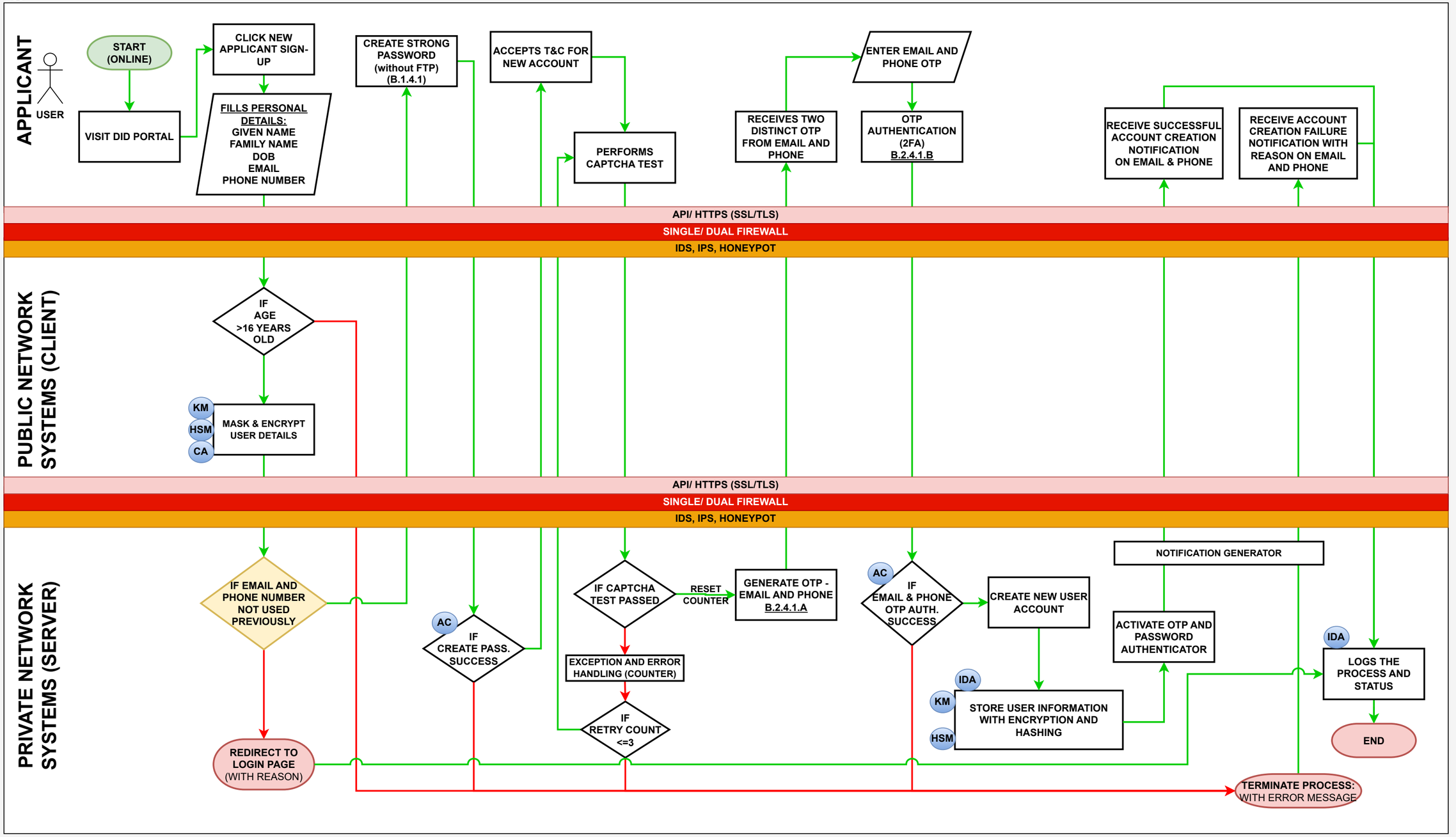
Purpose:
The SOP is designed to guide applicants through the process of registering a new account within the digital identity system.
This would typically include creating login credentials, passing security checks, and receiving confirmation notifications or error messages in case of failure.

Ⓐ

OB.1.1 REGISTER NEW ACCOUNT



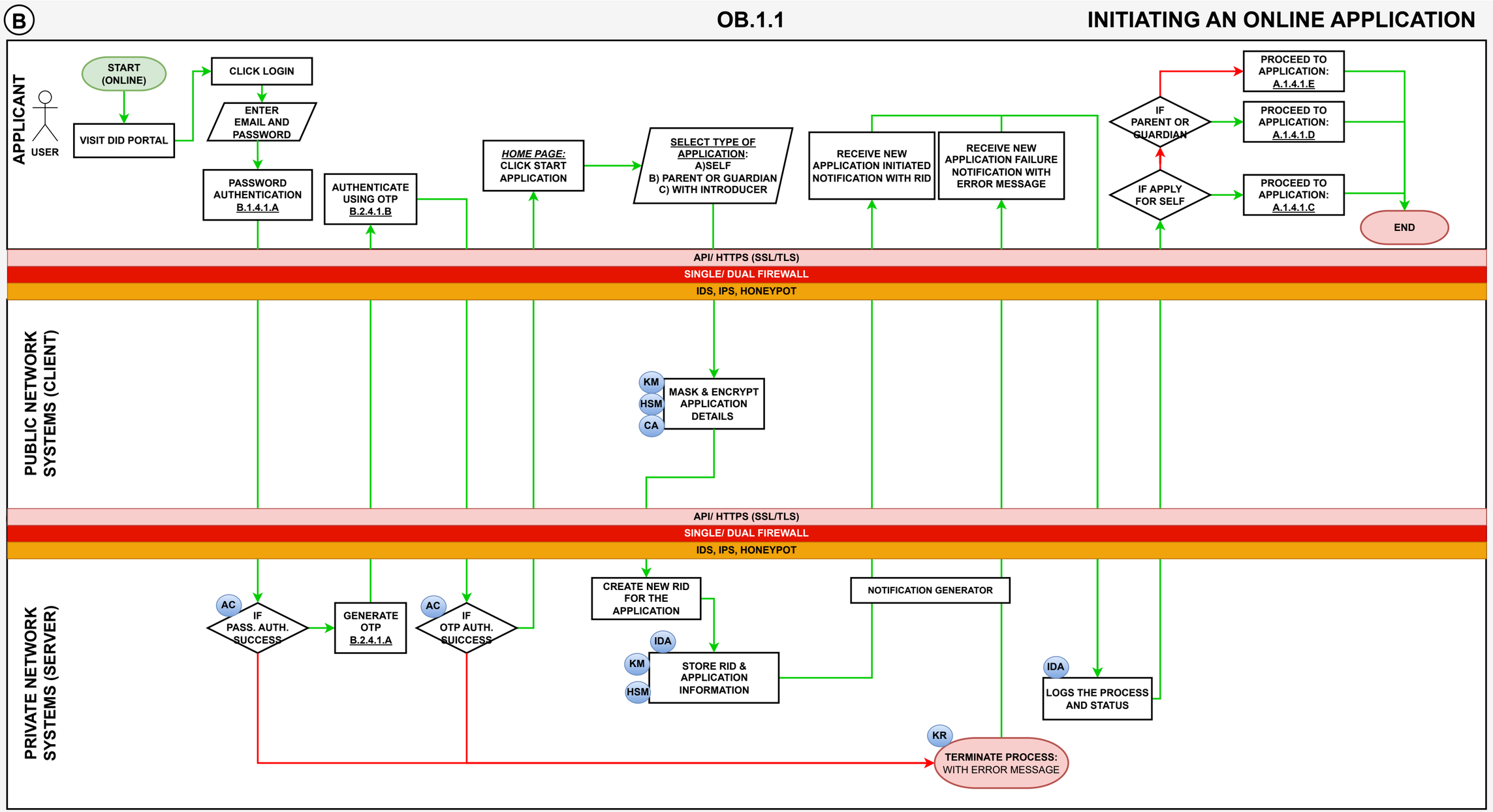
LEGEND

KM	Key Manager
KR	Key Revocation
HSM	Hardware Security Module
IDA	ID Authentication (DB)
AC	Access Control
CA	Certificate Authority
FTP	First Time Password

