation notifications or error messages in case of failure.

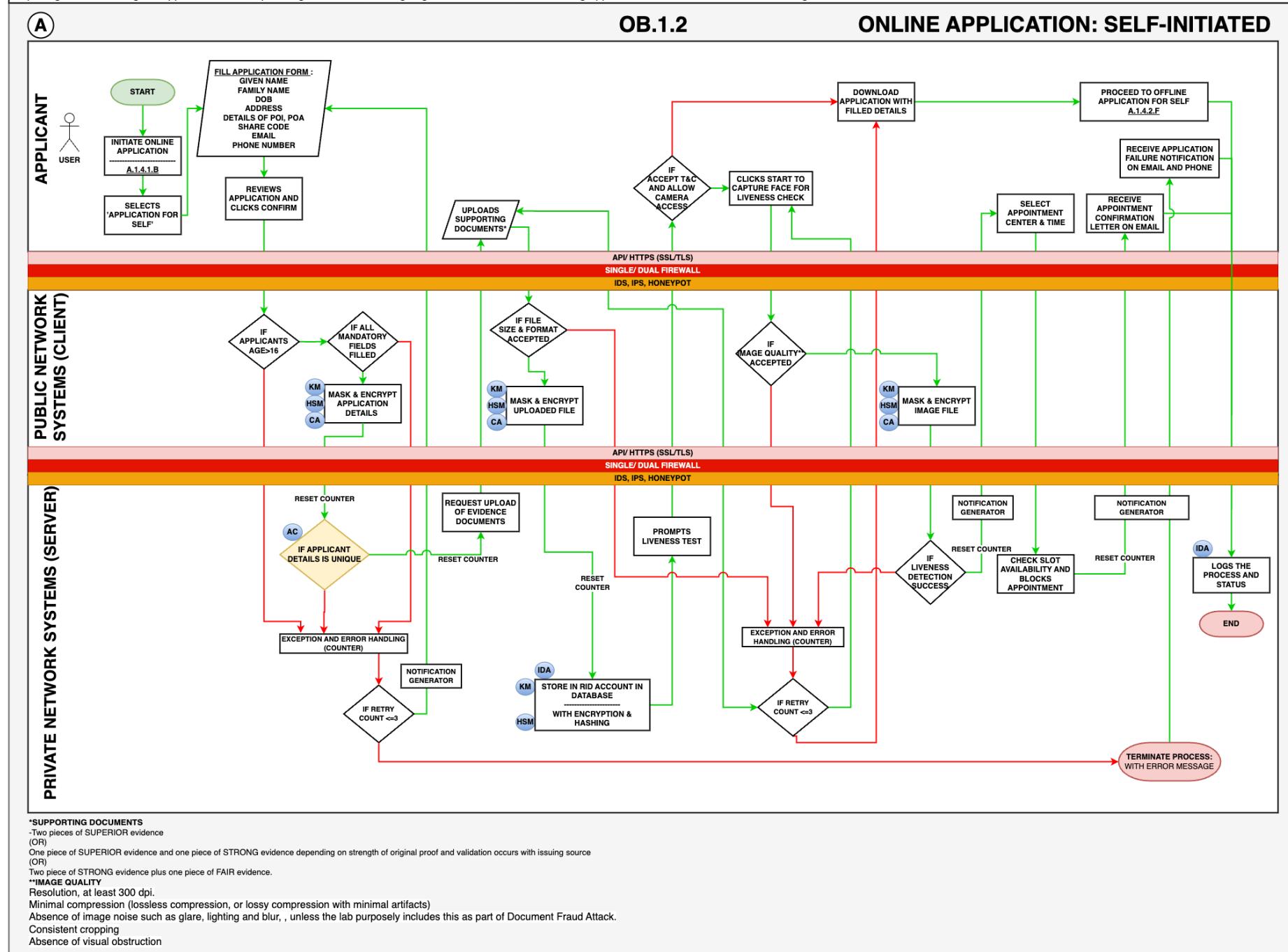




Purpose:

The SOP depicts the process an individual must follow to apply online on their own behalf.

Steps might include filling out application forms, uploading documents, undergoing liveness checks, and receiving appointment confirmations or error messages.

