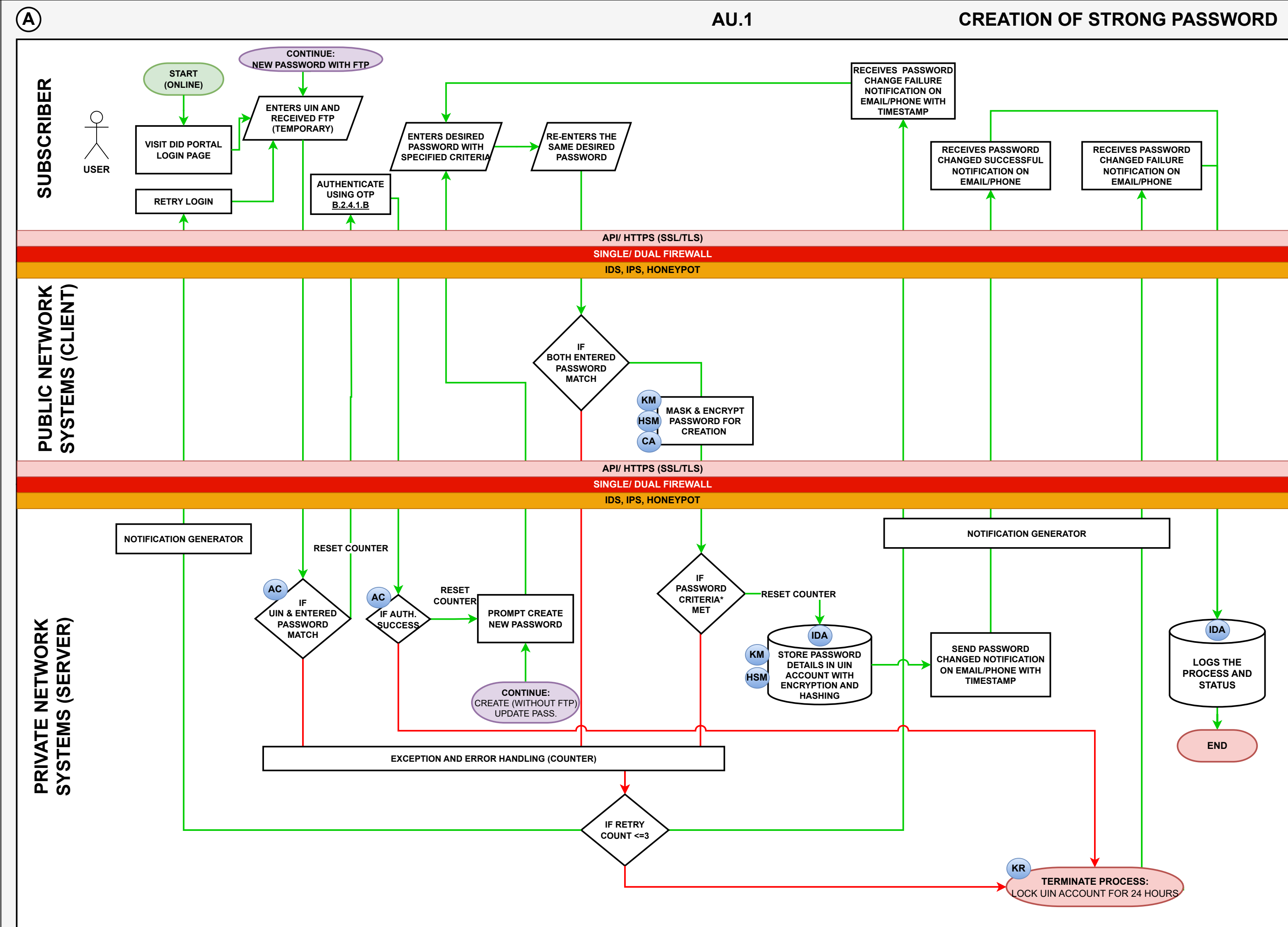








This SOP guides users in creating a strong and secure password.



***PASSWORD CRITERIA:**

- a. Should be minimum 12-character length
- b. Should be maximum 24 character length
- c. Should have character mix of upper and lower-case letters, numbers, and special characters.
- d. All printing ASCII characters as well as the space character should be acceptable.
- e. Unicode characters should be acceptable as well.
- f. If Unicode characters are accepted in memorable secret, the CSP should apply the normalisation Process for stabilized strings using either the NDKC or NFKD normalisation. (NIST SP 800 63B)
- g. Should not have any series of three consecutive characters.
- h. Should not have any consecutive space.
- i. Should be different from UID and password.
- j. Use of personal information, such as name or birthdate should be prohibited.
- K. Password should not match previous 3 passwords.

