certME Service Procedures

Document code: [Subject]

Document Version/Date: **v.1.0 - Feb.2021**

Document Security Level: **Public**

Important Notice

This document is property of certSIGN S.A.

Address: 29 A Tudor Vladimirescu Avenue,
AFI Tech Park 1, Bucharest, Romania
Phone: 004-031.101.1870
Web: www.certme.ro

Document History

Version	Date	Reason	The person who made the change
0.1	June 2020	Draft First version publishing	Policies Manager
0.2	July 2020	Procedures updates	Policies Manager
0.3	Feb.2021	Layout & corrections	Policies Manager
0.4	Feb. 2021	Corrections	Product Owner
1.0	Feb. 2021	First version	Product Owner

This document was created and is the property of:

Owner	Author	Date created
certME	PKI Policies Manager	June 2020

Distribution List

Destination	Date distributed
Public-Internet	

This document was approved by:

Version	Name	Date
1.0	Policies and Procedures Management Body	

Content

1 Introduction

Governments and companies alike are becoming more and more digital. Delivery of both public and private sector digital services requires a lot of user data. This raises a huge issue for service providers when it comes to ensuring the cyber security of their databases.

Digital services that involve certain risks must be based on legally binding digital interactions that require trusted identities and trusted user data. This raises another issue for service providers, as identities and their associated digital data need to have a high level of assurance.

At the same time, the GDPR Regulation requires service providers to give users complete control over their personal data. This raises an issue regarding transparency of data processing and traceability of access to data.

certME enables digital service providers to operate by providing trusted identity and personal data validation as a service. certME aims to deliver identity management and validation services using blockchain technology. The certME decentralized identity platform aims to support a complex digital ecosystem for all companies with needs and responsibilities in the identity validation area, such as banks, telcos and many more.

By using blockchain technology, the certME service is by design GDPR compliant. User identity hash data is stored in encrypted form on the blockchain and each user controls access of other users to their identity attributes. Identity providers within the ecosystem validate identity attributes, making user interactions legally binding in any EU member state.

By using blockchain and smart contract technology to store encrypted data, the certME platform ensures that data cannot be altered by any unauthorized parties and that the service has the highest possible availability. certME allows users to securely store their identity data within the wallet provided by the certME mobile DApp (decentralized application), while the blockchain only stores hashed and encrypted data.

Using certSIGN's infrastructure, with eIDAS compliant procedures and a large network of certified partners, certME identities and their associated digital data have a high level of assurance. This is how the electronic identity is bound to the real identity.

The certME mobile DApp allows users to give access to one or more data attributes associated with his/her identity. Coupled with the default transparency and traceability provided by blockchain technology, this ensures that access to data is logged with a very high degree of granularity.

1.1 Overview

certME is a B2B digital service delivered via a several DApps (mobile, web and API) that interact with smart contracts on a blockchain platform. The certME ecosystem supports three nonexclusive user roles: user (the data owner), service provider (data consumer) and validator (authorized identity verifier and data validator).

First, the user needs to install the certME mobile app on his device and meet with a validator to have his identity data checked. The validator stores proofs of verification of the user's data attributes to the blockchain and a certME smart-contract issues the certME eID of the user. Then, using his certME eID the user can register and authenticate to a service provider's website in order to receive services. The provider checks that the personal data provided by the certME mobile app represents a valid identity of a verified user. Using the certME API, the provider automatically sends a request for validation of the user's attributes to a smart contract sitting on the blockchain. Pursuant to the request, the user and its validator receive push notifications. The user responds to the notification with one tap on his mobile app. By responding to the request, the user sends to the smart contract his consent to have his identity validated by the service provider. Following the user's consent, the validator responds to the request by sending to the smart contract the proofs of verification of the user's attributes. After that, the provider checks that the data sent by the user corresponds to the proofs indicated by the validator, thus by completing the validation process.

This document presents the procedures that a certME Scheme Manager uses in order to maintain the whole certME ecosystem.

1.2 Document name and identification

This document represents the certME Service Procedures employed by the Scheme Manager in order to deliver the certME service.
The document is available in electronic format within the certME Repository

2 Participants

The certME ecosystem include the following nonexclusive user roles: **System/Scheme manager** (certSIGN) **User** (data owner), **Service Provider** (data consumer) and **Validator** (authorized identity verifier and data validator).