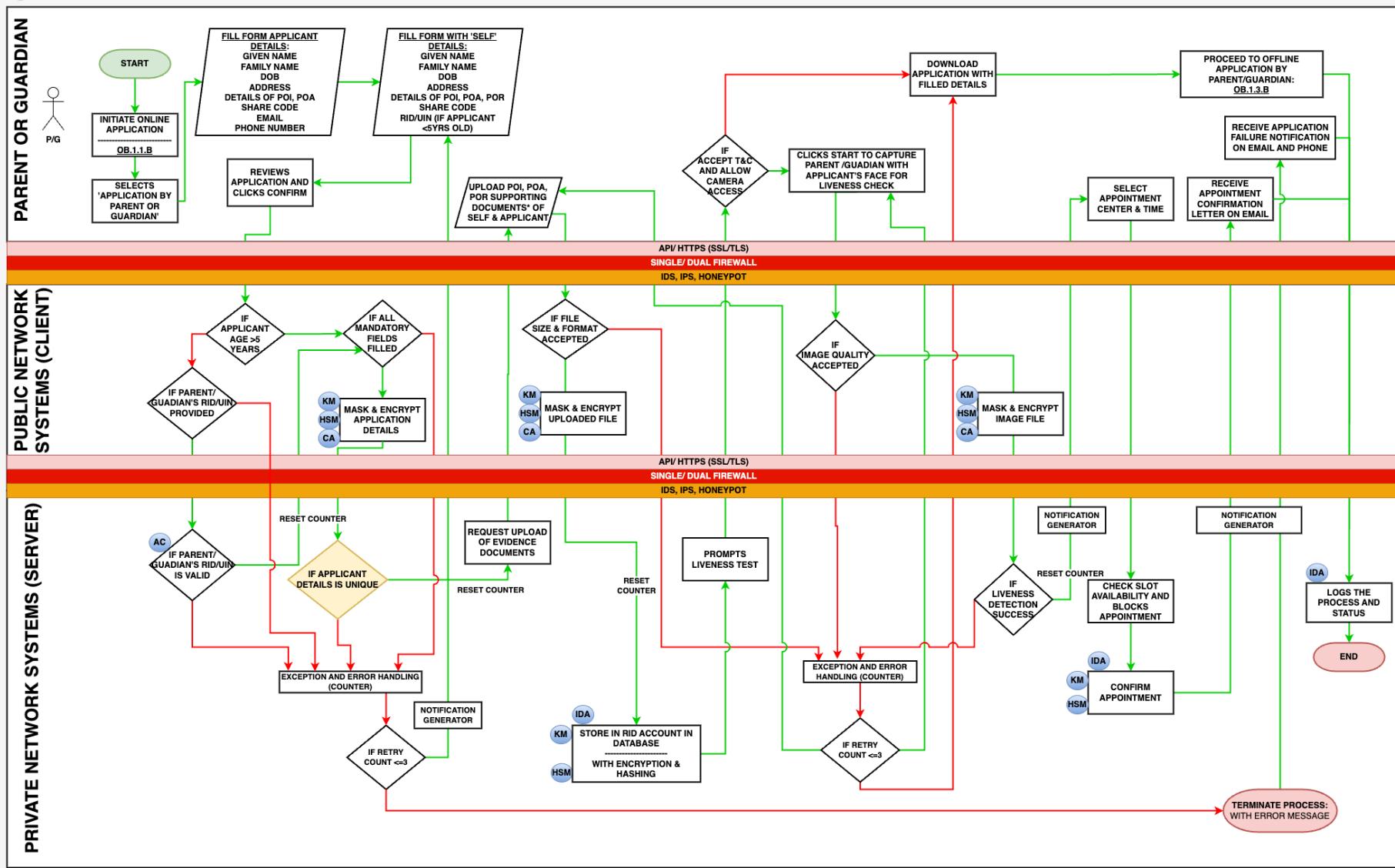


Purpose:

This SOP outlines a process to involve a parent or guardian filling out an application form with personal details and uploading supporting documents.

The process includes validation steps like RID/UID checks, liveness checks, and error handling mechanisms.

It concludes with an appointment confirmation or process termination if there are errors.

B**OB.1.2 ONLINE APPLICATION: APPLICATION BY PARENT/GUARDIAN**

LEGEND	
KM	Key Manager
HSM	Hardware Security Module
IDA	ID Authentication (DB)
AC	Access Control
CA	Certificate Authority
POI	Proof of Identity
POA	Proof of Address
POR	Proof of Relationship

PUBLIC NETWORK	
DNS SERVERS	
FTP SERVERS	
MAIL SERVERS	
PROXY SERVERS	
WEB SERVERS	

SUPPORTING DOCUMENTS

-Two pieces of SUPERIOR evidence

(OR)

One piece of SUPERIOR evidence and one piece of STRONG evidence depending on strength of original proof and validation occurs with issuing source

(OR)

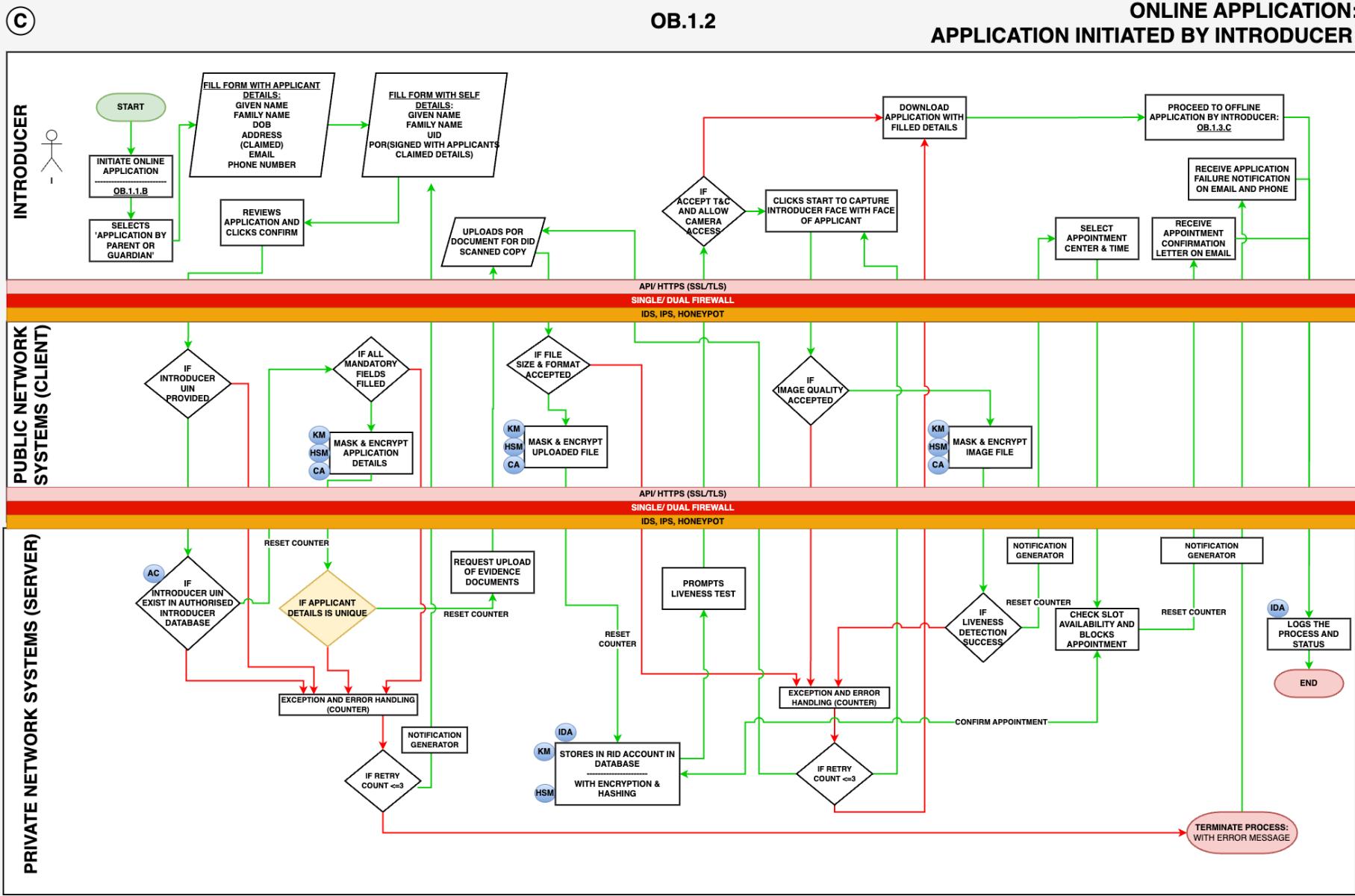
Two piece of STRONG evidence plus one piece of FAIR evidence.

Purpose:

This SOP outlines a process where an introducer fills out forms on behalf of an applicant and uploads required documents.

