



emdha Identity Verification Guidelines

| | |
|--------------------------|----------------|
| Issue Date: | 10-Aug-2021 |
| Effective Date: | 27-Feb-2022 |
| Document Identifier: | POL-COM-IVG-01 |
| Version: | 1.0 |
| Document Classification: | PUBLIC |
| Document Status: | FINAL |

| | | |
|------------------------|--|-----------|
| Document Owner: | Sivaraman Natrajan, Quality Assurance Manager | |
| Reviewer: | Navaneetha Gopala Krishnan General Manager | 27-FEB-22 |

Document Revision History

| Version | Date | Author(s) | Revision Notes and Comments |
|----------------|-------------|--------------------|------------------------------------|
| 1.0 | 10-Aug-21 | Sivaraman Natrajan | Initial Draft |

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

| | |
|--|----|
| Document Revision History | 2 |
| Document Control | 2 |
| Abbreviations | 4 |
| Definitions..... | 5 |
| 1. Introduction | 7 |
| 2. General Guidelines for Subscriber Registration..... | 7 |
| 3. Registration of Individual Person | 9 |
| 3.1 Registration by filling up Application on emdha eSign Portal..... | 9 |
| 3.2 Registration using Absher/IAM Credentials (Non-Biometric)..... | 10 |
| 3.3 Registration using Absher/IAM through Biometric Credentials | 11 |
| 4. Registration of an Organization | 12 |
| 4.1 Organization proof of existence/operations..... | 12 |
| 4.2 Registering an Authorized Signatory (AS) for the Organization..... | 13 |
| 4.3 Registering an Enrolment Admin (EA) for the Organization | 14 |
| 4.4 Onboarding of an Organization..... | 14 |
| 4.5 Issuing of Digital Stamp | 15 |
| Annexure A – Summary of Verification | 16 |

Abbreviations

| Abbreviation | Description |
|--------------|--|
| AS | Authorized Signatory |
| BTC | Baud Telecom Company |
| CA | Certification Authority |
| CP | Certificate Policy, used interchangeably with "Policy" |
| CPS | Certification Practices Statement |
| EA | Enrolment Admin |
| IAM | Identity and Access Management |
| KSA | Kingdom of Saudi Arabia |
| KYC | Know Your Customer |
| Mol | 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.

"Absher" is an online portal and mobile application developed and maintained by the Ministry of Interior (Mol) 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. emdha Registration authority (RA) is responsible for verification of subscriber credentials.
4. 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.
5. 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.
6. The verified subscriber information/personally identifiable information (PII) shall be encrypted and securely stored in emdha UAV.
 7. 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.
 8. 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.
 9. The application forms, supporting documents and all other verification information shall be preserved and archived by emdha for a period of 10 years.
 10. emdha may ask for more supporting documents, if they are not satisfied with the documents that have been submitted.
 11. 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

An individual can visit emdha portal and register for emdha eSign Services using ONE of the options below:

1. Registration by filling up Application on emdha eSign Portal
2. Registration using Absher/IAM Credentials (Non Biometric)
3. Registration using Absher/IAM through Biometric Credentials

3.1 Registration by filling up Application on emdha eSign Portal

1. On the emdha eSign Registration Portal, subscriber will opt for registration by Application form submission.
2. In order to verify the identity credentials of the subscriber, he/she shall enter his/her National ID/Residence Permit number, that shall be validated against a reliable KYC agency.
3. Upon validation, subscriber shall create a UAV account by entering an alphanumeric username. This will be followed by creating a password for the UAV account and reconfirming it. 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 on approval of UAV Account by emdha RA;
4. The subscriber must provide the following details during the registration process:
 - a) National Identity Number or Residence Permit (Iqama) Number;
 - b) Email Address (that shall be verified for possession);
 - c) Mobile Number (that shall be verified for possession);
 - d) Address, that should include city, state and country;
 - e) Upload a recent picture of himself/herself;
 - f) Upload a picture/scan of a photo-identity document as mentioned in (9);
 - g) Optionally upload a self-attested scan of subscriber profile from Absher.
5. On submitting the aforementioned details, emdha eSign shall optionally connect to a Reliable KYC Agency (RKA), and validate the subscriber identity details populated in (4).

6. Each subscriber must upload a government approved and recognized photo-identity document detailed below:

Document as proof of identity (Any one):

- a) National ID Card
 - b) Residence Permit (Iqama) Card
 - c) Driving License
 - d) Passport
 - e) Any Government issued photo ID card bearing the signatures of the individual.
7. Subscriber registration shall be approved by RAO(s)/VO(s) only after the details in the application form, uploaded picture and copy of supporting document(s) have been received online and verified at emdha eSign verification Office. A trusted person would be responsible for confirming the correctness of the documents provided, before approving the subscriber registration.

3.2 Registration using Absher/IAM Credentials (Non-Biometric)

1. On the emdha eSign Registration Portal, subscriber will opt for registration by Absher/IAM credentials, wherein, he/she shall be redirected to the Absher portal.
2. Subscriber shall authenticate as per the procedures of IAM/Absher portal, i.e. through his/her Absher user ID/password and further authenticate through a second factor One Time Password (OTP) sent as SMS to his registered mobile number.
3. On successful Absher authentication, emdha eSign shall receive a digitally signed response from Absher/IAM with subscriber identification details including name, national ID or Iqama number, address (city or state/emirate), email address, subscriber picture (optional) among other information.
4. Subscriber shall create a UAV account by entering an alphanumeric username. This will be followed by creating a password for the UAV account and reconfirming it. Subsequently, subscriber shall enter his 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 on approval of UAV Account by emdha RA;

5. The subscriber must provide the following details during the registration process:
 - a) Upload a recent picture of himself/herself;
 - b) Upload a picture/scan of a photo-identity document as mentioned in (6);

6. Each subscriber must upload a government approved and recognized photo-identity document detailed below:

Document as proof of identity (Any one):

- a) National ID Card
- b) Residence Permit (Iqama) Card
- c) Driving License
- d) Passport
- e) Any Government issued photo ID card bearing the signatures of the individual.

