emdha Identity Verification Guidelines

Issue Date:	10-Aug-2021
Effective Date:	08-Feb-2024
Document Identifier:	POL-COM-IVG-01
Version:	1.3
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 Manager	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	01-Dec-22	Sivaraman Natrajan	i) Updating the IVG to use the Self-Declaration KYC
1.2	01-Jul-23	Sivaraman Natrajan	Identity verification for DSC (Individual) Certificate Requests
1.3	30-Jul-23	Naif Alshehri	i. Updating the individual registration to use the NAFATH service ii. Update organization registration to be apply with current processes

Document Control

This document has to be reviewed and updated with any changes to the identity verification of subscribers adopted by emdha or/and enforced by regulatory bodies.

Table of Contents

Abbreviations

Abbreviation	Description
AS	Authorized Signatory
BTC	Baud Telecom Company
CA	Certification Authority
CP	Certificate Policy, used interchangeably with “Policy”
CPS	Certification Practices Statement
DSC	Digital Signature Certificate
EA	Enrolment Admin
IAM	Identity and Access Management
KSA	Kingdom of Saudi Arabia
KYC	Know Your Customer
MoI	Ministry of Interior
OID	Object Identifier
OTP	One Time Password
PAC	Policy Authority Committee
PKI	Public Key Infrastructure
RA	Registration Authority
RAO/VO	Registration Authority Officer/Validation Officer
RKA	Reliable KYC Agency
SIP	Signing Interface Provider
SMS	Short Message Service
TSP	Trust Services Provider
UAV	User Account Vault

Definitions

"CA premises" means the location where the Certifying Authority system is located.

"Registration Authority (RA) Office" means the office owned or leased by emdha for the purpose of verification of identification and address of any person registering for eSign Digital Signature Service.

"trusted person" means any person who has:-

a) direct responsibilities for the day-to-day operations, security and performance of those business activities that are regulated by emdha Certifying Authority,

OR

b) duties directly involving the issuance, renewal, suspension, revocation of Digital Signature Certificates (including the identification of any person requesting a Digital Signature Certificate from a emdha), creation of private keys or administration of a emdha CA's computing facilities.

"RA Officers (RAO)/Validation Officers (VO)" means trusted person involved in identity and address verification of digital signature applicant and approval of issuance of digital signature certificate and UAV account.

"Subscriber Identity Verification method" means the method used for the verification of the information (submitted by subscriber) that is required to be included in the Digital Signature Certificate issued to the subscriber.

"Attestation", for the purpose this document, is defined as certifying copies of document as true copies of the original.

"Digital Signature Certificate (DSC)" is a file which contains the electronic identity of a User and/or Organization with the associated Public Key generated by the Certification Authority (CA) through the use of Cryptographic methodology and Public Key Infrastructure (PKI). The CAs issue the digital certificate to a user after following a defined set of identity verification procedures. The user holds the corresponding Private Key related to the specific Public Key of the Digital Certificate, which is used to sign the electronic content digitally.

"**Absher/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.

"**Authorized Signatory (AS)**" is a personnel of an organization who has been granted the power to execute critical documents, legal/business contracts, agreements, instruments or any such documents, on behalf of the authorizing organization, thereby legally binding the organization. Also, "AS" is the only person granted rights in the emdha eSign Trust Service to use "Organization Digital Stamp/Seal" to attest any documents/contracts.

"Enrolment Admin (EA)" is an administrative role enabled in the emdha eSign Trust Service to monitor/manage the eSign Trust Service transactions specific to the organization and request/purchase eSign Trust Service counters from emdha. Also, EA has the right to enable Organization User (OU) roles (signer role) after verifying the identity and necessity of the signer to be enabled as the OU of the respective organization.

"Organization User (OU)" is a Legal Person of an organization enabled by EA, unlike Authorized Signatory, has limited capacity to sign less critical operational documents such as Invoices, Purchase Orders, Inter-department memos, etc., i.e., other than the documents that would intensely legally bind an organization into an agreement whose breach would incur severe legal consequences.

"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 identity verification procedures adopted by emdha for its subscribers prior to offering the trust services.

Identity verification is a necessary process that ensures a person's identity matches the one that is supposed to be. Identity is the attribute of identical, the correspondence of one thing with another when compared. It is the set of unique traits and characteristics associated with a unique and irreplaceable individual.

Identity verification is an essential requirement in most processes and procedures, in both online and offline environments, but it becomes more critical in online environment. This identity verification process is known as KYC (Know Your Customer).