PUBLIC NETWORK

- DNS SERVERS
- FTP SERVERS
- MAIL SERVERS
- PROXY SERVERS
- WEB SERVERS

Purpose:
This SOP outlines the steps required to start an online application for a digital identity.
It likely involves login procedures, OTP authentication, and the initiation of new application requests with subsequent confirmations or error handling.



LEGEND

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

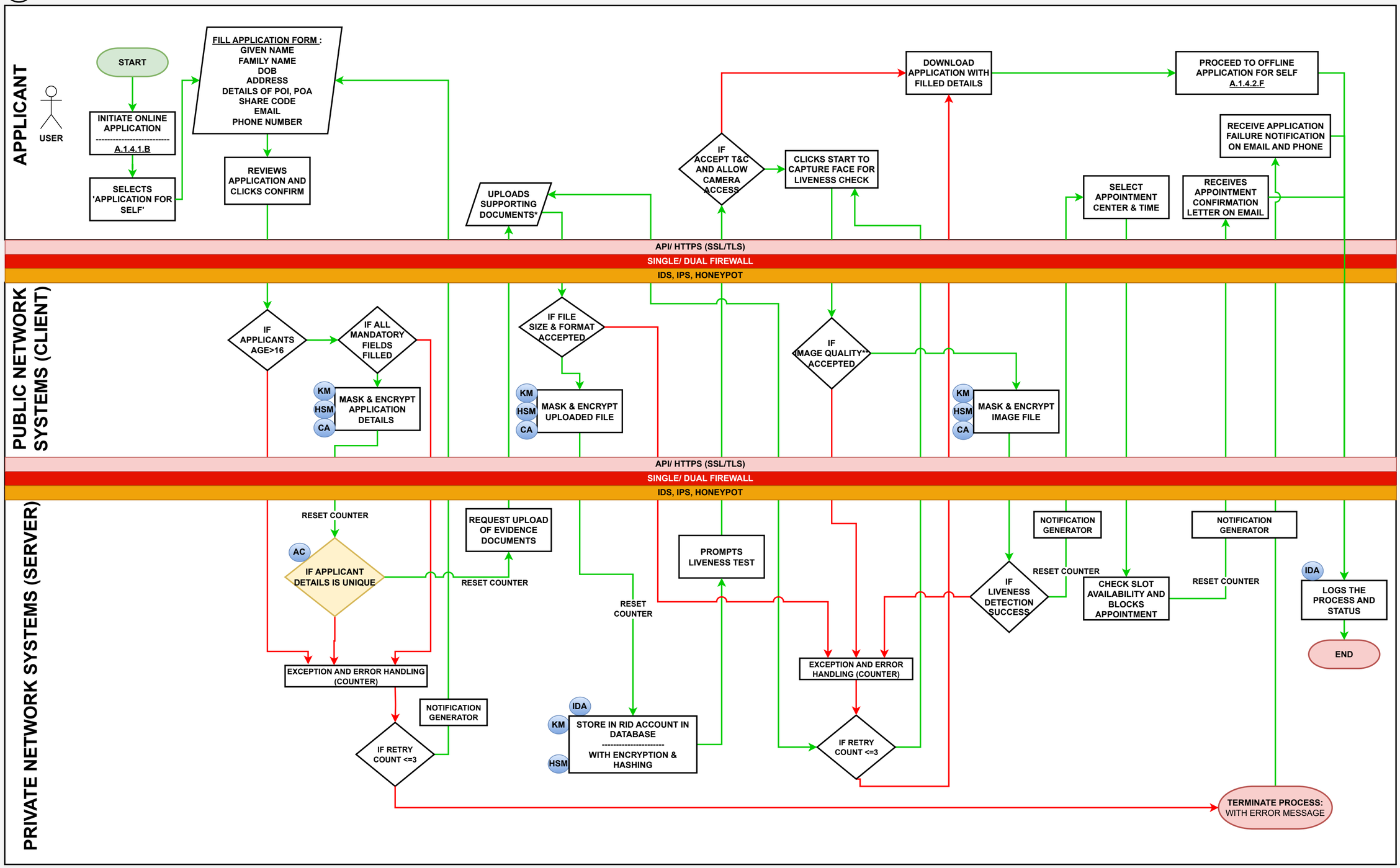
PUBLIC NETWORK

- DNS SERVERS
- FTP SERVERS
- MAIL SERVERS
- PROXY SERVERS
- WEB SERVERS

Purpose:
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.

Ⓐ

OB.1.2 ONLINE APPLICATION: SELF-INITIATED



***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.

****IMAGE QUALITY**
Resolution, at least 300 dpi.
Minimal compression (lossless compression, or lossy compression with minimal artifacts)
Absence of image noise such as glare, lighting and blur, , unless the lab purposely includes this as part of Document Fraud Attack.
Consistent cropping
Absence of visual obstruction