There is mention of authentication via introducer UIN and checks against an authorized introducer database.

Similar to the previous SOP, it concludes with appointment confirmation or error message if the process fails.

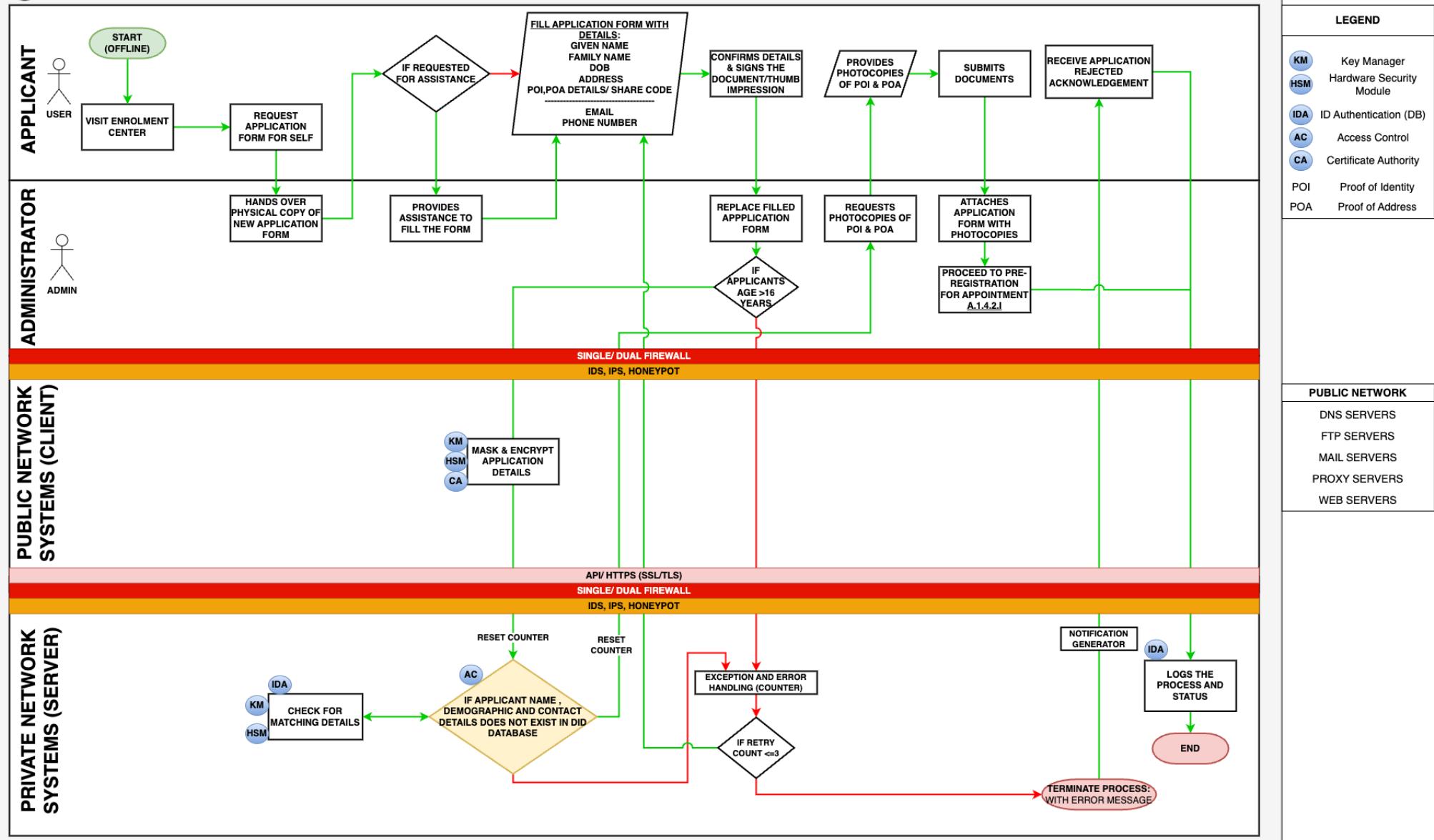
OB.1.2**ONLINE APPLICATION:
APPLICATION INITIATED BY INTRODUCER**

LEGEND	
KM	Key Manager
HSM	Hardware Security Module
IDA	ID Authentication (DB)
AC	Access Control
CA	Certificate Authority
POR	Proof of Relationship

PUBLIC NETWORK	
DNS SERVERS	
FTP SERVERS	
MAIL SERVERS	
PROXY SERVERS	
WEB SERVERS	

Purpose:

