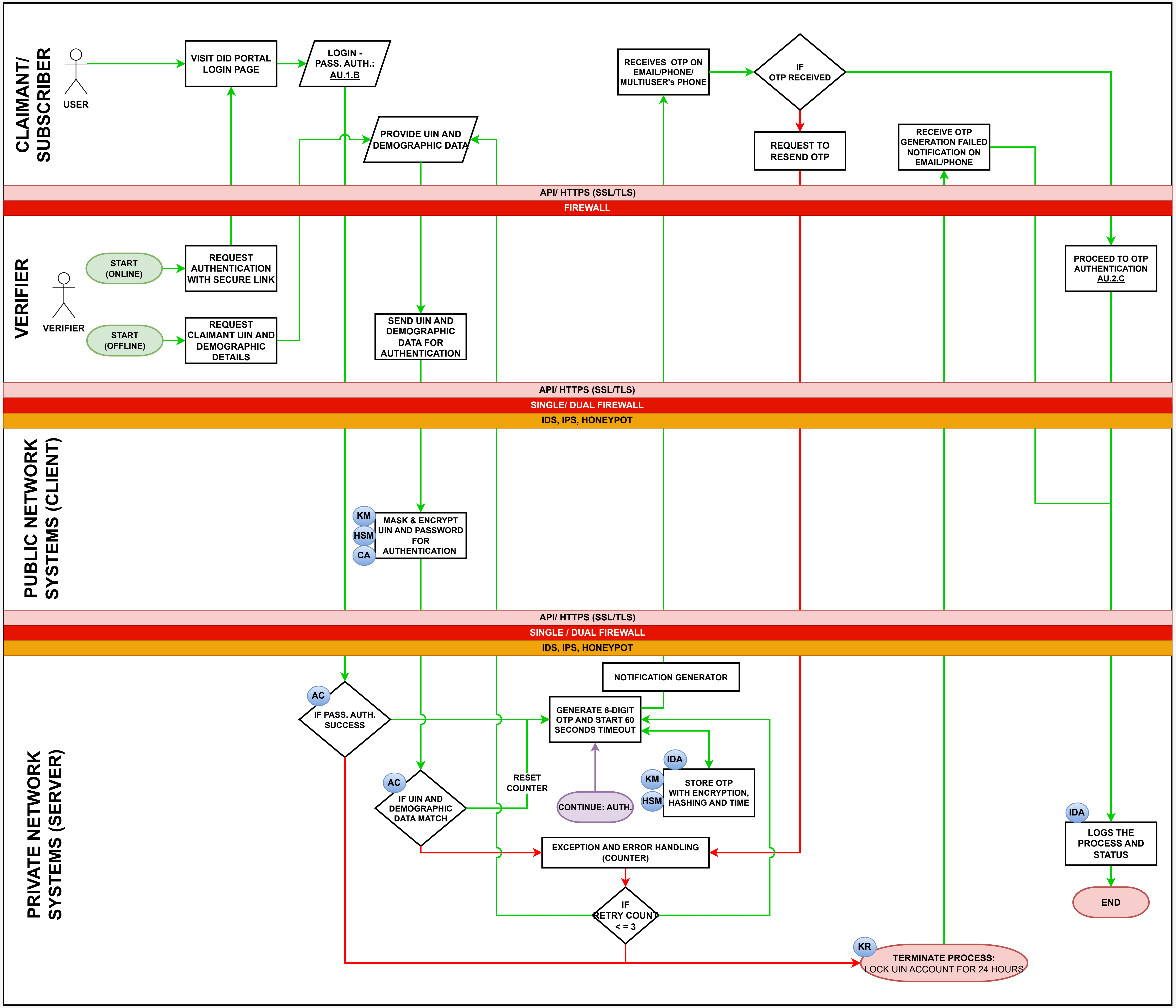
Purpose:

This SOP specifies the process for generating a one-time password for transactional security.