LEGEND

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

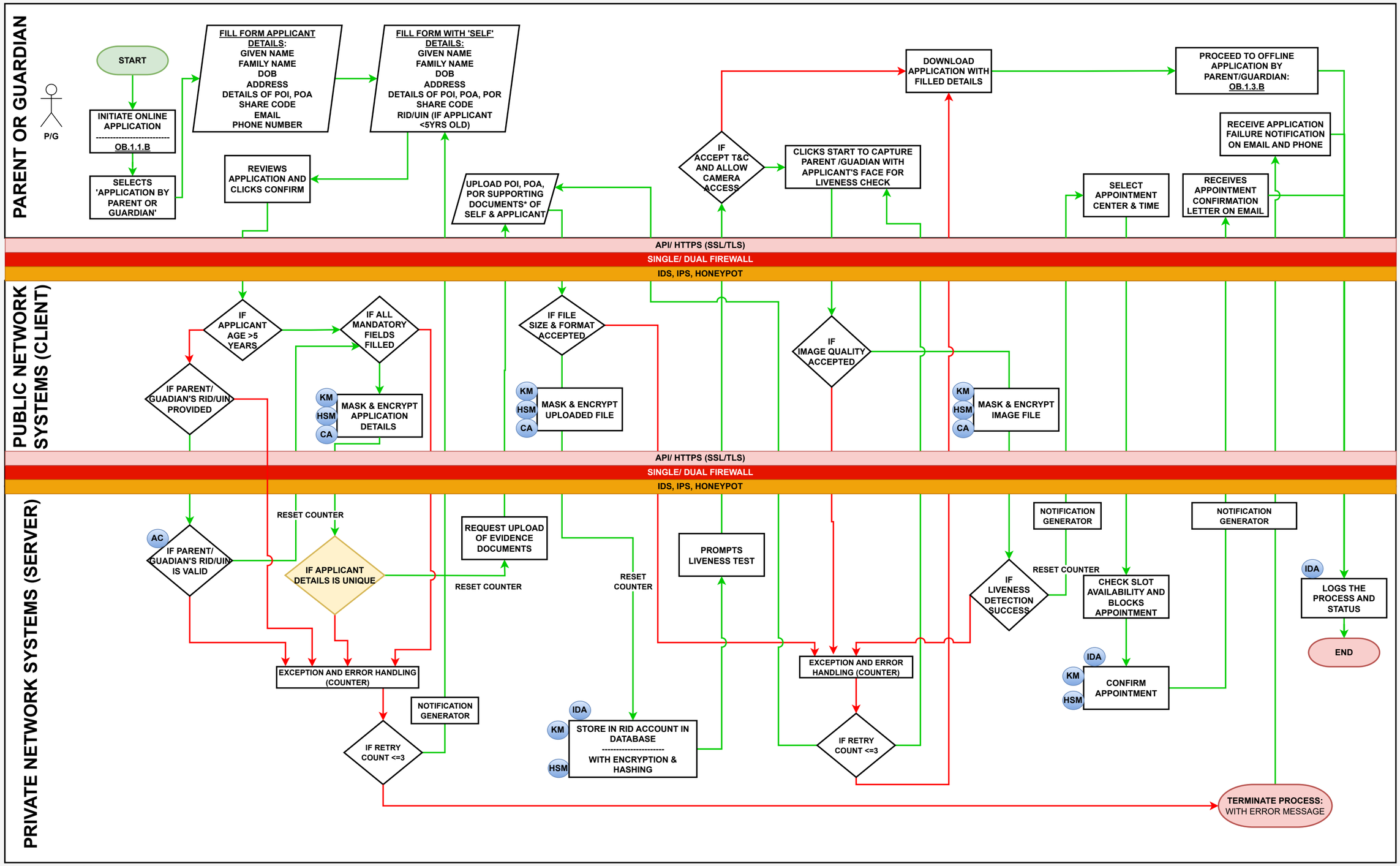
PUBLIC NETWORK

DNS SERVERS
FTP SERVERS
MAIL SERVERS
PROXY SERVERS
WEB SERVERS

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
KR	Key Revocation
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

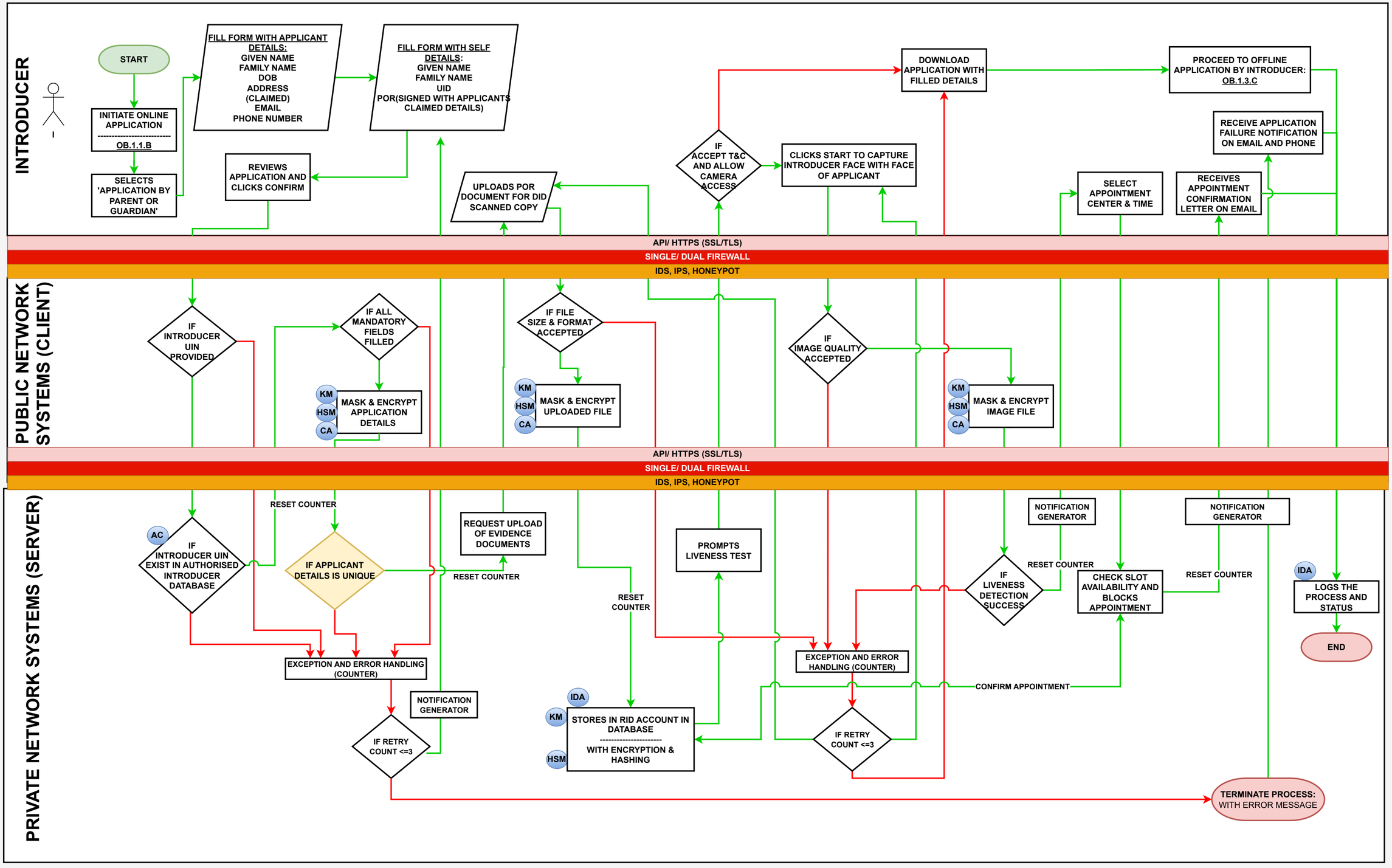
***SUPPORTING DOCUMENTS**
-Two pieces of SUPERIOR evidence
(OR)
One piece of SUPERIOR evidence and one piece of STRONG evidence depending on strength of original proof and validation occurs with issuing source
(OR)
Two piece of STRONG evidence plus one piece of FAIR evidence.