LEGEND	
	Key Manager
	Key Revocation
	Hardware Security Module
	ID Authentication (DB)
	Access Control
	Certificate Authority
FTP	FIRST TIME PASSWORD

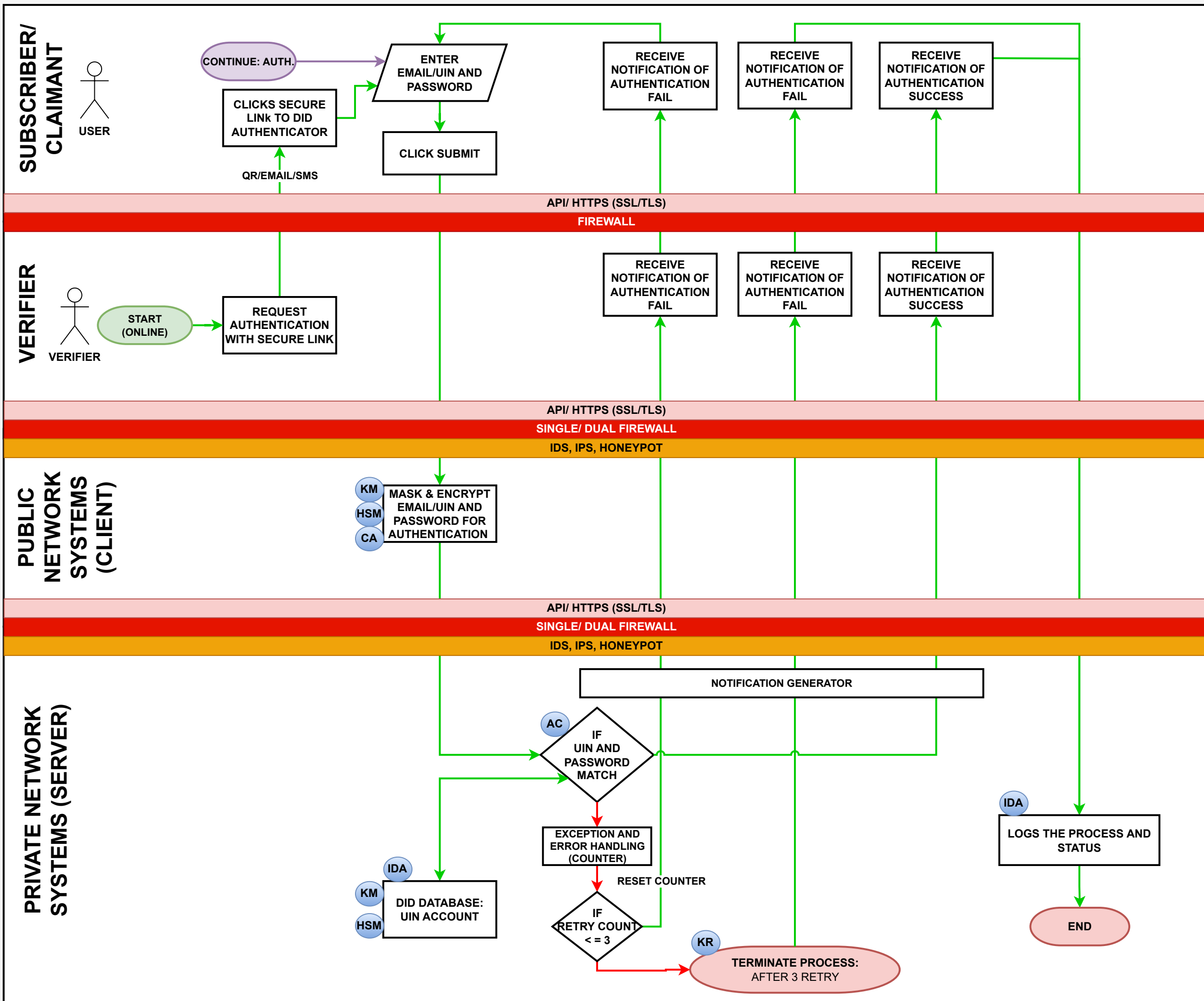
PUBLIC NETWORK
DNS SERVERS
FTP SERVERS
MAIL SERVERS
PROXY SERVERS
WEB SERVERS

Purpose:
This SOP specifies the process for authenticating users based on passwords.

