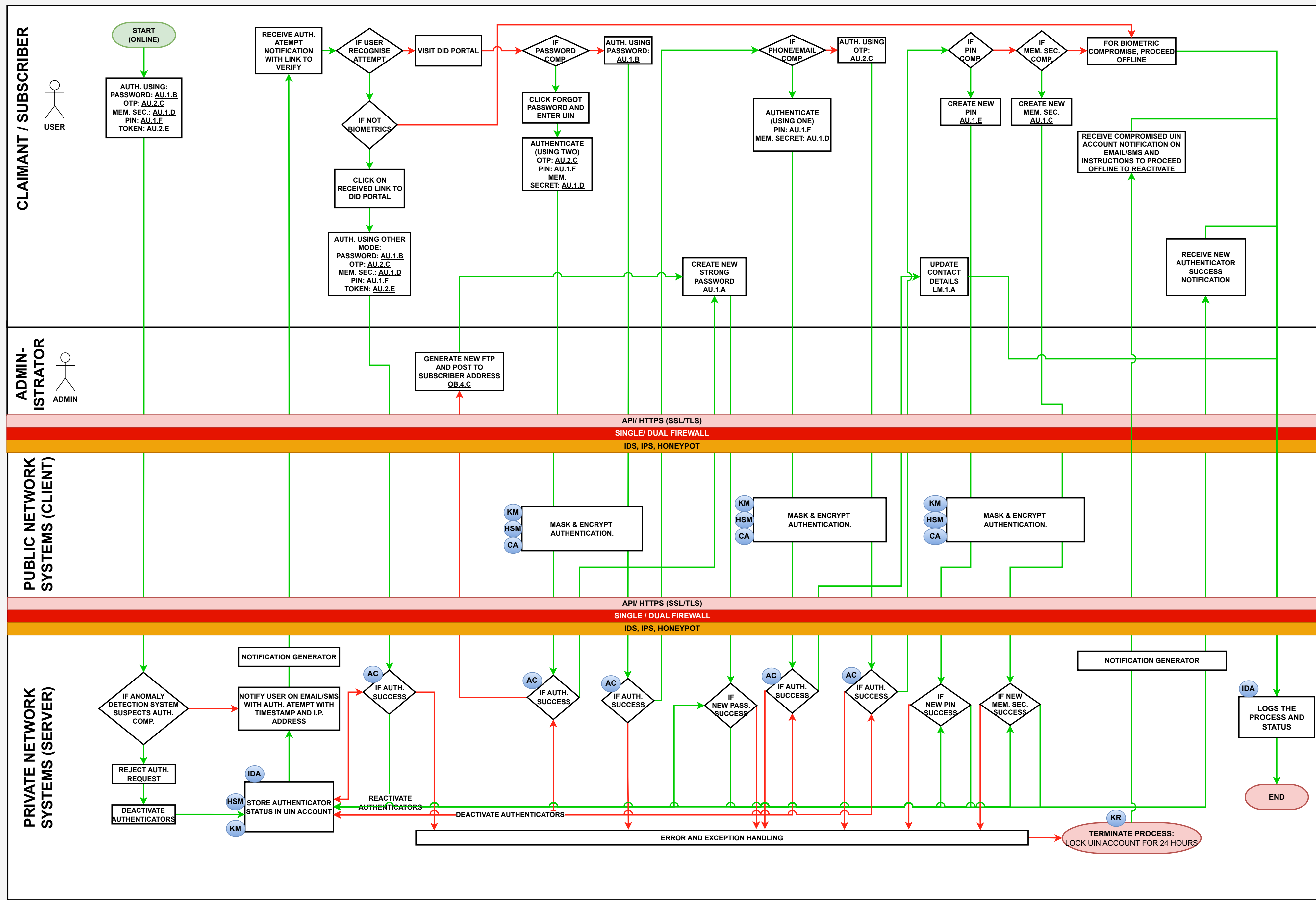**Purpose:**
This SOP specifies the process for reporting compromised security authenticators online.