A

AU.2 GENERATION OF ONE-TIME PASSWORD


CLAIMANT/ SUBSCRIBER
USER
VISIT DID PORTAL LOGIN PAGE
LOGIN - PASS. AUTH.: AU.1.B
PROVIDE UIN AND DEMOGRAPHIC DATA
RECEIVES OTP ON EMAIL/PHONE/ MULTIUSER's PHONE
IF OTP RECEIVED
REQUEST TO RESEND OTP
RECEIVE OTP GENERATION FAILED NOTIFICATION ON EMAIL/PHONE
API/ HTTPS (SSL/TLS)
FIREWALL
VERIFIER
VERIFIER
START (ONLINE)
REQUEST AUTHENTICATION WITH SECURE LINK
START (OFFLINE)
REQUEST CLAIMANT UIN AND DEMOGRAPHIC DETAILS
SEND UIN AND DEMOGRAPHIC DATA FOR AUTHENTICATION
PROCEED TO OTP AUTHENTICATION AU.2.C
API/ HTTPS (SSL/TLS)
SINGLE/ DUAL FIREWALL
IDS, IPS, HONEYPOT
PUBLIC NETWORK SYSTEMS (CLIENT)
KM
HSM
CA
MASK & ENCRYPT UIN AND PASSWORD FOR AUTHENTICATION
API/ HTTPS (SSL/TLS)
SINGLE / DUAL FIREWALL
IDS, IPS, HONEYPOT
PRIVATE NETWORK SYSTEMS (SERVER)
AC
IF PASS. AUTH. SUCCESS
NOTIFICATION GENERATOR
GENERATE 6-DIGIT OTP AND START 60 SECONDS TIMEOUT
AC
IF UIN AND DEMOGRAPHIC DATA MATCH
RESET COUNTER
CONTINUE: AUTH.
IDA
KM
HSM
STORE OTP WITH ENCRYPTION, HASHING AND TIME
EXCEPTION AND ERROR HANDLING (COUNTER)
IF RETRY COUNT < = 3
KR
TERMINATE PROCESS: LOCK UIN ACCOUNT FOR 24 HOURS
IDA
LOGS THE PROCESS AND STATUS
END

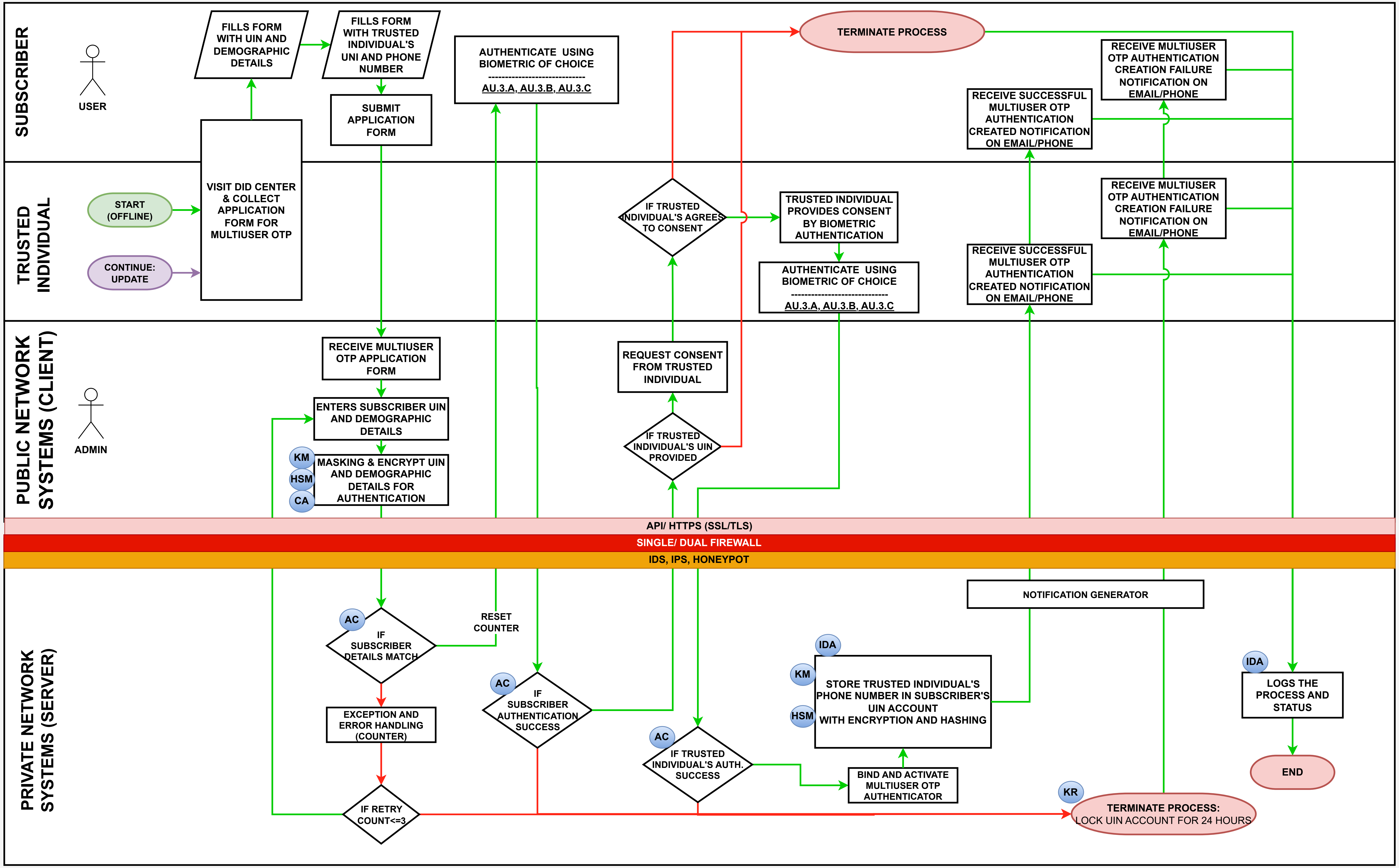
LEGEND	
KM	Key Manager
KR	Key Revocation
HSM	Hardware Security Module
IDA	ID Authentication (DB)
AC	Access Control
CA	Certificate Authority