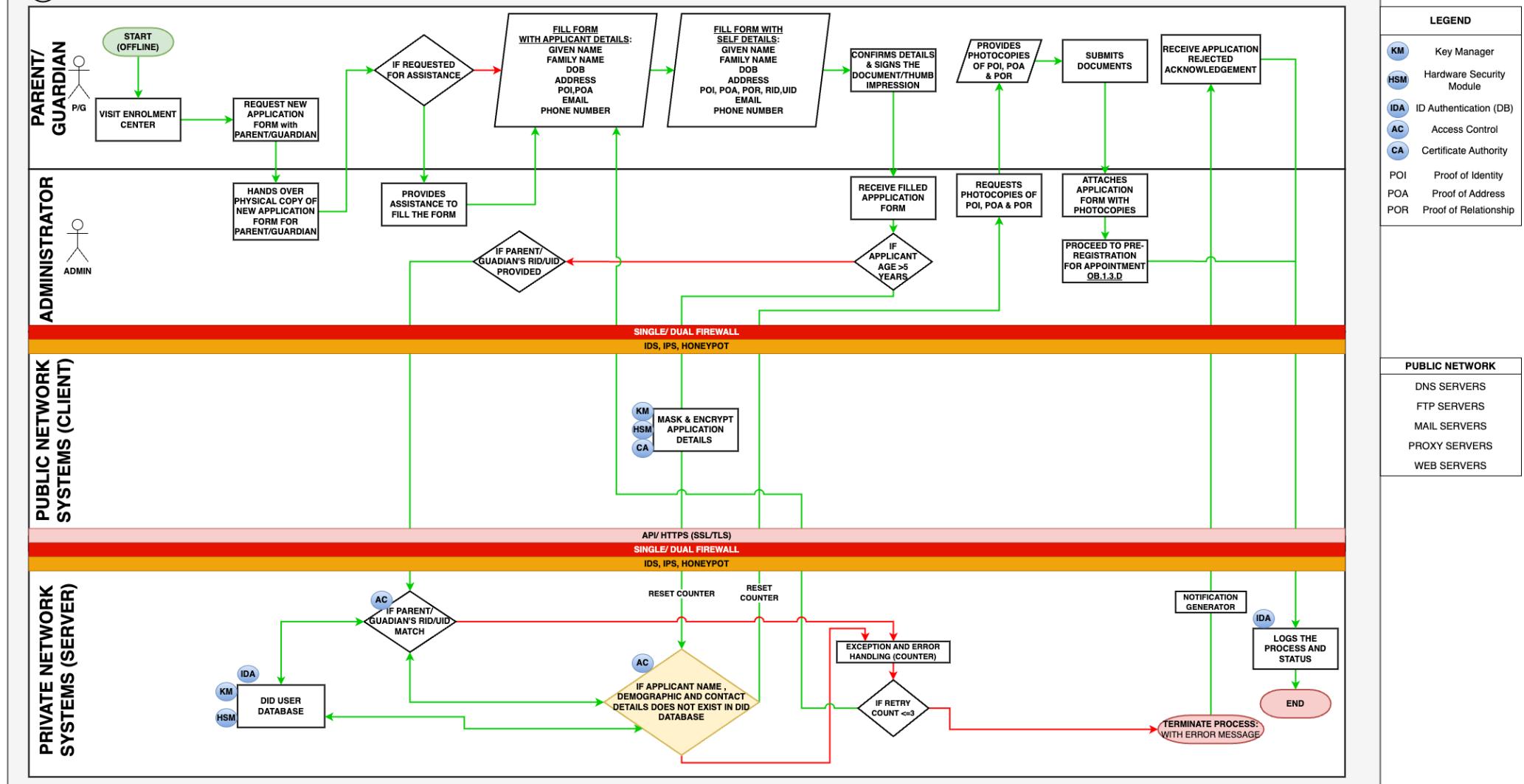
This SOP describe how an individual can apply in-person without online facilities, including submitting forms and documents to an enrollment center and receiving a physical acknowledgment.

A**OB.1.3****OFFLINE APPLICATION: SELF-INITIATED**

Purpose:

This SOP outlines the steps for a parent or guardian to apply offline on behalf of a child, which might involve visiting an enrollment center, filling out forms, and providing necessary documentation.

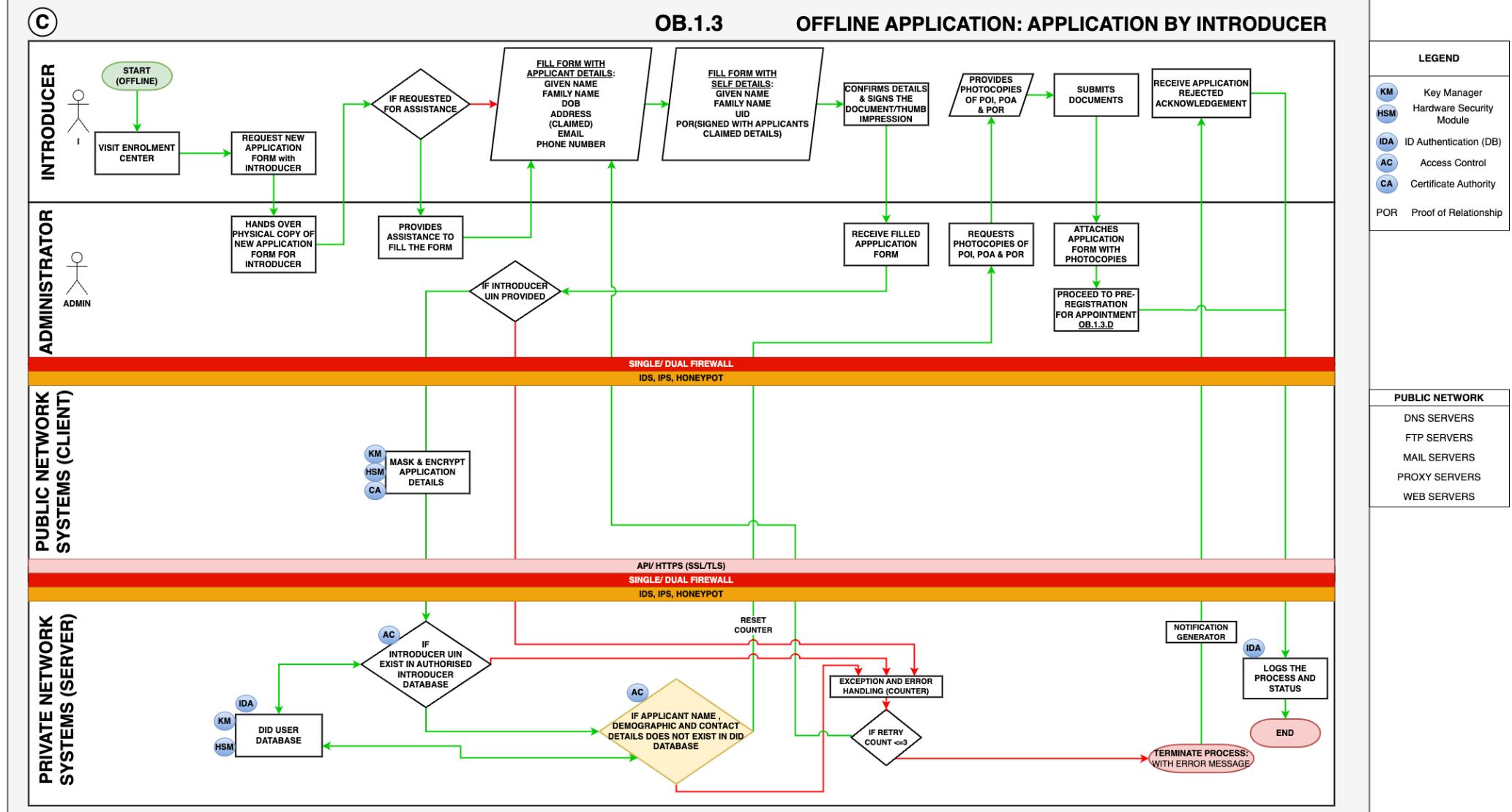
OB.1.3 OFFLINE APPLICATION: APPLICATION BY PARENT/GUARDIAN



Purpose:

This SOP describes a similar process to the second SOP, but carried out offline with the assistance of an introducer.