(A)

LM.3

REPORTING ONLINE: COMPROMISED AUTHENTICATORS

CLAIMANT / SUBSCRIBER

USER

START (ONLINE)

AUTH. USING:
PASSWORD: AU.1.B
OTP: AU.2.C
MEM. SEC.: AU.1.D
PIN: AU.1.F
TOKEN: AU.2.E

RECEIVE AUTH. ATEMPT NOTIFICATION WITH LINK TO VERIFY

IF USER RECOGNISE ATTEMPT

VISIT DID PORTAL

IF PASSWORD COMP

AUTH. USING PASSWORD: AU.1.B

IF PHONE/EMAIL COMP.

AUTH. USING OTP: AU.2.C

IF PIN COMP

IF MEM. SEC. COMP.

FOR BIOMETRIC COMPROMISE, PROCEED OFFLINE

IF NOT BIOMETRICS

CLICK FORGOT PASSWORD AND ENTER UIN

AUTHENTICATE (USING ONE)
PIN: AU.1.F
MEM. SECRET: AU.1.D

CREATE NEW PIN
AU.1.E

CREATE NEW MEM. SEC.
AU.1.C

CLICK ON RECEIVED LINK TO DID PORTAL

AUTHENTICATE (USING TWO)
OTP: AU.2.C
PIN: AU.1.F
MEM. SECRET: AU.1.D

RECEIVE COMPROMISED UIN ACCOUNT NOTIFICATION ON EMAIL/SMS AND INSTRUCTIONS TO PROCEED OFFLINE TO REACTIVATE

AUTH. USING OTHER MODE:
PASSWORD: AU.1.B
OTP: AU.2.C
MEM. SEC.: AU.1.D
PIN: AU.1.F
TOKEN: AU.2.E

CREATE NEW STRONG PASSWORD AU.1.A

UPDATE CONTACT DETAILS LM.1.A

RECEIVE NEW AUTHENTICATOR SUCCESS NOTIFICATION

ADMIN-ISTRATOR

ADMIN

GENERATE NEW FTP AND POST TO SUBSCRIBER ADDRESS OB.4.C

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

PUBLIC NETWORK SYSTEMS (CLIENT)

KM HSM CA — MASK & ENCRYPT AUTHENTICATION.

KM HSM CA — MASK & ENCRYPT AUTHENTICATION.

KM HSM CA — MASK & ENCRYPT AUTHENTICATION.

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

PRIVATE NETWORK SYSTEMS (SERVER)

NOTIFICATION GENERATOR

IF ANOMALY DETECTION SYSTEM SUSPECTS AUTH. COMP.

NOTIFY USER ON EMAIL/SMS WITH AUTH. ATEMPT WITH TIMESTAMP AND I.P. ADDRESS

AC — IF AUTH. SUCCESS.

AC — IF AUTH. SUCCESS

AC — IF AUTH. SUCCESS

IF NEW PASS. SUCCESS

AC — IF AUTH. SUCCESS

AC — IF AUTH. SUCCESS

IF NEW PIN SUCCESS

IF NEW MEM. SEC. SUCCESS

NOTIFICATION GENERATOR

IDA — LOGS THE PROCESS AND STATUS

REJECT AUTH. REQUEST

IDA HSM KM — STORE AUTHENTICATOR STATUS IN UIN ACCOUNT

REACTIVATE AUTHENTICATORS

DEACTIVATE AUTHENTICATORS

END

DEACTIVATE AUTHENTICATORS

ERROR AND EXCEPTION HANDLING

KR — TERMINATE PROCESS: LOCK UIN ACCOUNT FOR 24 HOURS

Purpose:
This SOP details how to report compromised authenticators offline.