PUBLIC NETWORK

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

Purpose:
This SOP details the creation of one-time passwords for multi-user environments.

Ⓑ AU.2 CREATION OF MULTI-USER ONE-TIME PASSWORD



SUBSCRIBER

USER

FILLS FORM WITH UIN AND DEMOGRAPHIC DETAILS

FILLS FORM WITH TRUSTED INDIVIDUAL'S UNI AND PHONE NUMBER

SUBMIT APPLICATION FORM

AUTHENTICATE USING BIOMETRIC OF CHOICE

AU.3.A, AU.3.B, AU.3.C

TERMINATE PROCESS

RECEIVE SUCCESSFUL MULTIUSER OTP AUTHENTICATION CREATED NOTIFICATION ON EMAIL/PHONE

RECEIVE MULTIUSER OTP AUTHENTICATION CREATION FAILURE NOTIFICATION ON EMAIL/PHONE

TRUSTED INDIVIDUAL

START (OFFLINE)

CONTINUE: UPDATE

VISIT DID CENTER & COLLECT APPLICATION FORM FOR MULTIUSER OTP

IF TRUSTED INDIVIDUAL'S AGREES TO CONSENT

TRUSTED INDIVIDUAL PROVIDES CONSENT BY BIOMETRIC AUTHENTICATION

AUTHENTICATE USING BIOMETRIC OF CHOICE

AU.3.A, AU.3.B, AU.3.C

RECEIVE SUCCESSFUL MULTIUSER OTP AUTHENTICATION CREATED NOTIFICATION ON EMAIL/PHONE

RECEIVE MULTIUSER OTP AUTHENTICATION CREATION FAILURE NOTIFICATION ON EMAIL/PHONE

PUBLIC NETWORK SYSTEMS (CLIENT)

ADMIN

RECEIVE MULTIUSER OTP APPLICATION FORM

ENTERS SUBSCRIBER UIN AND DEMOGRAPHIC DETAILS

KM HSM CA MASKING & ENCRYPT UIN AND DEMOGRAPHIC DETAILS FOR AUTHENTICATION

REQUEST CONSENT FROM TRUSTED INDIVIDUAL

IF TRUSTED INDIVIDUAL'S UIN PROVIDED

API/ HTTPS (SSL/TLS)