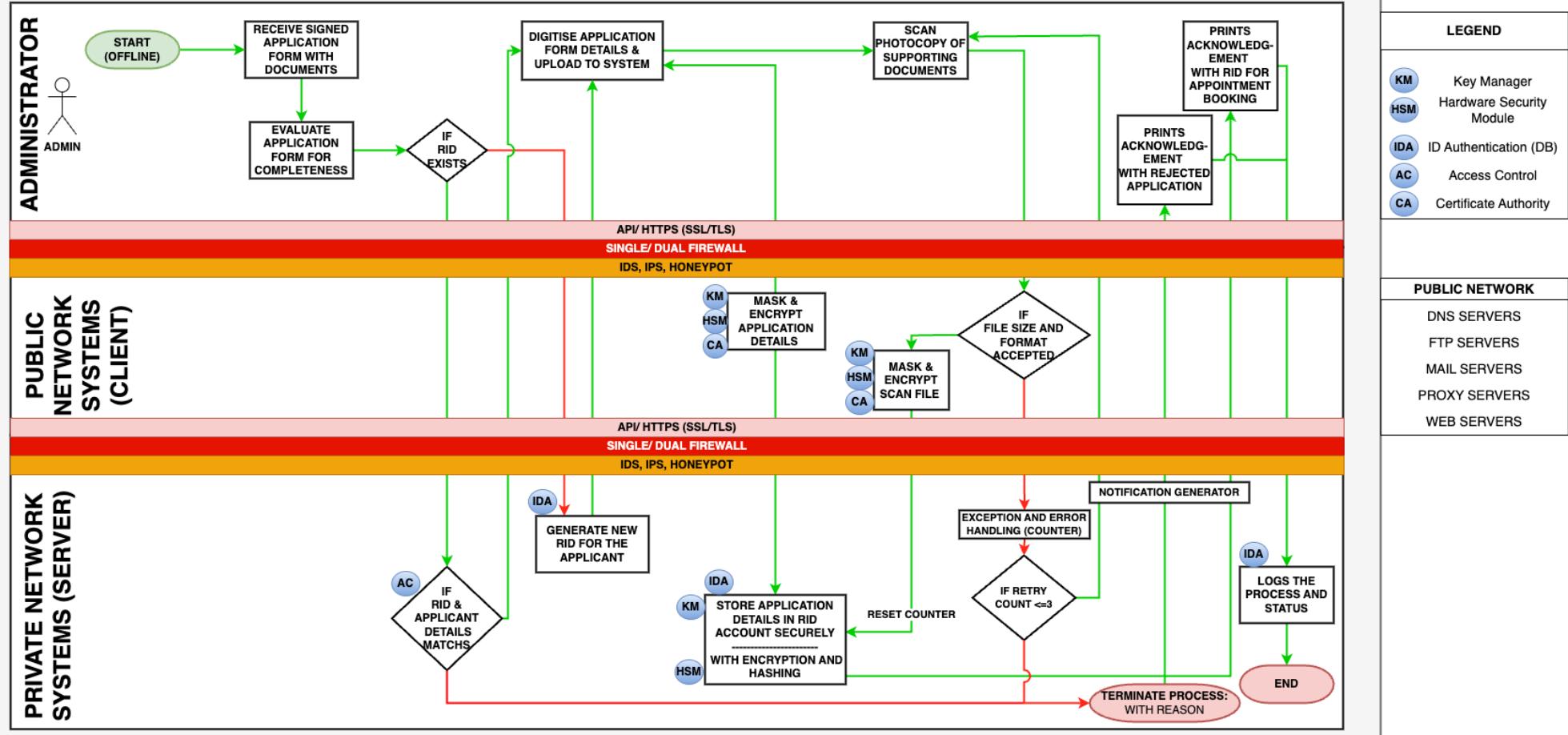
It includes document verification, form submission, and handling of exceptions and errors.



Purpose:

The SOP outlines the process for pre-registration and appointment booking in an offline setting.

It includes steps like receiving signed forms, digitizing application details, evaluating the application for completeness, and dealing with exceptions and errors.