2. General Guidelines for Subscriber Registration

1. emdha subscribers can be either Saudi nationals or non-Saudi residents of the Kingdom of Saudi Arabia. In other words, the subscribers should be holders of either a National ID Card or Resident Permit (Iqama) Card.
2. Subscriber shall visit emdha eSign Portal for the purpose of registration to avail emdha's digital signature services.
3. For all types of certificates, the identity credentials which appear in the certificate, like National ID number or Iqama Number, e-mail, mobile number and address details should be verified.
4. The mobile number and email address of subscriber is to be mandatorily provided during the registration process. The authentication credentials will be sent to the email and mobile of the subscriber. Prior to approval of the subscriber,
    - emdha eSign shall carry out an email verification either by sending a verification link or one time password (OTP) to the email of the subscriber. emdha shall log the information as part of audit logs.

AND

- emdha eSign shall send as a SMS a One Time Password (OTP) to the mobile number provided by the subscriber. The details of SMS (message id, subscriber mobile number, date and time) should be preserved as part of verification information.

5. The verified subscriber information/personally identifiable information (PII) shall be encrypted and securely stored in emdha UAV.

6. For an organization, it is a prerequisite for the "Authorized Signatory", "Enrolment Admin" and "Organization User" to be registered as individual subscribers in emdha UAV.

7. The inspection and approval of Digital Signature application form shall be carried out by a trusted person of emdha. Such approval shall be clearly indicated on the physical digital signature application form in the form of ink signature of trusted person of emdha along with name, designation and date. In the case of electronic application form, electronic approval shall be with the Digital Signature of trusted person (RA) only.

8. The application forms, supporting documents and all other verification information shall be preserved and archived by emdha for a period of 10 years.

9. emdha may ask for more supporting documents, if they are not satisfied with the documents that have been submitted.

10. emdha shall make sure that the trusted person' roles and responsibilities are not delegated to or controlled by anyone else. All the RAO(s)/VO(s) shall be employees of emdha and shall have undergone training by emdha in respect of verification.

3. Registration of Individual Person for eSign

An individual can register for emdha eSign Services using National Single Sign-On using **NAFATH** App through emdha eSign Portal or emdha mobile application:

3.1 Registration using NAFATH Service

1. On the emdha eSign Registration Portal, subscriber will opt for registration using NAFATH authentication service, wherein, he/she shall enter ID/Iqama number and complete the authentication through NAFATH application.
2. Subscriber shall authenticate as per the procedures of NAFATH application, i.e. through his/her ID/Iqama number and further authenticate through a random number that appears on emdha portal/mobile application.
3. On successful NAFATH authentication, emdha eSign shall receive a digitally signed response from NAFATH with subscriber identification details including name, national ID or Iqama number, address (city or state/emirate).
4. Subscriber shall create a UAV account by entering his/her mobile number and email address that shall be verified for possession. During this process, the subscriber shall provide his/her consent online, to:
    a) create UAV Account;
    b) emdha eSign to remote sign on his/her Subscriber Agreement
5. Subscriber registration is auto approved after complete the NAFATH authentication.

4. Registration of an Organization

4.1 Organization proof of existence/operations

The subscribing organization needs to provide proof of existence. The Organization Name (O Value) in the certificate should exactly match the organization name given below document proof :

Supporting Documents – Existence of Organization	
Category	**Documents required**
Government Entities	Copy of Royal Order letter.High resolution digital image of the Entitiy Seal to be used with Digital Stamp Certificate.
Private Entities	a) Copy of Organization Incorporation (Commercial Registration) Certificate. AND a) High resolution digital image of the Organization Seal to be used with Digital Stamp Certificate.

4.2 Registering an Authorized Signatory (AS) for the Organization

1. An Authorized Signatory (AS) shall duly authorize the Digital Signature application, which signifies as the authorization to avail digital signature services as an organizational person. The Authorized Signatory shall be verified in the form of documents given below:

Authorization to Authorized Signatories	
Category	**Documents required**
Government Entities	Authorization Letter with AS details enclosed, signed, stamped by highest position in the entity.
Private Entities	Authorization Letter with AS details enclosed, signed, stamped by AS and attested by the personnel authorized for Chamber of Commerce.

2. There can be more than one Authorized Signatory for an organization. For each additional one, the registration process remains the same as above.