SINGLE/ DUAL FIREWALL

IDS, IPS, HONEYPOT

PRIVATE NETWORK SYSTEMS (SERVER)

AC IF SUBSCRIBER DETAILS MATCH

RESET COUNTER

EXCEPTION AND ERROR HANDLING (COUNTER)

IF RETRY COUNT<=3

AC IF SUBSCRIBER AUTHENTICATION SUCCESS

AC IF TRUSTED INDIVIDUAL'S AUTH. SUCCESS

IDA KM HSM STORE TRUSTED INDIVIDUAL'S PHONE NUMBER IN SUBSCRIBER'S UIN ACCOUNT WITH ENCRYPTION AND HASHING

BIND AND ACTIVATE MULTIUSER OTP AUTHENTICATOR

NOTIFICATION GENERATOR

KR TERMINATE PROCESS: LOCK UIN ACCOUNT FOR 24 HOURS

IDA LOGS THE PROCESS AND STATUS

END

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

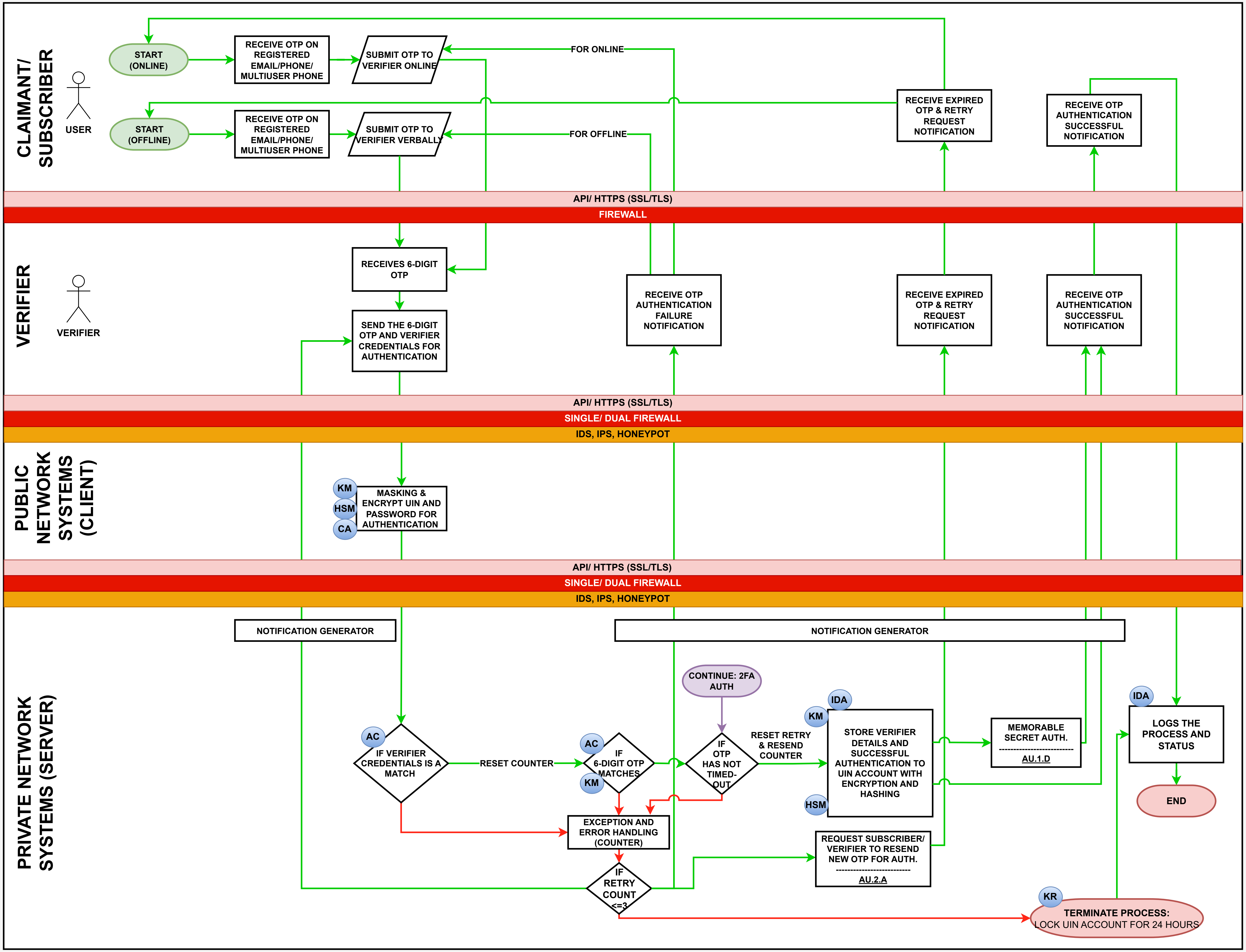
MAIL SERVERS

PROXY SERVERS

WEB SERVERS

Purpose:
This SOP guides the authentication process using multi-user one-time passwords.

AU.2 MULTI-USER ONE-TIME PASSWORD AUTHENTICATION


CLAIMANT/ SUBSCRIBER
USER
START (ONLINE)
RECEIVE OTP ON REGISTERED EMAIL/PHONE/ MULTIUSER PHONE
SUBMIT OTP TO VERIFIER ONLINE
FOR ONLINE
START (OFFLINE)
RECEIVE OTP ON REGISTERED EMAIL/PHONE/ MULTIUSER PHONE
SUBMIT OTP TO VERIFIER VERBALLY
FOR OFFLINE
RECEIVE EXPIRED OTP & RETRY REQUEST NOTIFICATION