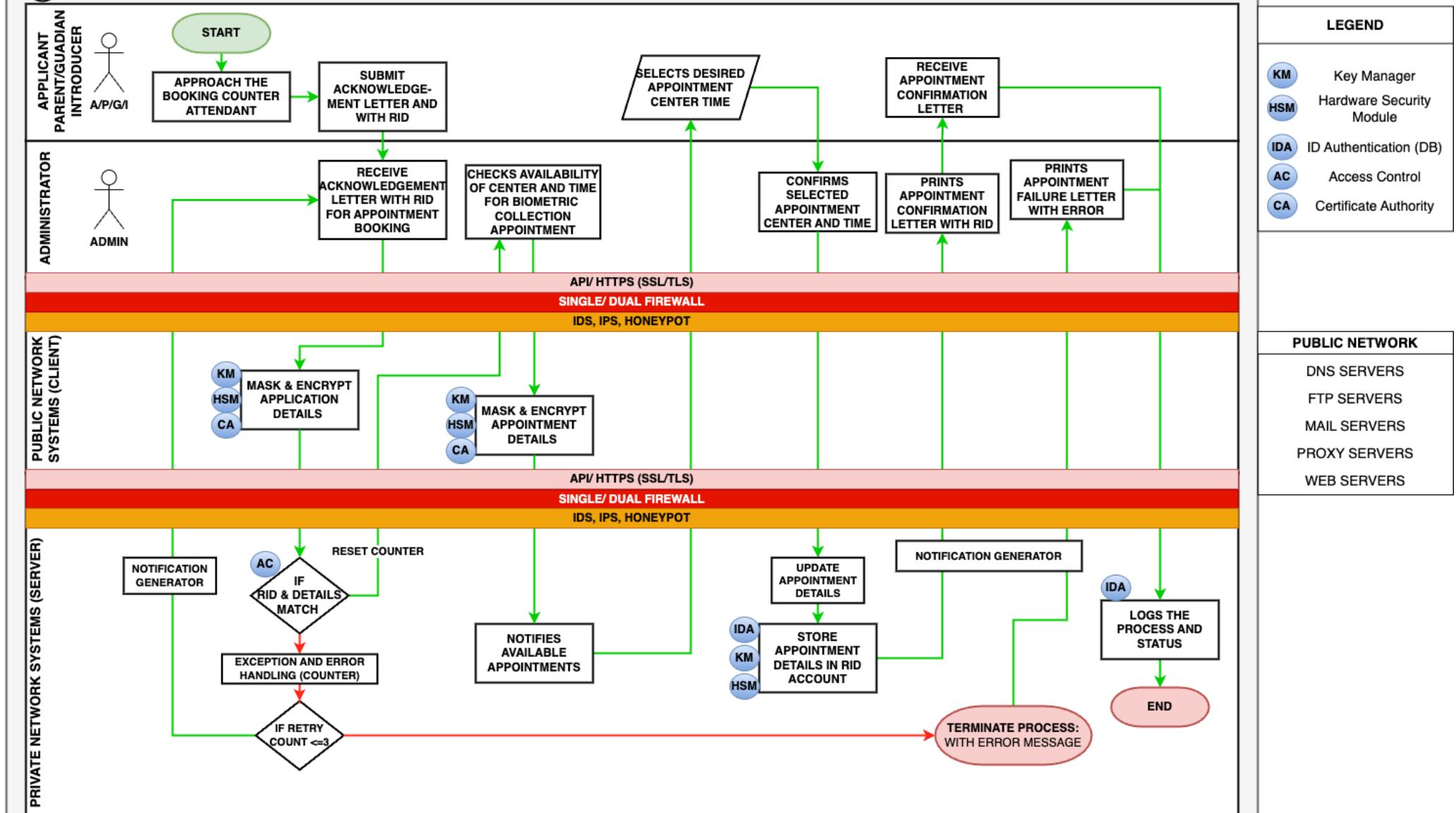
D**OB.1.3 PRE-REGISTRATION: APPOINTMENT BOOKING**

Purpose:

This SOP describes the steps for scheduling an appointment for offline biometric collection.

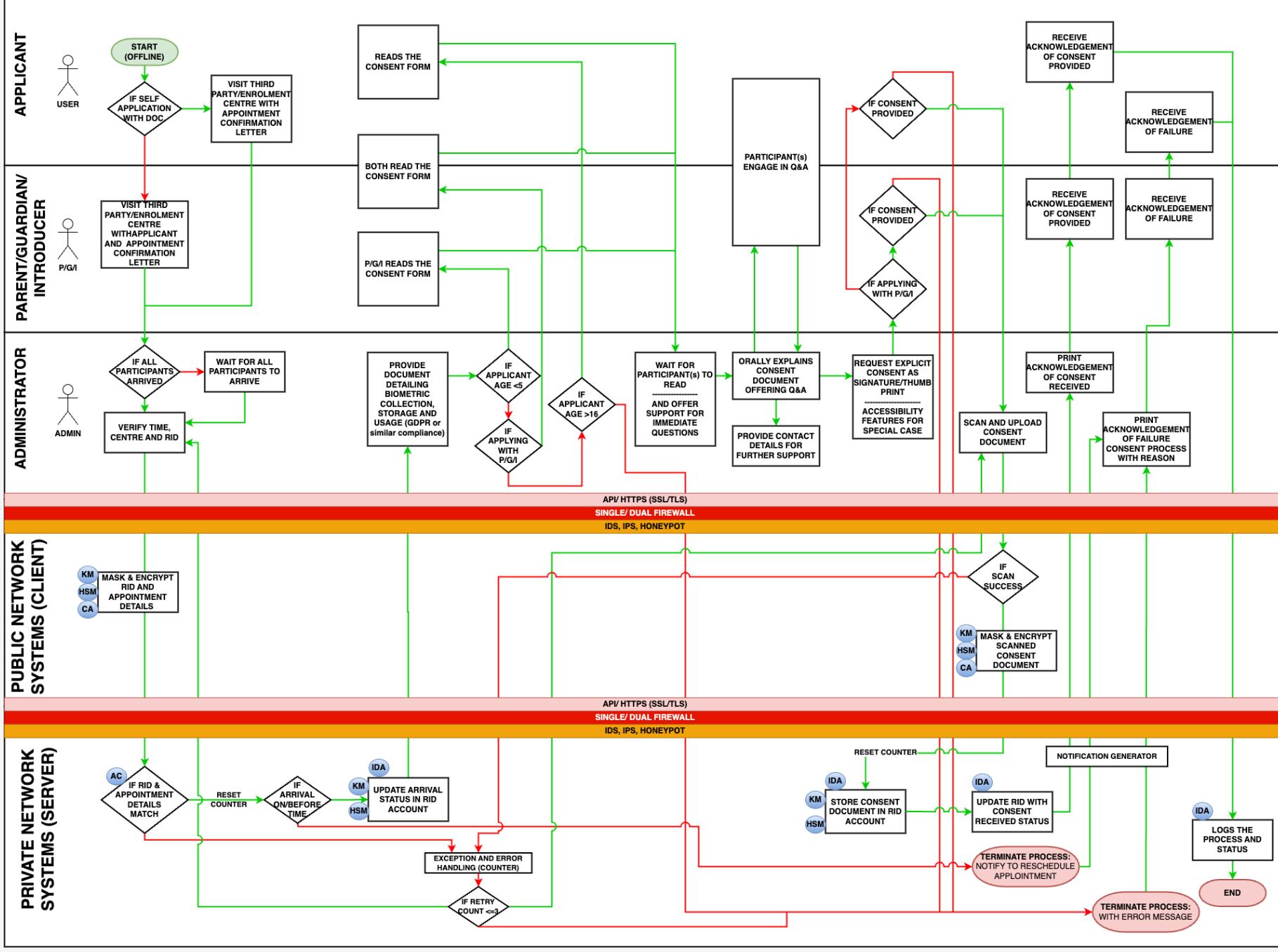
It involves submitting acknowledgment letters, checking the availability of centers and times, confirming appointments, and handling potential errors.

E OB.1.3 OFFLINE BIOMETRIC COLLECTION: APPOINTMENT



Purpose:

This SOP focuses on obtaining informed consent from the applicant or guardian for the collection and use of biometric data.