3.3 Registration using Absher/IAM through Biometric Credentials

1. On the emdha eSign Registration Portal, subscriber will opt for registration by Absher/IAM credentials.
2. Subscriber shall enter his National ID/Residence Permit number and provide his/her biometric.
3. On successful Absher authentication, emdha eSign shall receive a digitally signed response from Absher/IAM with subscriber identification details including name, national ID or Iqama number, address (city and state/emirate), email address, subscriber picture (optional) among other information.
4. Subscriber shall create a UAV account by entering an alphanumeric username. This will be followed by creating a password for the UAV account and reconfirming it. Subsequently, subscriber shall enter his mobile number and email address that shall be verified for possession.
5. During this process, the subscriber shall provide his/her consent online, to :
 - a) create UAV Account;
 - b) register for digital signature services; AND

- c) emdha eSign to remote sign on his/her Subscriber Agreement on approval of UAV Account by emdha RA;
6. In this registration scenario, the subscriber is automatically approved and does not need any further verification and approval from emdha RAO/VO.

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 |
| Corporate Entities (Licensed by Ministry of Commerce and Industry (MoCI)) | <ul style="list-style-type: none"> a) Original Bank Statement with transactions not less than 3 months of recent past, signed by the Bank. Bank Statement should be in the “organization name”. As an alternate to bank statement, a signed letter from the bank confirming the account existence with organization name can be provided; OR/AND b) Copy of Commercial Registration Certificate. AND a) High resolution digital image of the Organization Seal to be used with Digital Stamp Certificate. |
| Other Entities (Universities, Ministries, Trusts etc.) | <ul style="list-style-type: none"> b) Original Bank Statement with transactions not less than 3 months of recent past, signed by the Bank. Bank Statement should be in the “organization name”. As an alternate to bank statement, a signed letter from the bank confirming the account existence with organization name can be provided; OR/AND c) Copy of Organization Incorporation Certificate. AND d) 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 |
| Individual/Proprietor ship Firm: | <ol style="list-style-type: none"> 1. Business registration certificate containing name of the proprietor confirming the business ownership of AS (Proprietor). 2. If AS is not the Proprietor, an Authorization Letter with Photo-ID of AS enclosed, signed by the Proprietor and attested by Chamber of Commerce. |
| Partnership Firm: | <ol style="list-style-type: none"> 1. Copy of List of partners from Partnership Deed. (First page and page(s) containing Authorized Signatory/Partner Name) 2. If AS is not a partner, an Authorization Letter with Photo-ID of AS enclosed, signed by a partner and attested by Chamber of Commerce. 3. Optionally Organizational ID card of AS shall be enclosed. |
| Corporate Entities | <ol style="list-style-type: none"> 1. Copy of List of Directors. emdha RA shall cross verify such details from a reliable source. 2. If AS is not a director, Board Resolution OR Power of Attorney with Photo-ID of AS enclosed, attested by Chamber of Commerce. 3. Organizational ID card of AS shall be enclosed. |
| Limited Liability Company | <ol style="list-style-type: none"> 1. Copy of List of Directors. emdha RA shall cross verify such details from a reliable source. 2. If AS is not a director, Board Resolution OR Power of Attorney with Photo-ID of AS enclosed, attested by Chamber of Commerce. 3. Organizational ID card of AS shall be enclosed. |

| | |
|--|---|
| Non-Government Organization (NGO) /Trust | <ol style="list-style-type: none"> 1. Copy of resolution from the NGO / Trust authorizing the signatory with Photo-ID of AS enclosed, and attested by Chamber of Commerce. 2. Organizational ID card of AS shall be enclosed. |
|--|---|

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 with Photo-ID of EA enclosed, signed by the Authorized Signatory and attested by the Chamber of Commerce.
 - Organizational ID card of Enrolment Admin.
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 digital signature application form shall be submitted as detailed below:
 - Organization/SIP Onboarding Form
 - Authorization Letter for Authorized Signatory and Enrolment Admin
 - Authorized Signatory and Enrolment Admin Identity Proof
 - Proof of Organizational Existence
2. Organization shall fill, sign and submit 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.
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 UAV or IAM/Absher credentials. 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.

Annexure A – Summary of Verification

| Certificate Type | Registration Type | Identity Proof | Address Proof | Email/Mobile Verification | Physical Verification |
|---------------------|------------------------------------|--|-----------------------------------|---------------------------|-----------------------|
| Individual | Application Based | Photo ID | National RKA | CA | Not Applicable |
| | Absher Credentials (Non-Biometric) | Absher KYC | Absher KYC | CA | Not Applicable |
| | Absher Credentials (Biometric) | Absher KYC | Absher KYC | CA | Biometric |
| Organization | Authorized Signatory | emdha Individual UAV Account, Photo ID & Organization Letter | Organization Letter | CA | Not Applicable |
| | Enrolment Admin | emdha Individual UAV Account, Photo ID & 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 |