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

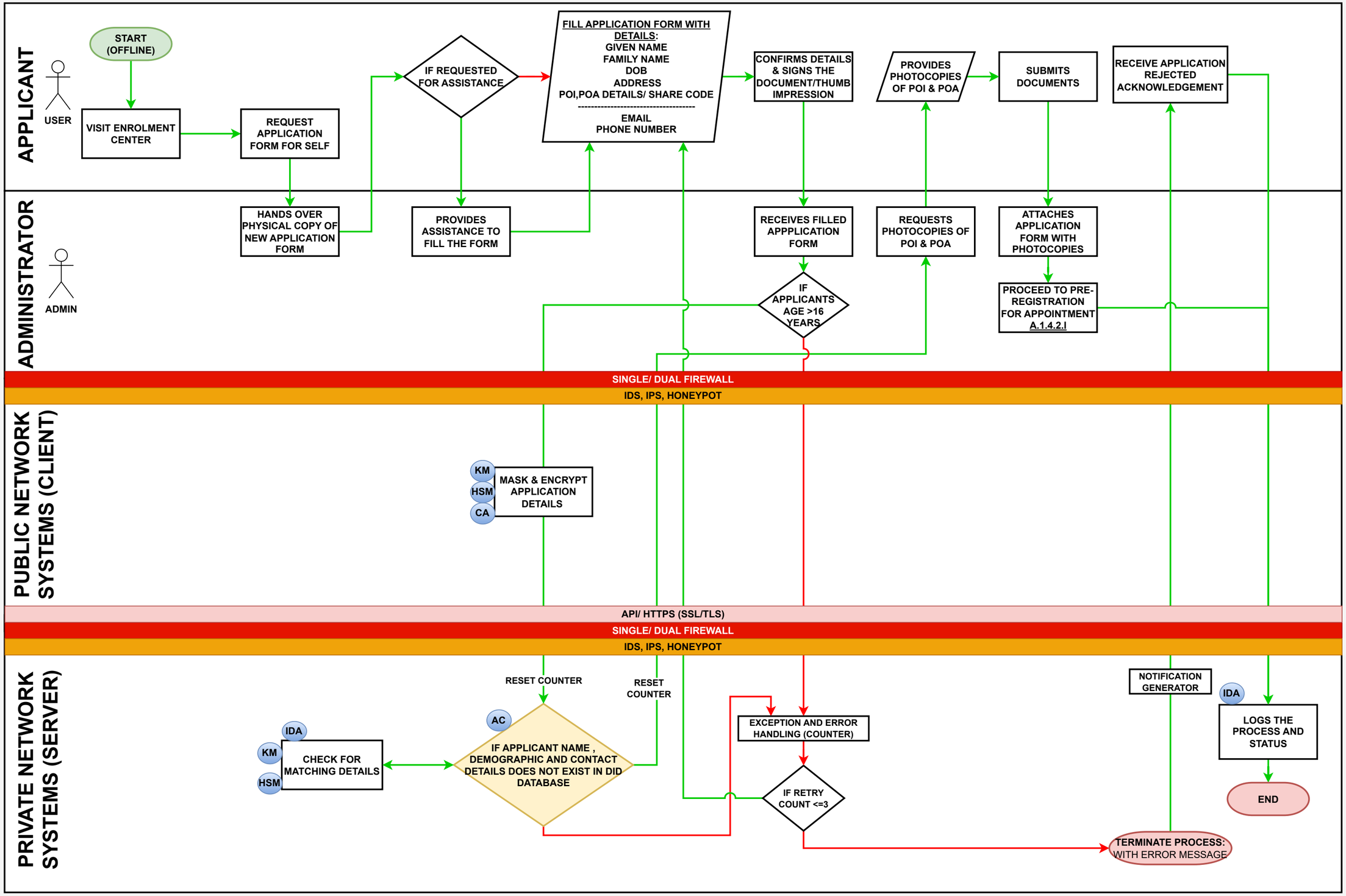
PUBLIC NETWORK

- 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



LEGEND

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

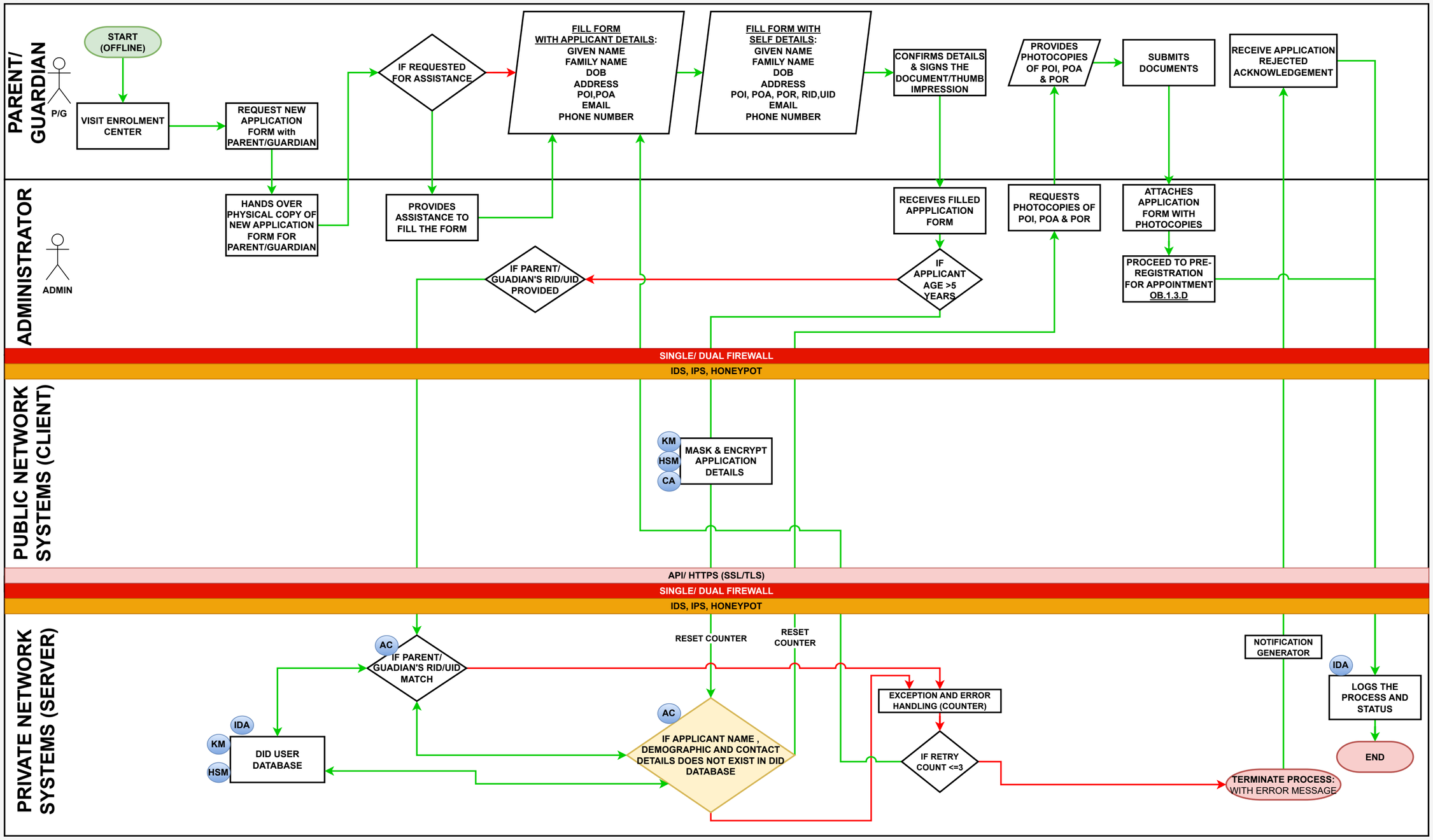
PUBLIC NETWORK

- DNS SERVERS
- FTP SERVERS
- MAIL SERVERS
- PROXY SERVERS
- WEB SERVERS

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.