RECEIVE OTP AUTHENTICATION SUCCESSFUL NOTIFICATION
API/ HTTPS (SSL/TLS)
FIREWALL
VERIFIER
VERIFIER
RECEIVES 6-DIGIT OTP
SEND THE 6-DIGIT OTP AND VERIFIER CREDENTIALS FOR AUTHENTICATION
RECEIVE OTP AUTHENTICATION FAILURE NOTIFICATION
RECEIVE EXPIRED OTP & RETRY REQUEST NOTIFICATION
RECEIVE OTP AUTHENTICATION SUCCESSFUL NOTIFICATION
API/ HTTPS (SSL/TLS)
SINGLE/ DUAL FIREWALL
IDS, IPS, HONEYPOT
PUBLIC NETWORK SYSTEMS (CLIENT)
KM
HSM
CA
MASKING & ENCRYPT UIN AND PASSWORD FOR AUTHENTICATION
API/ HTTPS (SSL/TLS)
SINGLE/ DUAL FIREWALL
IDS, IPS, HONEYPOT
PRIVATE NETWORK SYSTEMS (SERVER)
NOTIFICATION GENERATOR
NOTIFICATION GENERATOR
AC
IF VERIFIER CREDENTIALS IS A MATCH
RESET COUNTER
AC
IF 6-DIGIT OTP MATCHES
KM
CONTINUE: 2FA AUTH
IF OTP HAS NOT TIMED-OUT
RESET RETRY & RESEND COUNTER
IDA
KM
STORE VERIFIER DETAILS AND SUCCESSFUL AUTHENTICATION TO UIN ACCOUNT WITH ENCRYPTION AND HASHING
HSM
MEMORABLE SECRET AUTH.
AU.1.D
IDA
LOGS THE PROCESS AND STATUS
END
EXCEPTION AND ERROR HANDLING (COUNTER)
IF RETRY COUNT <=3
REQUEST SUBSCRIBER/ VERIFIER TO RESEND NEW OTP FOR AUTH.
AU.2.A
KR
TERMINATE PROCESS: LOCK UIN ACCOUNT FOR 24 HOURS