(B)

AU.1

PASSWORD-BASED AUTHENTICATION



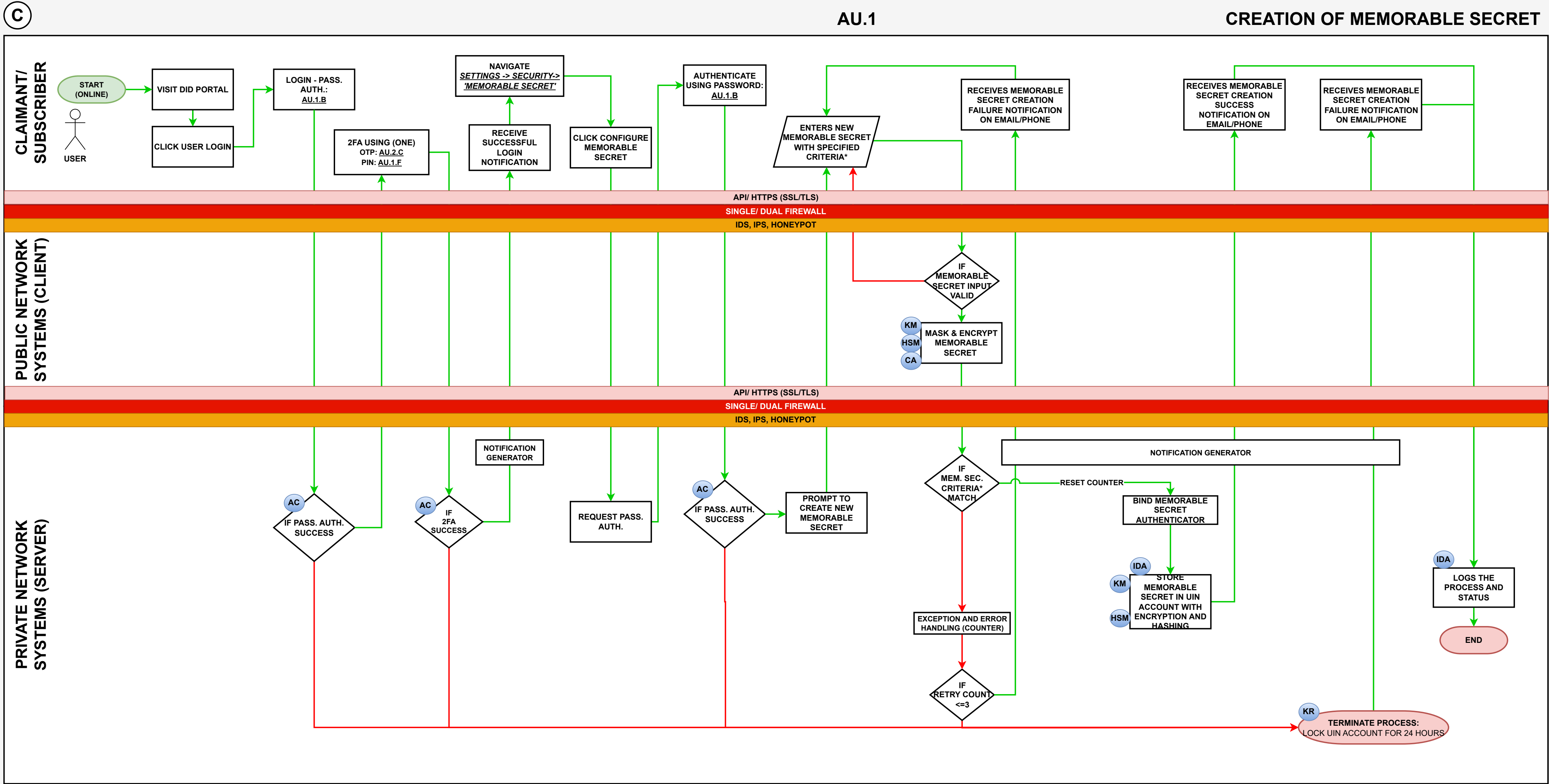
LEGEND

- 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 procedure for creating a memorable secret for authentication purposes.