B

OB.1.3 OFFLINE APPLICATION: APPLICATION BY PARENT/GUARDIAN



LEGEND

KM	Key Manager
KR	Key Revocation
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

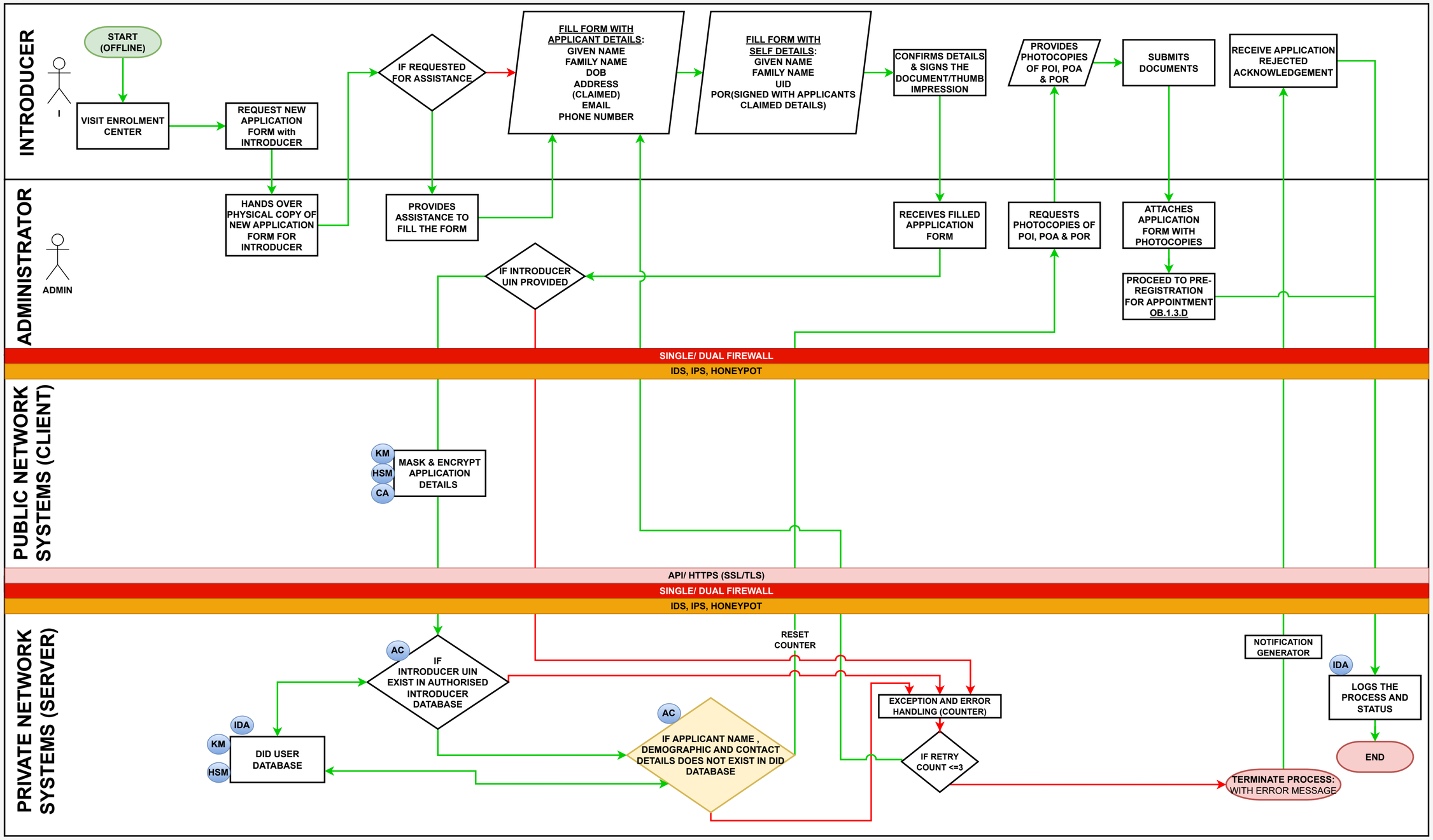
PUBLIC NETWORK

- DNS SERVERS
- FTP SERVERS
- MAIL SERVERS
- PROXY SERVERS
- WEB SERVERS

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.