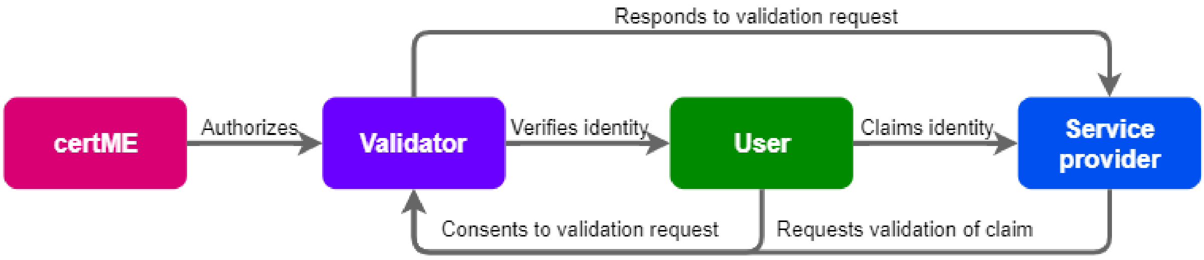
Responds to validation request
certME
Authorizes
Validator
Verifies identity
User
Claims identity
Service provider
Consents to validation request
Requests validation of claim

Figure 2-1 certME ecosystem participants

The **document** regulates the most important relations between entities belonging to certME, the advisory teams (including auditors) and customers/clients (users of the provided services).

2.1 System/Scheme manager - certME

Scheme manager - as legal representative of the certME eID scheme, the certSIGN company holds the ***Scheme manager*** role. By granting or revoking specific permissions on the certME smart-contracts, the scheme manager a) authorizes/deauthorizes *Validators* to register Users and request issuance, suspension, reactivation and revocation of electronic identification means; and b) authorizes/deauthorizes *Service Providers* to issue *User* authentication/validation requests. The *Scheme manager* can also suspend, reactivate or revoke any identification means in case of lost or compromised mobile devices. The scheme manager is also responsible for operating the authentication mechanism.

2.2 Validator

Validator – A certME partner organization authorized to:

- perform identity proofing,
- verify users' person identification data,
- register user's person identification data,
- request issuance, suspension, revocation and reactivation of electronic identification means and
- confirm credential validity checks registered by service providers on the smart-contracts.
  - A Validator can only respond to credential validity checks that are authorized by users and that concern users verified by said Validator.

2.3 Service Provider

Service Provider - is a certME client organization authorized to issue authentication requests and credential validity checks on behalf of *Users*. A *Validator* can also act as a *Service Provider* when interacting with *Users* enrolled by other *Validators*.

2.4 User

User – Is a natural person that has undergone an identity proofing, verification and registration process performed by a validator and has been issued a certME electronic identification means that can be used to register/authenticate to a service provider. Every authentication request issued by a service provider on behalf of a user, must be initiated and authorized by the user.

3 Scheme Manager Procedures Workflow

The generic workflow for the Scheme Manager within the certME ecosystem has the following main modules:

- Attributes Management
  - Add/activate/inactivate certME eID supported attributes
- Enrolments
  - For Service Providers
  - For Validators
- Management - Support / Updates / End of usage
  - For Users
  - For Service Providers
  - For Validators

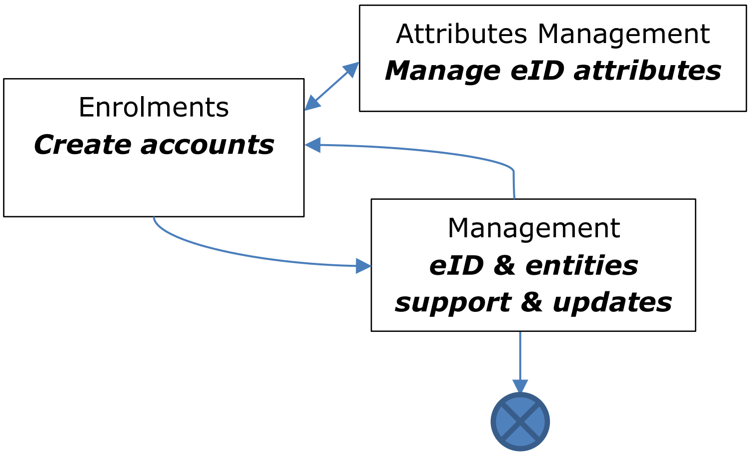

Figure 3-1 Scheme Manager workflow

3.1 Service Provider Enrolment Procedure

The enrolment procedure of a Service Provider to the certME ecosystem has a few steps:

1. The identification of the Service Provider according to the documents provided
2. The generation of the certME account of the Service Provider=
3. The authorization of the SP to perform identity claim validation requests
4. The installation of the certME API connector on the Service Provider app.