(B) LM.3   REPORTING OFFLINE: COMPROMISED AUTHENTICATORS

LEGEND

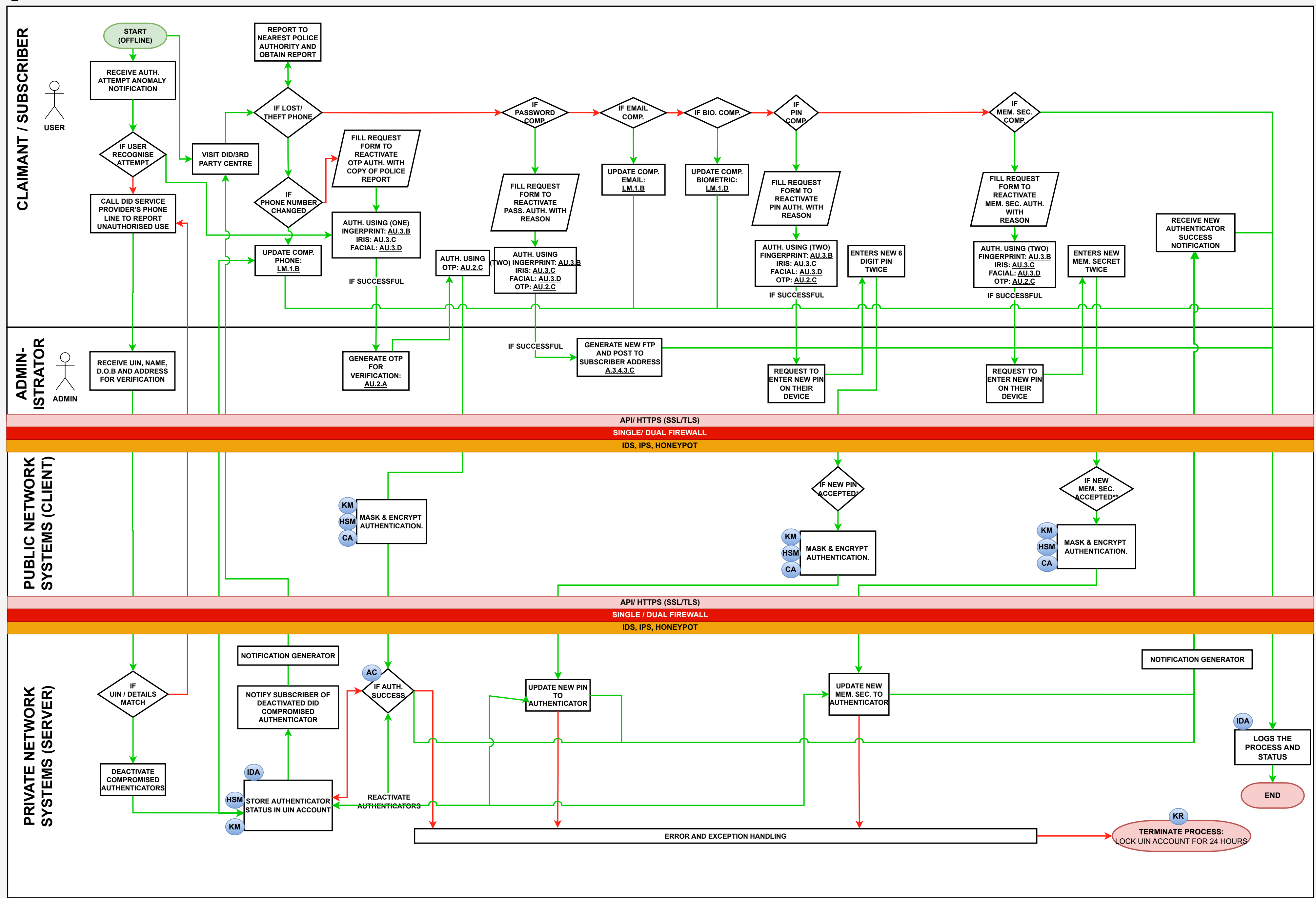|	
KM	Key Manager
KR	Key Revocation
HSM	Hardware Security Module
IDA	ID Authentication (DB)
AC	Access Control
CA	Certificate Authority