LEGEND

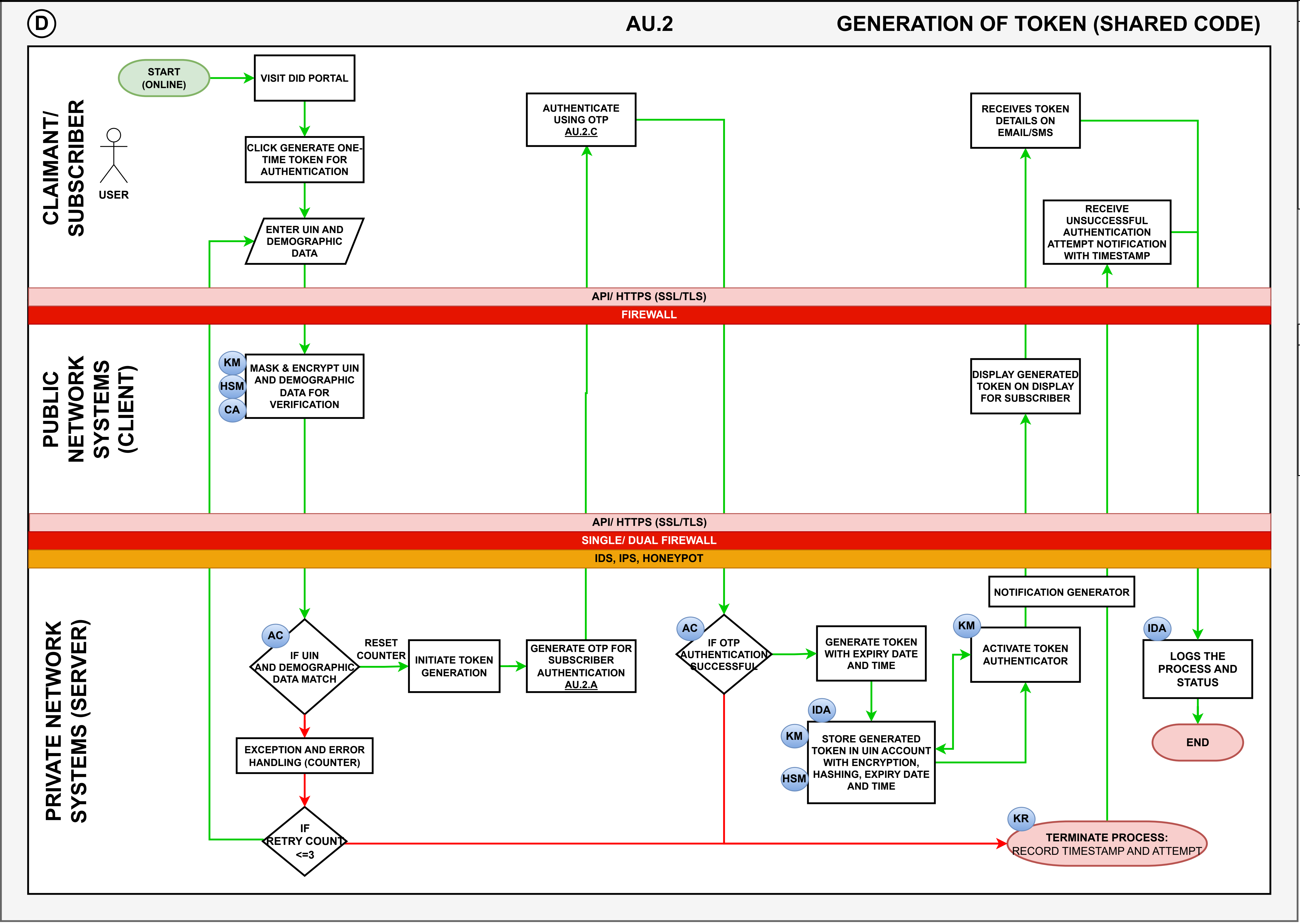
KM	Key Manager
KR	Key Revocation
HSM	Hardware Security Module
IDA	ID Authentication (DB)
AC	Access Control
CA	Certificate Authority

PUBLIC NETWORK

DNS SERVERS
FTP SERVERS
MAIL SERVERS
PROXY SERVERS
WEB SERVERS

Purpose:

This SOP guides the generation and distribution of temporary tokens for two-factor authentication, enhancing security by requiring both a password and a token for access.



