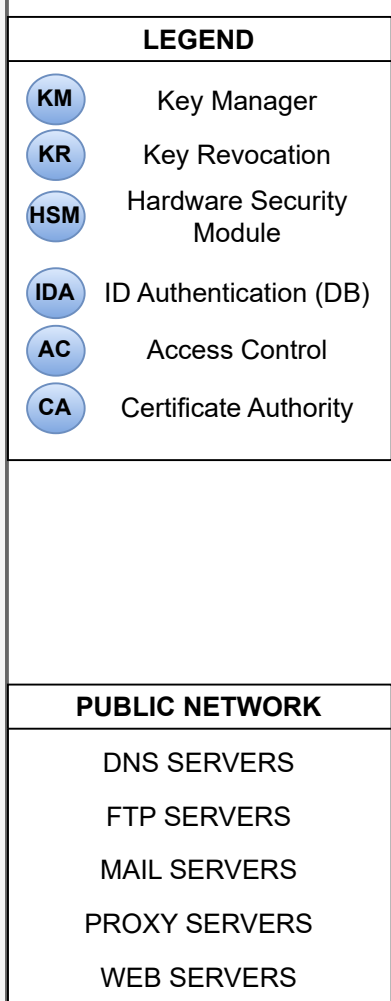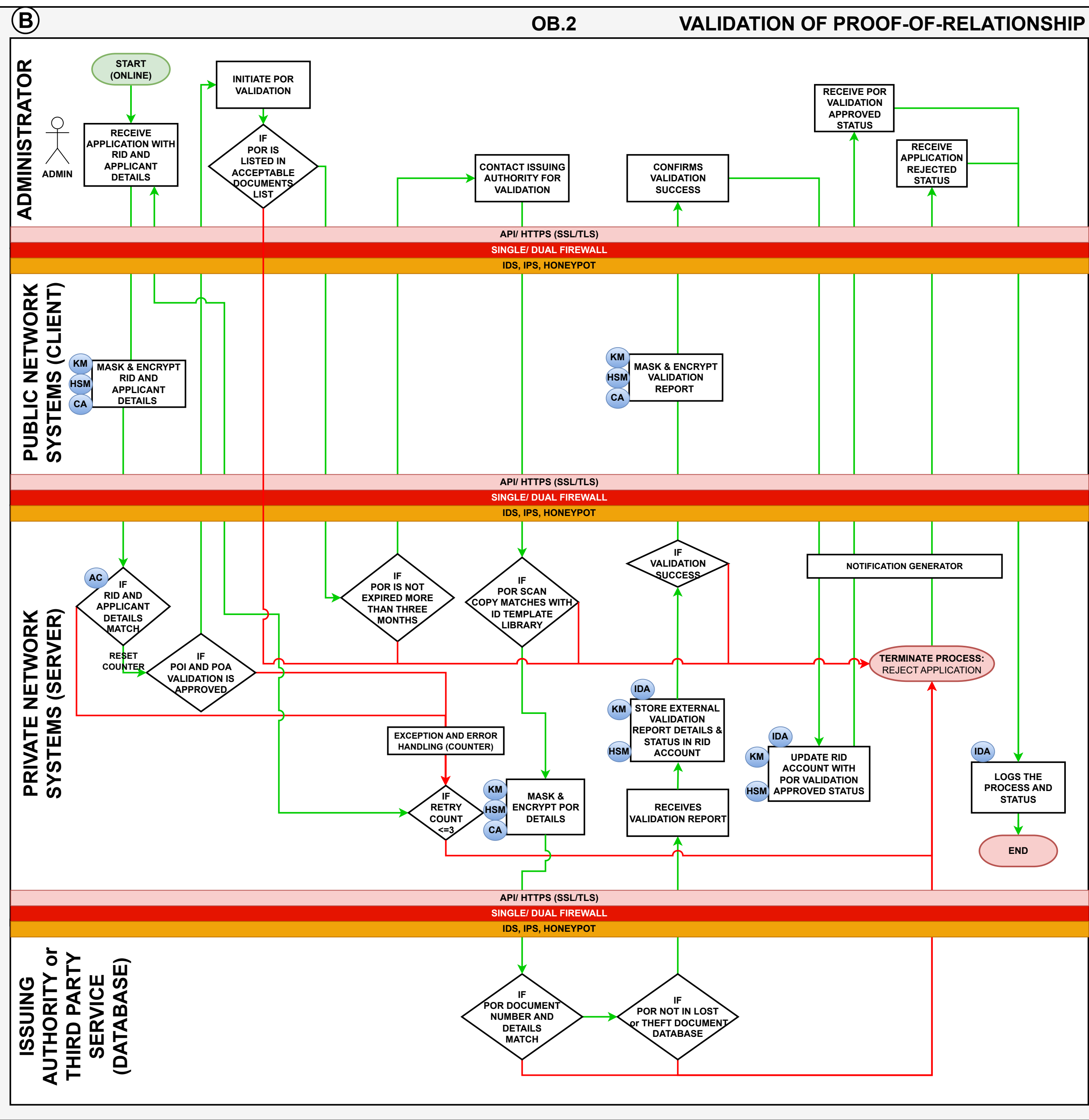**Purpose:**
This SOP details the validation process for identity and address proofs submitted by users.