Ⓒ

OB.1.3 OFFLINE APPLICATION: APPLICATION BY INTRODUCER



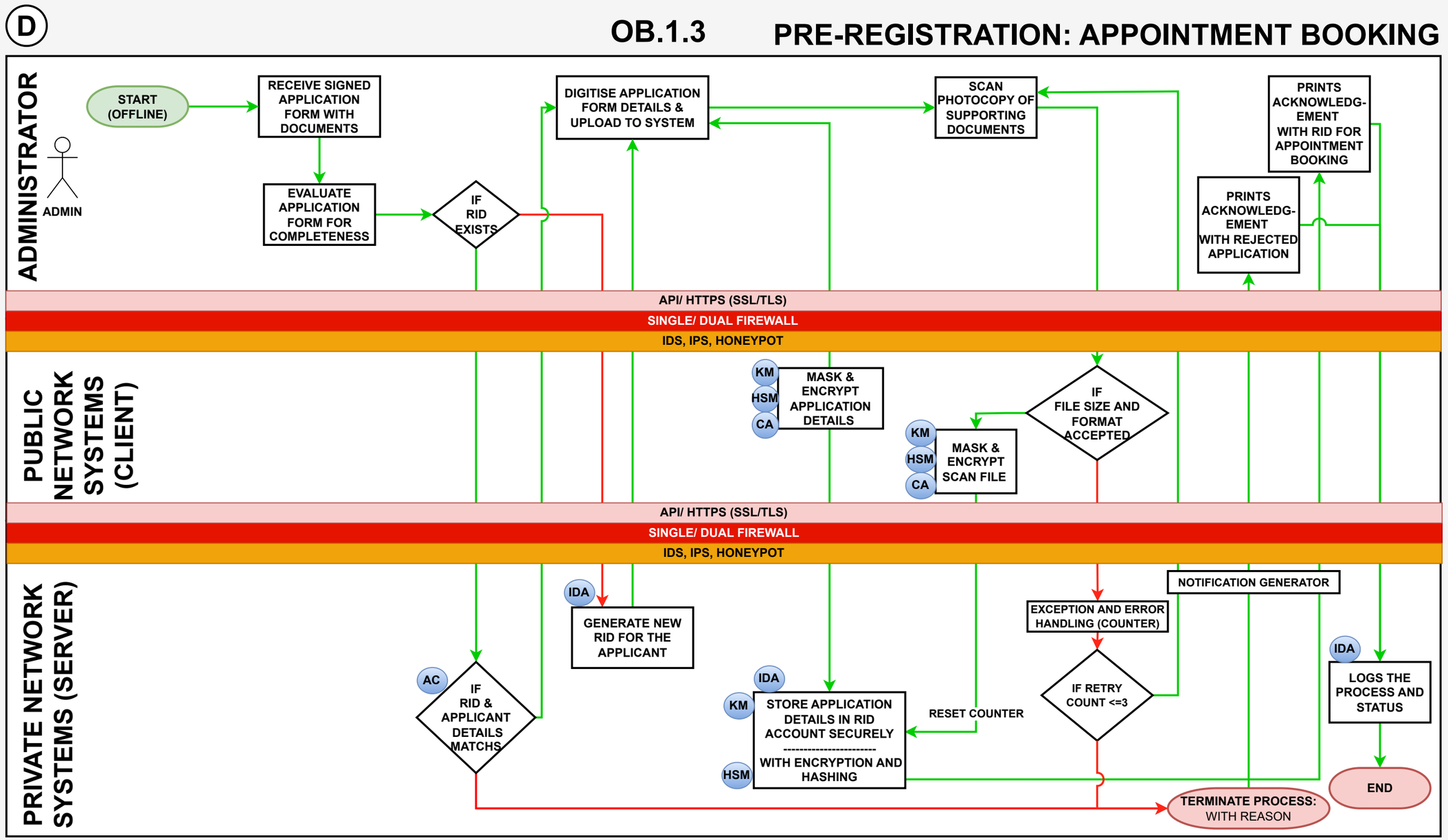
LEGEND

KM	Key Manager
KR	Key Revocation
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:
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.



LEGEND

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

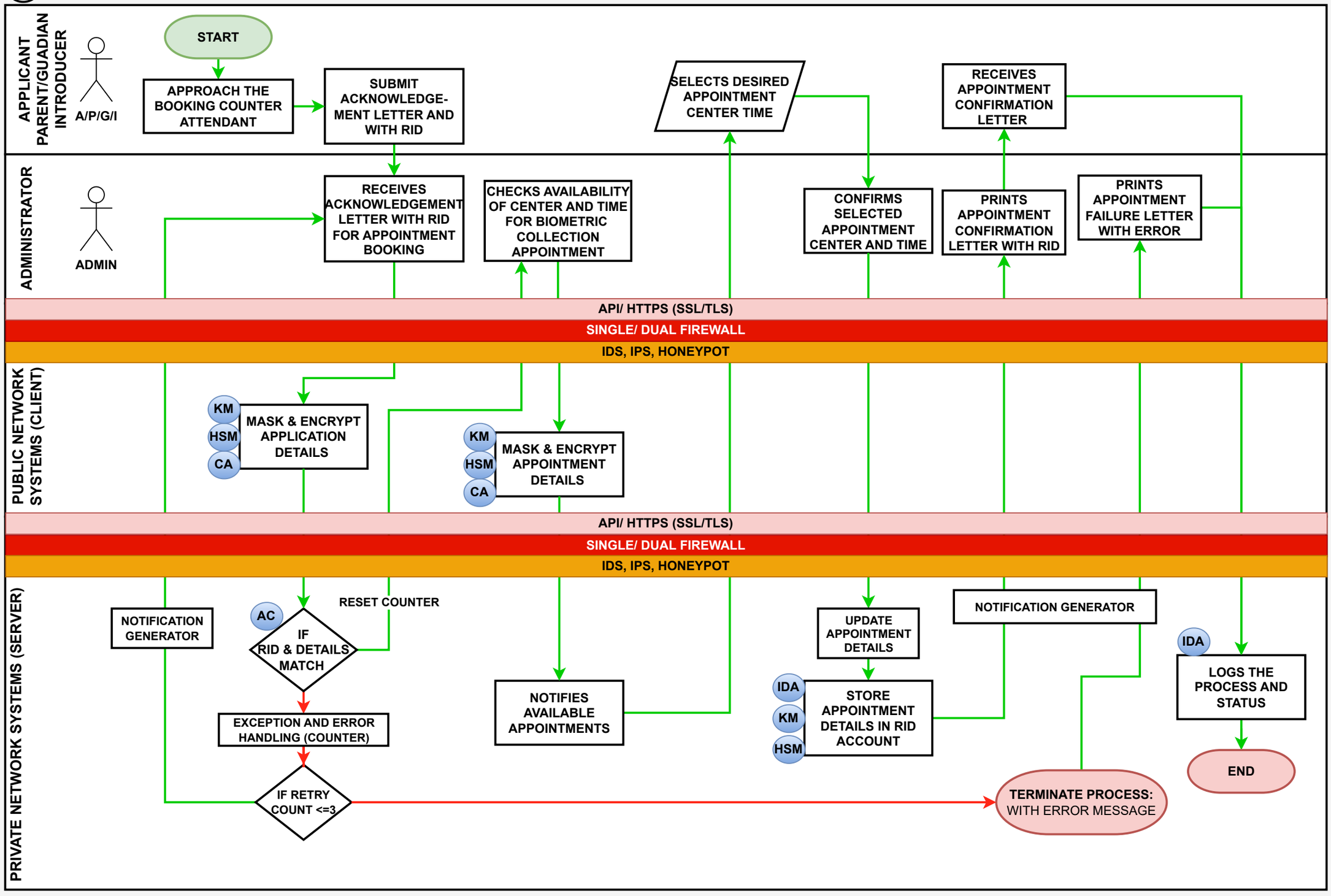
PUBLIC NETWORK

- DNS SERVERS
- FTP SERVERS
- MAIL SERVERS
- PROXY SERVERS
- WEB SERVERS

Purpose:
This SOP 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



LEGEND

KM	Key Manager
KR	Key Revocation
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 focuses on obtaining informed consent from the applicant or guardian for the collection and use of biometric data.

A

OB.1.4 OFFLINE BIOMETRIC COLLECTION: CONSENT

LEGEND

- KM — Key Manager
- KR — Key Revocation
- 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

APPLICANT

USER

START (OFFLINE)

IF SELF APPLICATION WITH DOC

VISIT THIRD PARTY/ENROLMENT CENTRE WITH APPOINTMENT CONFIRMATION LETTER

READS THE CONSENT FORM

PARTICIPANT(s) ENGAGE IN Q&A

IF CONSENT PROVIDED

RECEIVES ACKNOWLEDGEMENT OF CONSENT PROVIDED

RECEIVES ACKNOWLEDGEMENT OF FAILURE

PARENT/GUARDIAN/ INTRODUCER

P/G/I

VISIT THIRD PARTY/ENROLMENT CENTRE WITHAPPLICANT AND APPOINTMENT CONFIRMATION LETTER

BOTH READ THE CONSENT FORM

P/G/I READS THE CONSENT FORM

IF CONSENT PROVIDED

IF APPLYING WITH P/G/I

RECEIVES ACKNOWLEDGEMENT OF CONSENT PROVIDED

RECEIVES ACKNOWLEDGEMENT OF FAILURE

ADMINISTRATOR

ADMIN

IF ALL PARTICIPANTS ARRIVED

WAIT FOR ALL PARTICIPANTS TO ARRIVE

VERIFY TIME, CENTRE AND RID

PROVIDE DOCUMENT DETAILING BIOMETRIC COLLECTION, STORAGE AND USAGE (GDPR or similar compliance)