***MEMORABLE SECRET CRITERIA**

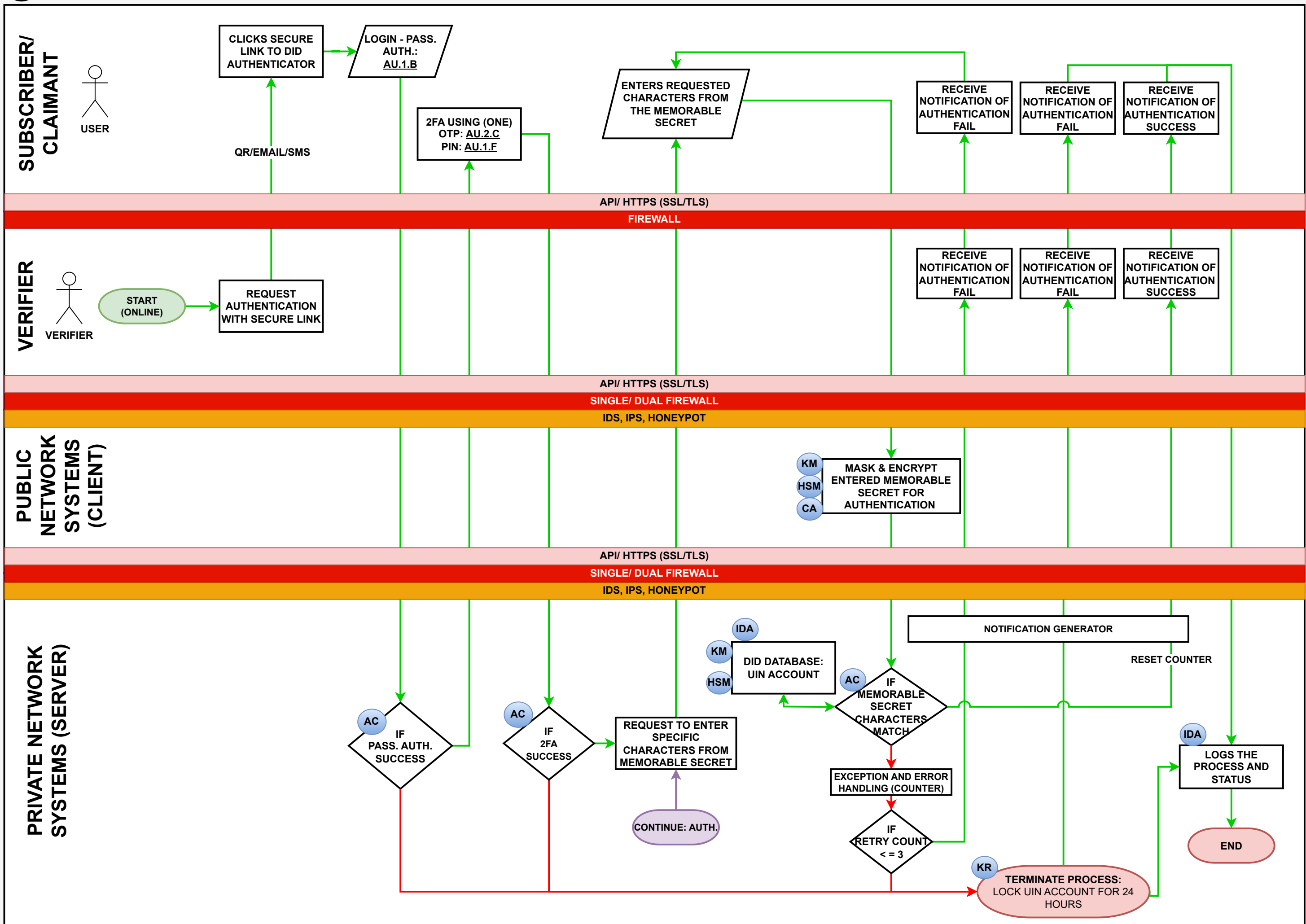
- a. Should be at least 6 characters in length.
- b. Should be at most 25 characters in length.
- c. All printing ASCII characters as well as the space character should be acceptable.
- d. Unicode characters should be acceptable as well.
- e. If Unicode characters are accepted in memorable secret, the administrator should apply the normalisation Process for stabilized strings using either the NDKC or NFKD normalisation. (NIST SP 800 63B)
- f. Should not have any series of three consecutive characters.
- g. Should not have any consecutive space.
- h. Should be different from UID and password.
- i. Should not be same as last three memorable secret.

Purpose:
This SOP outlines the authentication process using a memorable secret.

D

AU.1

MEMORABLE SECRET-BASED AUTHENTICATION



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

This SOP guides the creation of a secure personal identification number (PIN).



