emdha Authentication for Signature Guidelines

Issue Date:	10-Aug-2021
Effective Date:	08-Feb-2024
Document Identifier:	POL-COM-ASG-01
Version:	1.1
Document Classification:	**PUBLIC**
Document Status:	**FINAL**

Document Owner:	Naif Alshehri, Operations Manager	
Reviewer:	**Sivaraman Natrajan,** Quality Assurance & Compliance Manager	**06-Feb-2024**
Approver:	**Navaneetha Gopala Krishnan,** General Manger	**07-Feb-2024**

Document Revision History

Version	Date	Author(s)	Revision Notes and Comments
1.0	10-Aug-21	Sivaraman Natrajan	Initial Draft
1.1	28-Aug-2023	Naif Alshehri	• Updating the assurance level (Medium & High) • Adding NAFATH service authentication

Document Control

This document must be reviewed and updated with any changes to the authentication process of subscribers during the signing process.

Table of Contents

Abbreviations

Abbreviation	Description
BTC	Baud Telecom Company
CA	Certification Authority
CP	Certificate Policy, used interchangeably with “Policy”
CPS	Certification Practices Statement
IAM	Identity and Access Management
KSA	Kingdom of Saudi Arabia
KYC	Know Your Customer
OID	Object Identifier
OTP	One Time Password
PAC	Policy Authority Committee
PKI	Public Key Infrastructure
SIP	Signing Interface Provider
SNRCA	Saudi National Root Certification Authority
TSP	Trust Services Provider
UAV	User Account Vault

Definitions

"**Absher/IAM/NAFATH"** is an online portal and mobile application developed and maintained by the Ministry of Interior (MoI) that offers digital services to Saudi nationals and residents. This site is accessed using national ID number/resident permit (Iqama) number/user ID and password, and a second factor "one time password" to the registered mobile number.

"**Relying Party"** is an individual or/and entity that relies on the validity of the binding of the CA's or subscriber's identity to a public key.

"**Level of Assurance**" is a measure of the degree of confidence in the identification and authentication processes and is therefore key to establishing the reliability of the identity management system.

"User Account Vault (UAV)" is a highly secured database set up within an extremely secure and trusted zone that contains subscriber identification information obtained from a trusted and reliable source of Know Your Customer (KYC) information. The primary functions of UAV are :

- Encrypting and storing subscriber data during the registration process;
- Associating multiple authenticated roles with a registered subscriber account;
- Verifying a registered subscriber on the basis of two-factor authentication mechanism;
- Providing reliable KYC information (that has to be included in the certificate) during the digital signature process;

1. Introduction

The purpose of this document is to provide a guideline for the authentication procedures adopted by emdha for its subscribers while requesting for a digital signature service.

emdha eSign offers two levels of assurances for certificate issuance during the digital signature process, namely, Medium Level of Assurance and High Level of Assurance. The assurances are linked to the authentication credentials used by the subscriber to access the eSign remote signature service.

Medium Level of Assurance provides substantial confidence in the accuracy or legitimacy of the claimed identity. It is intended for Subscribers handling information of medium value within substantially secured environments. Identity assertions at this level are appropriate for transactions with serious (substantial) consequences to Relying Parties from the registration of a fraudulent identity.

High Level of Assurance provides high confidence in the accuracy or legitimacy of the claimed identity. It is intended for Subscribers handling information of high value within highly secured environments. Identity assertions at this level are appropriate for transactions with catastrophic consequences to Relying Parties from the registration of a fraudulent identity.

During the signing process, the subscriber selects the assurance level of the certificate for that particular transaction.

For all signing transactions, dual factor authentication is mandatory.

Assurance Type	First Factor	Second Factor
Medium Level of Assurance (Using NAFATH authentication)	National ID/Iqama Number & NAFATH verification code (Random number)	NAFATH application passcode
High Level of Assurance (Using NAFATH authentication)	National ID/Iqama Number & NAFATH verification code (Random number)	NAFAH application passcode + Biometric

2. Authentication process for Medium Level of Assurance Certificate

For Medium Level of Assurance Certificate,

1. Subscriber accesses eSign Service via emdha Signer Gateway, through SIP or Organization portal.
2. Subscriber authenticates using NAFATH service, namely,
   - National ID or Iqama Number;
   - NAFATH verification code (Random Number)
   - Nafath Application passcode

   Note : In this step the subscriber's authenticates with NAFATH service, which is a secure and reliable source of KYC information. The subscriber needs to enter the verification code (random number) that appears on emdha signing interface at the NAFATH application to proceed with the digital signature. On entering the correct verification code, followed by NAFATH Application passcode, the subscriber's identity stands authenticated, and the subscriber is allowed to proceed with the digital signature transaction.
3. Upon successful authentication, the subscriber selects the type of account to be used for the digital signature, namely, Individual or Organization. If an Organization is selected, the subscriber must further select the specific organization and the "role" within the selected organization, that shall be used for signature purposes.
4. Before proceeding with the signature, the subscriber must provide consent to use his/her information to digitally sign the documents.
5. On "role" selection and receipt of consent, UAV passes the respective KYC information of the selected UAV account to emdha eSign Service for the signing process.
6. The certificate issued to the subscriber by the eSign service is of a Medium level of assurance.

3. Authentication process for High Level of Assurance Certificate

For High Level of Assurance Certificate,

1. Subscriber accesses eSign Service via emdha Signer Gateway, through SIP or Organization portal.
2. Subscriber authenticates using NAFATH service, namely,
   - National ID or Iqama Number;

- NAFATH verification code
- NAFATH Application passcode
- NAFATH Biometric verification

Note : In this step the subscriber's authenticates with NAFATH service, which is a secure and reliable source of KYC information. The subscriber needs to enter the verification code (random number) that appeared on emdha portal at NAFATH application to proceed with the digital signature. On entering the correct verification code, followed by NAFATH application passcode, the subscriber needs to complete the biometric verification process on the NAFATH application. On completing the biometric verification, the subscriber's identity stands authenticated, and the subscriber is allowed to proceed with the digital signature transaction.

3. Upon successful authentication, the subscriber selects the type of account to be used for the digital signature, namely, Individual or Organization. If Organization is selected, subscriber must further select the specific organization and the "role" within the selected organization, that shall be used for signature purpose.
4. Before proceeding for the signature, the subscriber has to provide consent to use his/her information to digitally sign the documents.
5. On "role" selection and receipt of consent, UAV passes the respective KYC information of the selected UAV account to emdha eSign Service for the signing process.
6. The certificate issued to the subscriber by the eSign service is of High level of assurance.