(A) OB.2   VALIDATION OF PROOF-OF-IDENTITY AND PROOF-OF-ADDRESS

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

ADMINISTRATOR

ADMIN

START (ONLINE)

RECEIVE APPLICATION WITH RID AND APPLICANT DETAILS

INITIATE POI/POA VALIDATION

IF POI/POA IS LISTED IN ACCEPTABLE DOCUMENTS LIST

IF SHARE CODE IS PROVIDED BY APPLICANT

VISIT ISSUING AUTHORITY WEBSITE TO VALIDATE SHARE CODE

ENTERS POI/POA DOCUMENT NUMBER AND DETAILS WITH SHARECODE

RECEIVE VALIDATION APPROVED STATUS

CONTACT ISSUING AUTHORITY FOR VALIDATION

CONFIRMS VALIDATION SUCCESS

RECEIVE APPLICATION REJECTED STATUS

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

PUBLIC NETWORK SYSTEMS (CLIENT)

KM HSM CA — MASK & ENCRYPT RID AND APPLICANT DETAILS

KM HSM CA — MASK & ENCRYPT VALIDATION REPORT

KM HSM CA — MASK & ENCRYPT SHARECODE AND APPLICANT DETAILS

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

PRIVATE NETWORK SYSTEMS (SERVER)

AC — IF RID AND APPLICANT DETAILS MATCH

RESET COUNTER

IF COLLECTION AND RESOLUTION IS COMPLETE

IF POI/POA IS NOT EXPIRED MORE THAN THREE MONTHS

IF POI/POA SCAN COPY MATCHES WITH ID TEMPLATE LIBRARY

IF VALIDATION SUCCESS

NOTIFICATION GENERATOR

IDA — LOGS THE PROCESS AND STATUS

EXCEPTION AND ERROR HANDLING (COUNTER)

IF RETRY COUNT <=3

KM HSM CA — MASK & ENCRYPT POI/POA DETAILS

RECEIVES VALIDATION REPORT

KM IDA HSM — STORE EXTERNAL VALIDATION REPORT DETAILS IN RID ACCOUNT

KM IDA HSM — UPDATE RID ACCOUNT WITH POI/POA VALIDATION APPROVED STATUS

TERMINATE PROCESS: REJECT APPLICATION

END

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

ISSUING AUTHORITY or THIRD PARTY SERVICE (DATABASE)

IF POI/POA DOCUMENT NUMBER AND DETAILS MATCH

IF POI/POA NOT IN LOST or THEFT DOCUMENT DATABASE

IF SHARECODE AND POI/POA DOCUMENT DEATILS MATCH

---

*ACCEPTABLE DOCUMENTS LIST (COUNTRY SPECIFIC)

POI (Proof of Identity) :
All POI SHOULD have NAME, DOB & Issuing Authority details.
At lease one POI SHOULD have PHOTO, SIGNATURE.

POA (Proof of Address) :
All POA SHOULD have NAME, ADDRESS & Issuing Authority details.

Purpose:
This SOP specifies how proof of relationship documents are validated within the system.

B   **OB.2**   **VALIDATION OF PROOF-OF-RELATIONSHIP**

ADMINISTRATOR

START (ONLINE)

RECEIVE APPLICATION WITH RID AND APPLICANT DETAILS

INITIATE POR VALIDATION

IF POR IS LISTED IN ACCEPTABLE DOCUMENTS LIST

CONTACT ISSUING AUTHORITY FOR VALIDATION

CONFIRMS VALIDATION SUCCESS

RECEIVE POR VALIDATION APPROVED STATUS

RECEIVE APPLICATION REJECTED STATUS

ADMIN

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

PUBLIC NETWORK SYSTEMS (CLIENT)

KM HSM CA — MASK & ENCRYPT RID AND APPLICANT DETAILS

KM HSM CA — MASK & ENCRYPT VALIDATION REPORT

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

PRIVATE NETWORK SYSTEMS (SERVER)

AC — IF RID AND APPLICANT DETAILS MATCH

RESET COUNTER

IF POI AND POA VALIDATION IS APPROVED

IF POR IS NOT EXPIRED MORE THAN THREE MONTHS

IF POR SCAN COPY MATCHES WITH ID TEMPLATE LIBRARY

IF VALIDATION SUCCESS

NOTIFICATION GENERATOR

TERMINATE PROCESS: REJECT APPLICATION

EXCEPTION AND ERROR HANDLING (COUNTER)

IDA KM HSM — STORE EXTERNAL VALIDATION REPORT DETAILS & STATUS IN RID ACCOUNT

IDA KM HSM — UPDATE RID ACCOUNT WITH POR VALIDATION APPROVED STATUS

IDA — LOGS THE PROCESS AND STATUS

IF RETRY COUNT <=3

KM HSM CA — MASK & ENCRYPT POR DETAILS

RECEIVES VALIDATION REPORT

END

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

ISSUING AUTHORITY or THIRD PARTY SERVICE (DATABASE)

IF POR DOCUMENT NUMBER AND DETAILS MATCH

IF POR NOT IN LOST or THEFT DOCUMENT DATABASE