4.3 Registering an Enrolment Admin (EA) for the Organization

1. The Organization shall duly authorize an Enrolment Admin (EA), who is responsible for verifying and enrolling organization users for digital signature services within the scope of organization requirements. The Enrolment Admin shall be verified in the form of documents provided below :
    - Authorization Letter mentioned EA details enclosed, signed, and stamped by the Authorized Signatory.

2. There can be more than one Enrolment Admin for an organization. For each additional one, the registration process remains the same as above.

4.4 Onboarding of an Organization

With the documents in 4.1, 4.2 and 4.3, the following conditions will apply

1. For an organization registering for emdha trust services, the onboarding documents shall be submitted as detailed below:
    - Organization/SIP agreement.
    - Organization/SIP application form
    - Authorization Letter for Authorized Signatory and Enrolment Admin
    - Proof of Organizational Existence

2. Organization shall review, sign and submit the agreement and the Application form, in hard-copy original, to emdha RA Office, along with the following:

    a) Organization shall provide the documents specified as per the category mentioned in the aforementioned tables. Organization shall authorize the AS to sign the Organization agreement, and to act as the authority from the Organization side to take and communicate all decisions with regards to the emdha Trust Services.
    b) Organization shall accept and sign Organization agreement, in hard-copy original.
    c) Organization shall provide proof of it being a licensed entity in the Kingdom of Saudi Arabia, which is verified by a RAO/VO.

3. emdha RAO(s)/VO(s) review the submitted documents against the specified organization category and on successful verification shall assign an Organization/SIP ID in emdha eSign Trust Services system

4. The organization details are verified independently by a different emdha RAO(s)/VO(s) through a reliable KYC source, and on success, the organization is approved in emdha eSign Trust Service.

5. After organization approval, notification is sent to AS and EA to proceed with mapping/association of their emdha UAV Individual account with the organization.

6. For emdha UAV Individual Account mapping/associating with concerned organization, the AS and EA shall provide their consent for their respective organization roles and authenticate using UAV Individual Account credentials. On successful verification, an "organizational role" shall be added to their profile in the UAV, along with associated "possession verified" organization email address or/and mobile number.

7. The organization, AS and EA details are verified independently by a different emdha RAO(s)/VO(s) through a reliable KYC source, and on success, the organization, AS and EA are activated in emdha eSign Trust Service.

8. The EA is responsible to vet and onboard organization personnel ("Organization User") to emdha eSign Trust Service, each of whom will provide their consent and authenticate themselves using NAFATH. The EA will provide the organization user email address and mobile number that shall be verified for possession by emdha eSign Trust Service before adding the "organization user role" mapping/association in the UAV.

4.5 Issuing of Digital Stamp

With the documents in 4.1, emdha RAO(s)/VO(s) review the submitted documents against the specified organization category and on successful verification shall issue the Digital Stamp to the Organization.

5. Request for DSC by Individual (Natural Person)

An individual (Natural Person) can request for DSC using the option below:

5.1. Request by filling up DSC Application Form

1. For new and existing subscribers, there is the option of requesting DSC through an Application Form.
2. Subscriber duly fills up the "Digital Signature Certificate Request Form (Individual)", signs it and shares it by email to emdha. Subscriber shall include along with the DSC Application form, the copy of ANY ONE of the below photo-identity documents.

   Document as proof of identity (Any one):

   a) National ID Card
   a) Residence Permit (Iqama) Card
   b) Driving License

   OPTIONALLY, to support the aforementioned identity proofs,

   a) Passport
   b) Any Government issued photo ID card bearing the signatures of the individual but has no National ID/Resident ID number.

3. emdha's RAO/VOs shall review and verify the information in the DSC Application form against the supporting photo-identity documents.
4. On approval, the DSC shall be issued on the Subscriber's crypto Token.

Annexure A – Summary of Verification

Certificate Type	Registration Type	Identity Proof	Address Proof	Email/Mobile Verification	Physical Verification
Individual	NAFATH Service	NAFATH KYC	NAFATH KYC	CA	Not Applicable
Organization	Authorized Signatory	emdha Individual UAV Account & Organization Letter	Organization Letter	CA	Not Applicable
	Enrolment Admin	emdha Individual UAV Account & Organization Letter	Organization Letter	CA	Not Applicable
	Organization User	emdha Individual UAV Account & Enrolment Admin Approval	Enrolment Admin Approval	CA	Not Applicable
	Digital Stamp	Commercial Register or equivalent	Commercial Register or equivalent	Not Applicable	Not Applicable
DSC for Individual (Natural Person)	Application Based	Photo-ID	UAV OR National RKA OR DSC Request Form	CA	Not Applicable