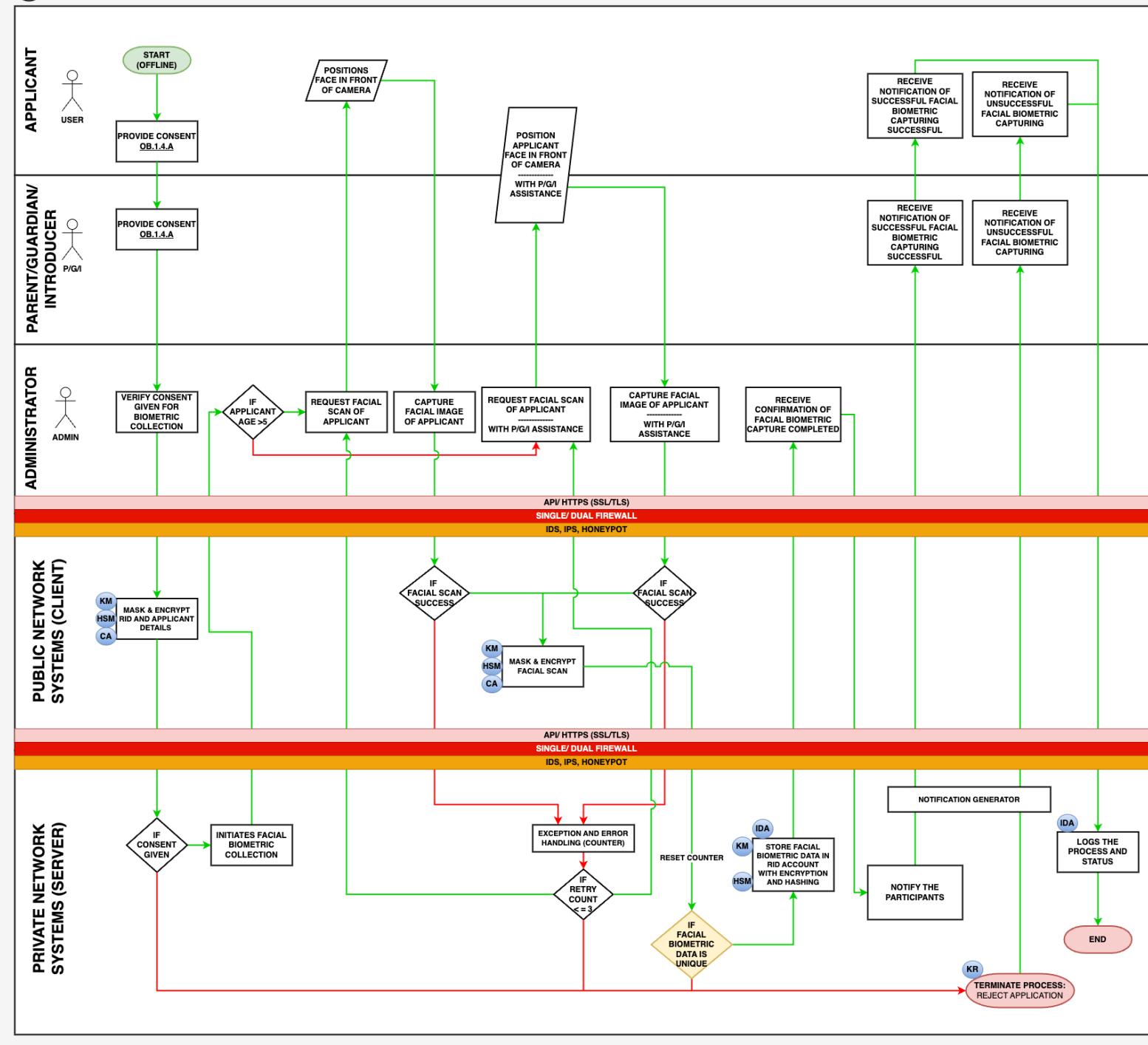
OB.1.4**OFFLINE BIOMETRIC COLLECTION: CONSENT**

LEGEND	
KM	Key Manager
HSM	Hardware Security Module
IDA	ID Authentication (DB)
AC	Access Control
CA	Certificate Authority

PUBLIC NETWORK	
DNS SERVERS	
FTP SERVERS	
MAIL SERVERS	
PROXY SERVERS	
WEB SERVERS	

Purpose:

This SOP details the steps for capturing and securely processing an applicant's facial biometric data for identity services.