IF APPLICANT AGE <5

IF APPLYING WITH P/G/I

IF APPLICANT AGE >16

WAIT FOR PARTICIPANT(s) TO READ

AND OFFER SUPPORT FOR IMMEDIATE QUESTIONS

ORALLY EXPLAINS CONSENT DOCUMENT OFFERING Q&A

PROVIDE CONTACT DETAILS FOR FURTHER SUPPORT

REQUEST EXPLICIT CONSENT AS SIGNATURE/THUMB PRINT

ACCESSIBILITY FEATURES FOR SPECIAL CASE

SCAN AND UPLOAD CONSENT DOCUMENT

PRINT ACKNOWLEDGEMENT OF CONSENT RECEIVED

PRINT ACKNOWLEDGEMENT OF FAILURE CONSENT PROCESS WITH REASON

API/ HTTPS (SSL/TLS)

SINGLE/ DUAL FIREWALL

IDS, IPS, HONEYPOT

PUBLIC NETWORK SYSTEMS (CLIENT)

KM HSM CA — MASK & ENCRYPT RID AND APPOINTMENT DETAILS

IF SCAN SUCCESS

KM HSM CA — MASK & ENCRYPT SCANNED CONSENT DOCUMENT

API/ HTTPS (SSL/TLS)

SINGLE/ DUAL FIREWALL

IDS, IPS, HONEYPOT

PRIVATE NETWORK SYSTEMS (SERVER)

AC — IF RID & APPOINTMENT DETAILS MATCH

RESET COUNTER

IF ARRIVAL ON/BEFORE TIME

IDA KM HSM — UPDATE ARRIVAL STATUS IN RID ACCOUNT

EXCEPTION AND ERROR HANDLING (COUNTER)

IF RETRY COUNT <=3

RESET COUNTER

IDA KM HSM — STORE CONSENT DOCUMENT IN RID ACCOUNT

NOTIFICATION GENERATOR

IDA — UPDATE RID WITH CONSENT RECEIVED STATUS

TERMINATE PROCESS: NOTIFY TO RESCHEDULE APPLOINTMENT

TERMINATE PROCESS: WITH ERROR MESSAGE

IDA — LOGS THE PROCESS AND STATUS

END

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
- KR — Key Revocation
- 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

APPLICANT

USER

START (OFFLINE)

PROVIDE CONSENT OB.1.4.A

POSITIONS FACE IN FRONT OF CAMERA

POSITION APPLICANT FACE IN FRONT OF CAMERA

WITH P/G/I ASSISTANCE

RECEIVES NOTIFICATION OF SUCCESSFUL FACIAL BIOMETRIC CAPTURING SUCCESSFUL

RECEIVES NOTIFICATION OF UNSUCCESSFUL FACIAL BIOMETRIC CAPTURING

PARENT/GUARDIAN/ INTRODUCER

P/G/I

PROVIDE CONSENT OB.1.4.A

RECEIVES NOTIFICATION OF SUCCESSFUL FACIAL BIOMETRIC CAPTURING SUCCESSFUL

RECEIVES NOTIFICATION OF UNSUCCESSFUL FACIAL BIOMETRIC CAPTURING

ADMINISTRATOR

ADMIN

VERIFY CONSENT GIVEN FOR BIOMETRIC COLLECTION

IF APPLICANT AGE >5

REQUEST FACIAL SCAN OF APPLICANT

CAPTURE FACIAL IMAGE OF APPLICANT

REQUEST FACIAL SCAN OF APPLICANT

WITH P/G/I ASSISTANCE

CAPTURE FACIAL IMAGE OF APPLICANT

WITH P/G/I ASSISTANCE

RECEIVES CONFIRMATION OF FACIAL BIOMETRIC CAPTURE COMPLETED

API/ HTTPS (SSL/TLS)

SINGLE/ DUAL FIREWALL

IDS, IPS, HONEYPOT

PUBLIC NETWORK SYSTEMS (CLIENT)

KM HSM CA — MASK & ENCRYPT RID AND APPLICANT DETAILS

IF FACIAL SCAN SUCCESS

KM HSM CA — MASK & ENCRYPT FACIAL SCAN

IF FACIAL SCAN SUCCESS

API/ HTTPS (SSL/TLS)

SINGLE/ DUAL FIREWALL

IDS, IPS, HONEYPOT

PRIVATE NETWORK SYSTEMS (SERVER)

IF CONSENT GIVEN

INITIATES FACIAL BIOMETRIC COLLECTION

EXCEPTION AND ERROR HANDLING (COUNTER)