CREATION OF PERSONAL IDENTIFICATION NUMBER



USER

**PUBLIC
NETWORK
SYSTEMS
(CLIENT)**

PRIVATE NETWORK SYSTEMS (SERVER)

*PIN CRITERIA

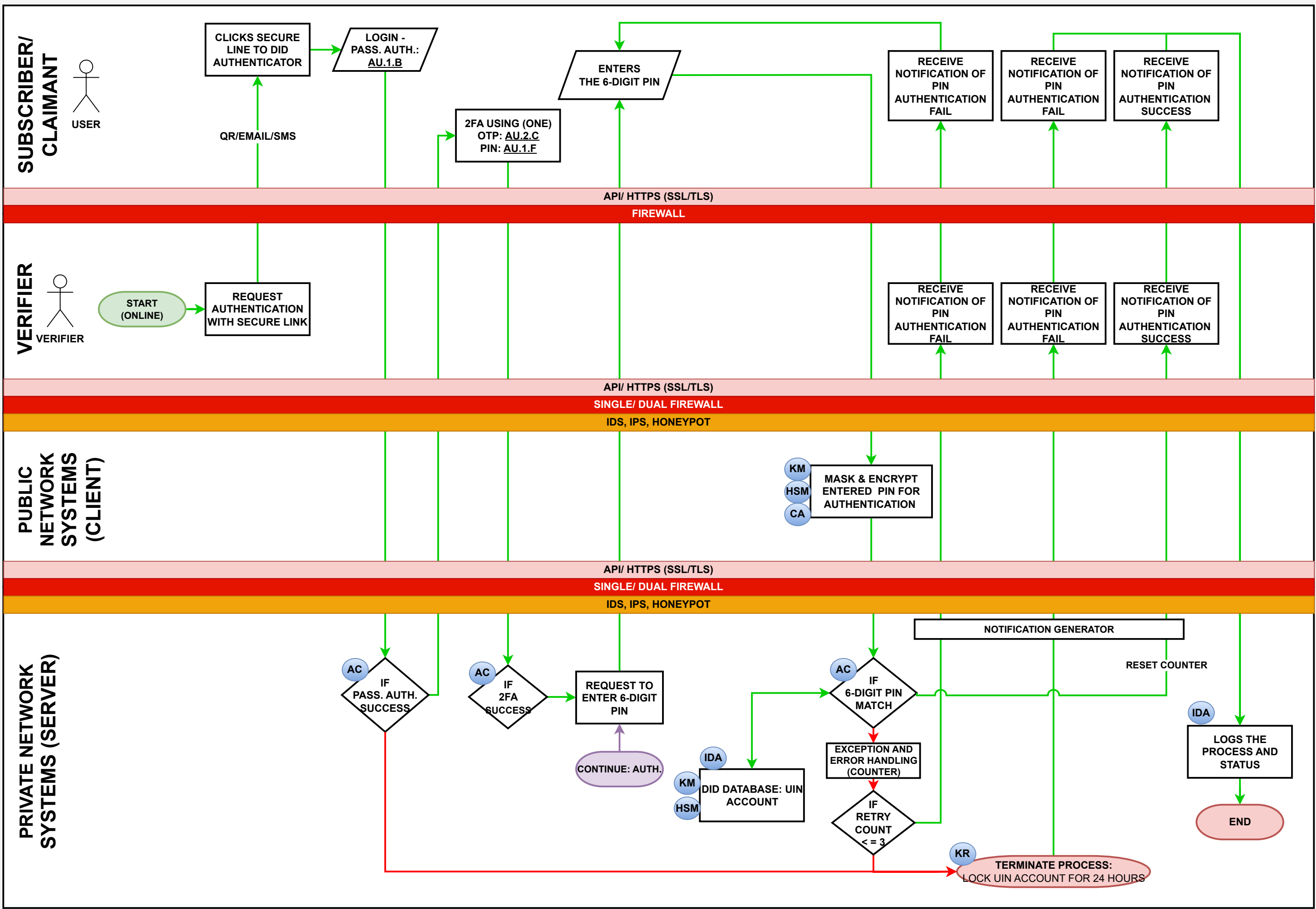
LEGEND	
KM	Key Manager
KR	Key Revocation
HSM	Hardware Security Module
IDA	ID Authentication (DB)
AC	Access Control
CA	Certificate Authority

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

Purpose:
This SOP details the PIN-based user authentication process.

F

AU.1 PERSONAL IDENTIFICATION NUMBER BASED AUTHENTICATION



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