PUBLIC NETWORK

DNS SERVERS
FTP SERVERS
MAIL SERVERS
PROXY SERVERS
WEB SERVERS

CLAIMANT / SUBSCRIBER

USER

START (OFFLINE)
RECEIVE AUTH. ATTEMPT ANOMALY NOTIFICATION
IF USER RECOGNISE ATTEMPT
CALL DID SERVICE PROVIDER'S PHONE LINE TO REPORT UNAUTHORISED USE
VISIT DID/3RD PARTY CENTRE
REPORT TO NEAREST POLICE AUTHORITY AND OBTAIN REPORT
IF LOST/ THEFT PHONE
IF PHONE NUMBER CHANGED
UPDATE COMP. PHONE: LM.1.B
FILL REQUEST FORM TO REACTIVATE OTP AUTH. WITH COPY OF POLICE REPORT
AUTH. USING (ONE) INGERPRINT: AU.3.B IRIS: AU.3.C FACIAL: AU.3.D
IF SUCCESSFUL
AUTH. USING OTP: AU.2.C
IF PASSWORD COMP.
FILL REQUEST FORM TO REACTIVATE PASS. AUTH. WITH REASON
AUTH. USING (TWO) INGERPRINT: AU.3.B IRIS: AU.3.C FACIAL: AU.3.D OTP: AU.2.C
IF EMAIL COMP.
UPDATE COMP. EMAIL: LM.1.B
IF BIO. COMP.
UPDATE COMP. BIOMETRIC: LM.1.D
IF PIN COMP.
FILL REQUEST FORM TO REACTIVATE PIN AUTH. WITH REASON
AUTH. USING (TWO) FINGERPRINT: AU.3.B IRIS: AU.3.C FACIAL: AU.3.D OTP: AU.2.C
IF SUCCESSFUL
ENTERS NEW 6 DIGIT PIN TWICE
IF MEM. SEC. COMP.
FILL REQUEST FORM TO REACTIVATE MEM. SEC. AUTH. WITH REASON
AUTH. USING (TWO) FINGERPRINT: AU.3.B IRIS: AU.3.C FACIAL: AU.3.D OTP: AU.2.C
IF SUCCESSFUL
ENTERS NEW MEM. SECRET TWICE
RECEIVE NEW AUTHENTICATOR SUCCESS NOTIFICATION

ADMINISTRATOR

ADMIN

RECEIVE UIN, NAME, D.O.B AND ADDRESS FOR VERIFICATION
GENERATE OTP FOR VERIFICATION: AU.2.A
IF SUCCESSFUL
GENERATE NEW FTP AND POST TO SUBSCRIBER ADDRESS A.3.4.3.C
REQUEST TO ENTER NEW PIN ON THEIR DEVICE
REQUEST TO ENTER NEW PIN ON THEIR DEVICE

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

PUBLIC NETWORK SYSTEMS (CLIENT)

KM HSM CA — MASK & ENCRYPT AUTHENTICATION.
IF NEW PIN ACCEPTED
KM HSM CA — MASK & ENCRYPT AUTHENTICATION.
IF NEW MEM. SEC. ACCEPTED**
KM HSM CA — MASK & ENCRYPT AUTHENTICATION.

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

PRIVATE NETWORK SYSTEMS (SERVER)

IF UIN / DETAILS MATCH
NOTIFICATION GENERATOR
NOTIFY SUBSCRIBER OF DEACTIVATED DID COMPROMISED AUTHENTICATOR
AC — IF AUTH. SUCCESS
UPDATE NEW PIN TO AUTHENTICATOR
UPDATE NEW MEM. SEC. TO AUTHENTICATOR
NOTIFICATION GENERATOR
IDA — LOGS THE PROCESS AND STATUS
DEACTIVATE COMPROMISED AUTHENTICATORS
IDA HSM KM — STORE AUTHENTICATOR STATUS IN UIN ACCOUNT
REACTIVATE AUTHENTICATORS
END
ERROR AND EXCEPTION HANDLING
KR — TERMINATE PROCESS: LOCK UIN ACCOUNT FOR 24 HOURS