D
AU.2
GENERATION OF TOKEN (SHARED CODE)
CLAIMANT/ SUBSCRIBER
USER
START (ONLINE)
VISIT DID PORTAL
CLICK GENERATE ONE-TIME TOKEN FOR AUTHENTICATION
ENTER UIN AND DEMOGRAPHIC DATA
AUTHENTICATE USING OTP AU.2.C
RECEIVES TOKEN DETAILS ON EMAIL/SMS
RECEIVE UNSUCCESSFUL AUTHENTICATION ATTEMPT NOTIFICATION WITH TIMESTAMP
API/ HTTPS (SSL/TLS)
FIREWALL
PUBLIC NETWORK SYSTEMS (CLIENT)
KM
HSM
CA
MASK & ENCRYPT UIN AND DEMOGRAPHIC DATA FOR VERIFICATION
DISPLAY GENERATED TOKEN ON DISPLAY FOR SUBSCRIBER
API/ HTTPS (SSL/TLS)
SINGLE/ DUAL FIREWALL
IDS, IPS, HONEYPOT
PRIVATE NETWORK SYSTEMS (SERVER)
AC
IF UIN AND DEMOGRAPHIC DATA MATCH
RESET COUNTER
INITIATE TOKEN GENERATION
GENERATE OTP FOR SUBSCRIBER AUTHENTICATION AU.2.A
AC
IF OTP AUTHENTICATION SUCCESSFUL
GENERATE TOKEN WITH EXPIRY DATE AND TIME
IDA
KM
HSM
STORE GENERATED TOKEN IN UIN ACCOUNT WITH ENCRYPTION, HASHING, EXPIRY DATE AND TIME
NOTIFICATION GENERATOR
KM
ACTIVATE TOKEN AUTHENTICATOR
IDA
LOGS THE PROCESS AND STATUS
END
EXCEPTION AND ERROR HANDLING (COUNTER)
IF RETRY COUNT <=3
KR
TERMINATE PROCESS: RECORD TIMESTAMP AND ATTEMPT