IF RETRY COUNT < = 3

RESET COUNTER

IF FACIAL BIOMETRIC DATA IS UNIQUE

IDA KM HSM — STORE FACIAL BIOMETRIC DATA IN RID ACCOUNT WITH ENCRYPTION AND HASHING

NOTIFICATION GENERATOR

NOTIFY THE PARTICIPANTS

IDA — LOGS THE PROCESS AND STATUS

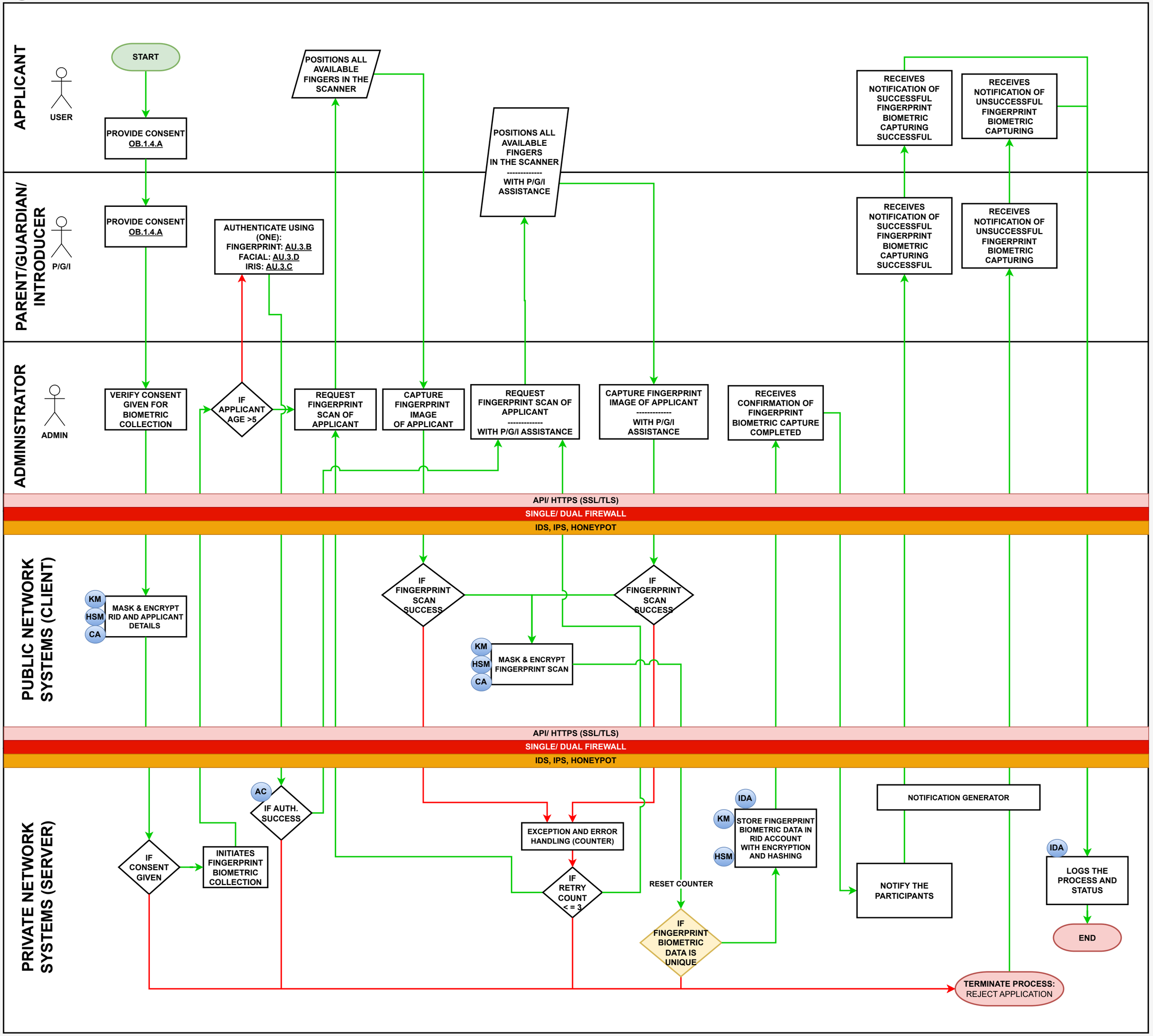
END

KR — TERMINATE PROCESS: REJECT APPLICATION

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
- KR — Key Revocation
- 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

APPLICANT

USER

START (OFFLINE)

PROVIDE CONSENT OB.1.4.A

POSITIONS IRIS IN FRONT OF CAMERA

RECEIVES NOTIFICATION OF SUCCESSFUL IRIS BIOMETRIC CAPTURING SUCCESSFUL

RECEIVES NOTIFICATION OF UNSUCCESSFUL IRIS BIOMETRIC CAPTURING

PARENT/GUARDIAN/ INTRODUCER

P/G/I

PROVIDE CONSENT OB.1.4.A

RECEIVES NOTIFICATION OF SUCCESSFUL IRIS BIOMETRIC CAPTURING SUCCESSFUL

RECEIVES NOTIFICATION OF UNSUCCESSFUL IRIS BIOMETRIC CAPTURING

ADMINISTRATOR

ADMIN

VERIFY CONSENT GIVEN FOR BIOMETRIC COLLECTION

IF APPLICANT IRIS PRESENT

REQUEST IRIS SCAN OF APPLICANT

CAPTURE IRIS IMAGE OF APPLICANT

RECEIVES CONFIRMATION OF IRIS BIOMETRIC CAPTURE COMPLETED

API/ HTTPS (SSL/TLS)

SINGLE/ DUAL FIREWALL

IDS, IPS, HONEYPOT

PUBLIC NETWORK SYSTEMS (CLIENT)

KM HSM CA MASK & ENCRYPT RID AND APPLICANT DETAILS

IF IRIS SCAN SUCCESS

KM HSM CA MASK & ENCRYPT IRIS SCAN

API/ HTTPS (SSL/TLS)

SINGLE/ DUAL FIREWALL

IDS, IPS, HONEYPOT

PRIVATE NETWORK SYSTEMS (SERVER)

IF CONSENT GIVEN

INITIATES IRIS BIOMETRIC COLLECTION

AC IF ATLEAST 1 BIOMETRIC COLLECTED

RECORD SPECIAL CASE

EXCEPTION AND ERROR HANDLING (COUNTER)

RESET COUNTER

IF RETRY COUNT < = 3

IDA KM HSM STORE IRIS BIOMETRIC DATA IN RID ACCOUNT WITH ENCRYPTION AND HASHING

IF IRIS BIOMETRIC DATA IS UNIQUE

NOTIFICATION GENERATOR

NOTIFY THE PARTICIPANTS

IDA LOGS THE PROCESS AND STATUS

END

KR TERMINATE PROCESS: REJECT APPLICATION

LEGEND

- KM — Key Manager
- KR — Key Revocation
- 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 outlines the criteria and process for the approval or rejection of an applicant's identity verification based on biometric and documentation verification.

Ⓔ

OB.1.4 APPLICATION APPROVAL/REJECTION

APPLICANT

USER

RECEIVE REJECTED APPLICATION NOTIFICATION ON EMAIL AND PHONE WITH REASON

RECEIVES SUCCESSFUL COLLECTION AND RESOLUTION NOTIFICATION ON REGISTERED EMAIL AND PHONE NUMBER

PARENT/ GUARDIAN/ INTRODUCER

P/G/I

AUTHENTICATE USING (ONE):
FINGERPRINT: AU.3.B
IRIS: AU.3.C
FACIAL: AU.3.D

RECEIVE REJECTED APPLICATION NOTIFICATION ON EMAIL AND PHONE WITH REASON

RECEIVES SUCCESSFUL COLLECTION AND RESOLUTION NOTIFICATION ON REGISTERED EMAIL AND PHONE NUMBER

ADMINISTRATOR

ADMIN

START

RECEIVES RID OF APPLICANT

CHECK COMPLETENESS OF APPLICANT DATA

FILLS APPROPRIATE REASON FOR MISSING BIOMETRIC DATA

APPROVES APPLICATION FOR IDENTITY PROOFING WITH FINAL COMMENTS

API/ HTTPS (SSL/TLS)
SINGLE/ DUAL FIREWALL
IDS, IPS, HONEYPOT

PUBLIC NETWORK SYSTEMS (CLIENT)

KM HSM CA — MASK & ENCRYPT BIOMETRIC MISSING REASON

API/ HTTPS (SSL/TLS)
SINGLE/ DUAL FIREWALL
IDS, IPS, HONEYPOT

PRIVATE NETWORK SYSTEMS (SERVER)

AC — IF RID ACCOUNT EXIST

IF ALL BIOMETRIC DATA OF APPLICANT CAPTURED

IF ATLEAST ONE BIOMETRIC DATA OF APPLICANT CAPTURED

IF BIOMETRIC DATA MISSING WITH REASON

IDA KM HSM — STORES SPECIAL CASE REASON FOR MISSING BIOMETRIC DATA IN RID ACCOUNT

IF APPLYING WITH P/G/I

IF P/G/I UIN/RID NEEDED

IF P/G/I UIN/RID PROVIDED

IF APPLICANT DEMOGRAPHIC AND BIOMETRIC DATA IS UNIQUE

AC — IF AUTH. SUCCESS

IDA KM HSM — STORE APPROVAL STATUS AND NOTIFY APPLICANT

IDA — LOGS THE PROCESS AND STATUS

END

TERMINATE PROCESS: REJECT APPLICATION

LEGEND

- KM — Key Manager
- KR — Key Revocation
- 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