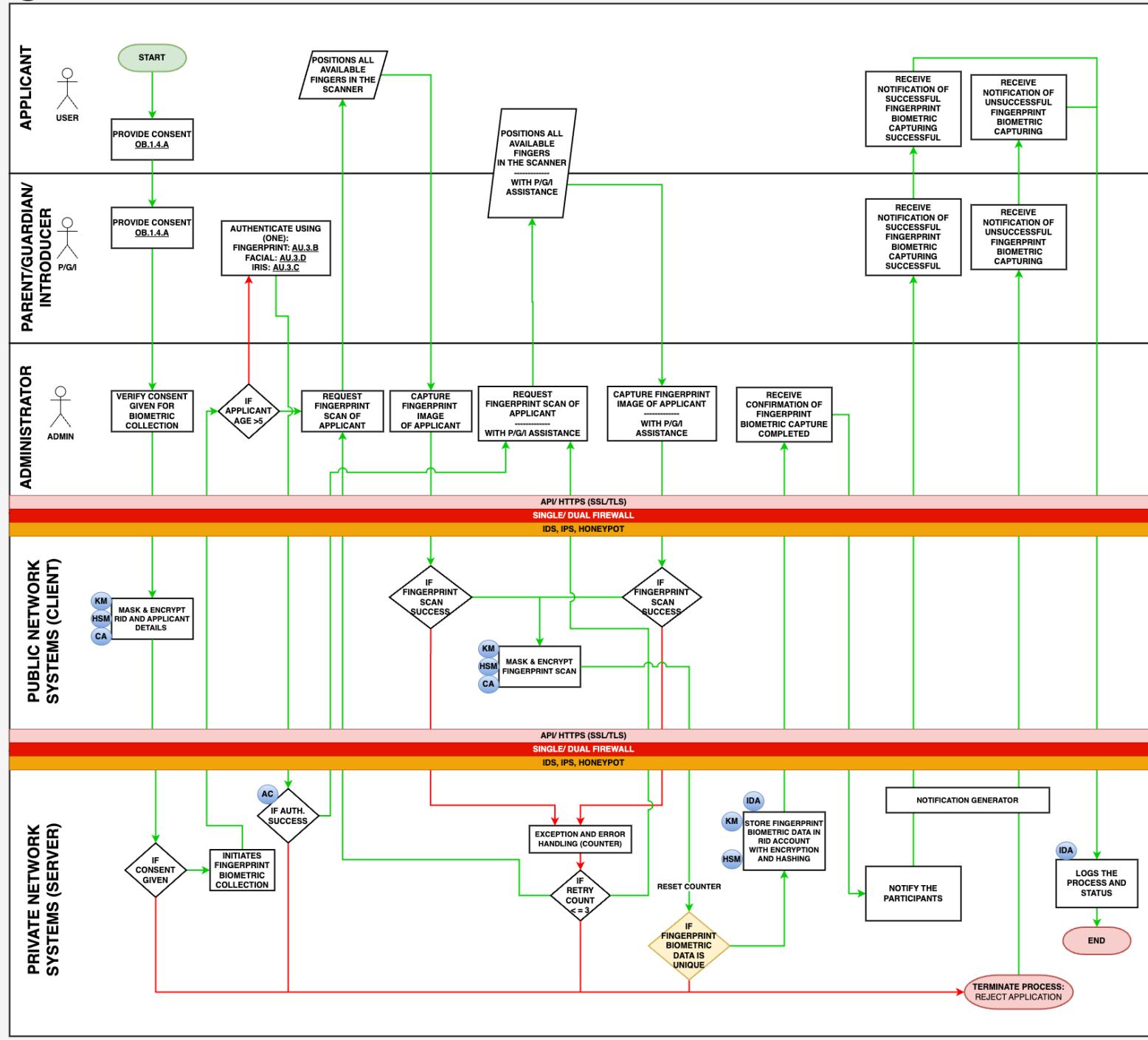
B**OB.1.4 OFFLINE BIOMETRIC COLLECTION: FACIAL DATA**

LEGEND	
KM	Key Manager
HSM	Hardware Security Module
IDA	ID Authentication (DB)
CA	Certificate Authority
	Deduplication Process

PUBLIC NETWORK	
DNS SERVERS	
FTP SERVERS	
MAIL SERVERS	
PROXY SERVERS	
WEB SERVERS	

Purpose:

This SOP covers the process of collecting an applicant's fingerprint biometrics, including consent acquisition, secure capture, and data transmission.

C**OB.1.4 OFFLINE BIOMETRIC COLLECTION: FINGERPRINT DATA****LEGEND**

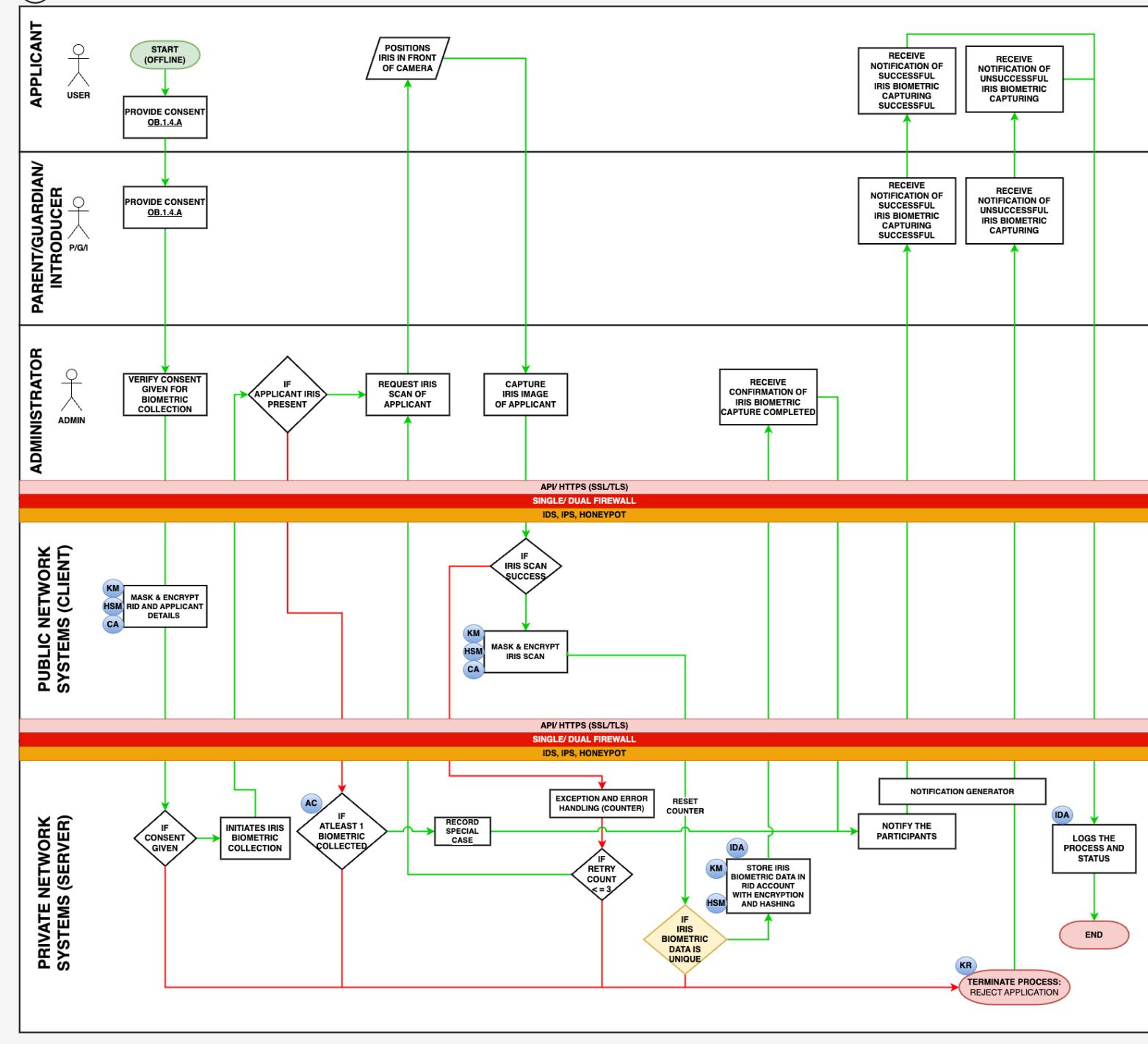
KM	Key Manager
HSM	Hardware Security Module
IDA	ID Authentication (DB)
AC	Access Control
CA	Certificate Authority
Deduplication Process	

PUBLIC NETWORK

DNS SERVERS
FTP SERVERS
MAIL SERVERS
PROXY SERVERS
WEB SERVERS

Purpose:

This SOP describes the procedures for collecting iris biometrics from applicants, ensuring data encryption and secure transfer for authentication.

D**OB.1.4 OFFLINE BIOMETRIC COLLECTION: IRIS DATA****LEGEND**

KM	Key Manager
HSM	Hardware Security Module
IDA	ID Authentication (DB)
AC	Access Control
CA	Certificate Authority
D	Deduplication Process

PUBLIC NETWORK

DNS SERVERS
FTP SERVERS
MAIL SERVERS
PROXY SERVERS
WEB SERVERS

KR

TERMINATE PROCESS:
REJECT APPLICATION

Purpose:

This SOP outlines the criteria and process for the approval or rejection of an applicant's identity verification based on biometric and documentation verification.