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

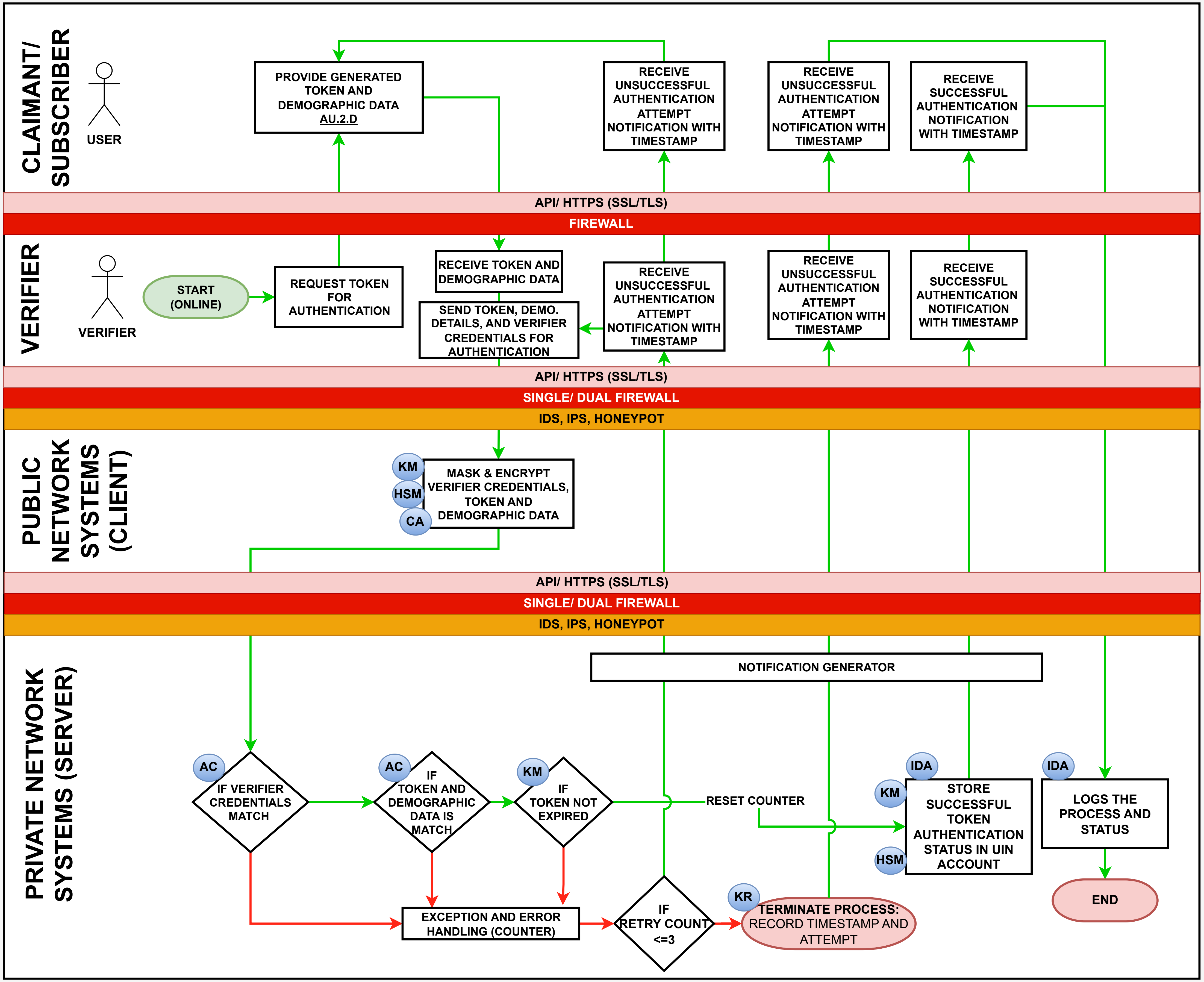
PROXY SERVERS

WEB SERVERS

Purpose:
This SOP specifies the procedure for authenticating users through tokens or shared codes.

E

AU.2 TOKEN-BASED AUTHENTICATION



CLAIMANT/ SUBSCRIBER

USER

PROVIDE GENERATED TOKEN AND DEMOGRAPHIC DATA AU.2.D

RECEIVE UNSUCCESSFUL AUTHENTICATION ATTEMPT NOTIFICATION WITH TIMESTAMP

RECEIVE UNSUCCESSFUL AUTHENTICATION ATTEMPT NOTIFICATION WITH TIMESTAMP

RECEIVE SUCCESSFUL AUTHENTICATION NOTIFICATION WITH TIMESTAMP

API/ HTTPS (SSL/TLS)

FIREWALL

VERIFIER

VERIFIER

START (ONLINE)

REQUEST TOKEN FOR AUTHENTICATION

RECEIVE TOKEN AND DEMOGRAPHIC DATA

SEND TOKEN, DEMO. DETAILS, AND VERIFIER CREDENTIALS FOR AUTHENTICATION

RECEIVE UNSUCCESSFUL AUTHENTICATION ATTEMPT NOTIFICATION WITH TIMESTAMP

RECEIVE UNSUCCESSFUL AUTHENTICATION ATTEMPT NOTIFICATION WITH TIMESTAMP

RECEIVE SUCCESSFUL AUTHENTICATION NOTIFICATION WITH TIMESTAMP

API/ HTTPS (SSL/TLS)

SINGLE/ DUAL FIREWALL

IDS, IPS, HONEYPOT

PUBLIC NETWORK SYSTEMS (CLIENT)

KM HSM CA MASK & ENCRYPT VERIFIER CREDENTIALS, TOKEN AND DEMOGRAPHIC DATA

API/ HTTPS (SSL/TLS)

SINGLE/ DUAL FIREWALL

IDS, IPS, HONEYPOT

PRIVATE NETWORK SYSTEMS (SERVER)

NOTIFICATION GENERATOR

AC IF VERIFIER CREDENTIALS MATCH

AC IF TOKEN AND DEMOGRAPHIC DATA IS MATCH

KM IF TOKEN NOT EXPIRED

RESET COUNTER

IDA KM HSM STORE SUCCESSFUL TOKEN AUTHENTICATION STATUS IN UIN ACCOUNT

IDA LOGS THE PROCESS AND STATUS

END

EXCEPTION AND ERROR HANDLING (COUNTER)

IF RETRY COUNT <=3

KR TERMINATE PROCESS: RECORD TIMESTAMP AND ATTEMPT

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