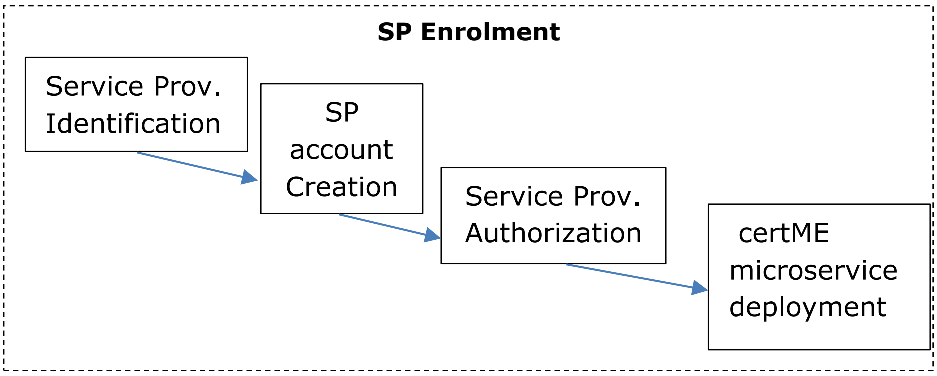
SP Enrolment
Service Prov. Identification
SP account Creation
Service Prov. Authorization
certME microservice deployment

Figure 3-2 Service Provider Enrolment workflow

3.1.1 Enrolment Process and Responsibilities

The responsibility of the Scheme Manager entity is to collect the required documents and approvals for the subsequent validation of the SP's identity and attributes.

The Scheme Manager operator performs a first verification of the documents and verifies that the collected information is complete and correct.

After the complete verification of the SP data, the Scheme Manager also informs the Service Provider representative about their rights and obligations.

The Scheme Manager verifies and completes the enrolment data. The SP is responsible for the accuracy of the data that will be incorporated in the certME account. The Scheme Manager is responsible for the correct registration/enrolment of the SP and for supplying the Blockchain with the correct content for the variable fields in the certME account.

The Scheme Manager officer is responsible for the verification of the following items:

- The claimed identity of the SP,
- The claimed attributes of the SP,
- The SP's entitlement to the requested account

The enrolment process is performed in compliance with the rules and methods described herein and in the internal guidelines and instructions of the Scheme Manager and the applicable law.

The Service Provider is provided with the following information and documents:

- The SP agreement
- The Terms and conditions
- The procedures, notifications or other documents provided by the SP

By signing the SP agreement the SP accepts and understand the following:

- Their responsibility that the information provided to the Scheme Manager is correct, complete, valid and up to date,
- That certME ecosystem maintains a retention period of minimum 10 years from the date of certME SP account creation for all the information related to the SP account.
- That in case the current Scheme Manager ceases its activities, this data may be transferred to a third party, with Scheme Manager role.
- Acknowledges the rights, obligations and responsibilities of certME and of partners, as defined in the SP Agreement and by national laws,
- That the SP has the obligation to inform certME on any change or event that may affect the validity or the content of the certME SP account

The enrolment process continues with the data generation for the certME SP account creation and Service Provider authorization, and ends at the Scheme Manager with the certME API connector and notifications installation.

3.1.2 Service Provider Identification & Documents Verification

The Service Provider enrolment process is done by enrolling the company through its legal representative identification and documents verification both for the person and the company.

Identification documents required to verify the identity of individuals must be valid and meet the minimum-security standards. These are included in the certME Acceptable Identity Documents.

The verification of natural persons' identity is required when the natural person represents a legal entity that enters into a contractual agreement with certSIGN.

All the documents necessary to identify the natural persons will be presented to the representatives of Scheme Manager in original and in a legal copy. The documents necessary to identify the legal person will be provided in a legal form in original or certified copies. Also it is required to have the proof of acceptance of the SP Agreement for the provision of identification services according to this document.

3.1.3 Service Provider Account Creation

Specially designated operators of certSIGN having specific roles (System administrator along with 2 Key Admins), generate within a HSM a non-exportable secp256k1 elliptic curve private key (used by the Ethereum blockchain) for the Service Provider's account. The Service Provider is issued a X509 certificate which it will use to authenticate to the HSM (via a CryptoServer API) in order to sign blockchain transactions with the private key.

3.1.4 Service Provider authorization

The private key (present within the HSM) issued in relation to the Service Provider's account, has a corresponding public key which is used in conjunction with the keccak256 algorithm to obtain the blockchain address of the Service Provider. The Scheme Manager representatives (DApp Manager role) issue a blockchain transaction containing the Service Provider's blockchain address to add the role of Service Provider into the smart-contract responsible with the Service Provider registry.

3.1.5 SP installation of the certME API Connector Installation

certSIGN provides the software component to the Service Provider to install it on their system.

The Service Provider should interconnect his existing apps with the API connector using RESTfull interfaces. The API connector uses the X509 digital certificate issued to the legal representative of the Service Provider in order to authenticate to certME CryptoServer and sign blockchain transactions with his private key stored in HSM.

3.2 Validator Enrolment Procedure

The enrolment procedure of a Validator to the certME ecosystem has the following steps:

1. The identification of the Validator legal entity according to the documents provided
2. The generation of the Validator's certME account and private key
3. Authorization of the Validator to perform user identity proofing, verification & registrations and to respond to identity claim validation requests
4. The deployment of the certME microservice on the Validator system/infrastructure.

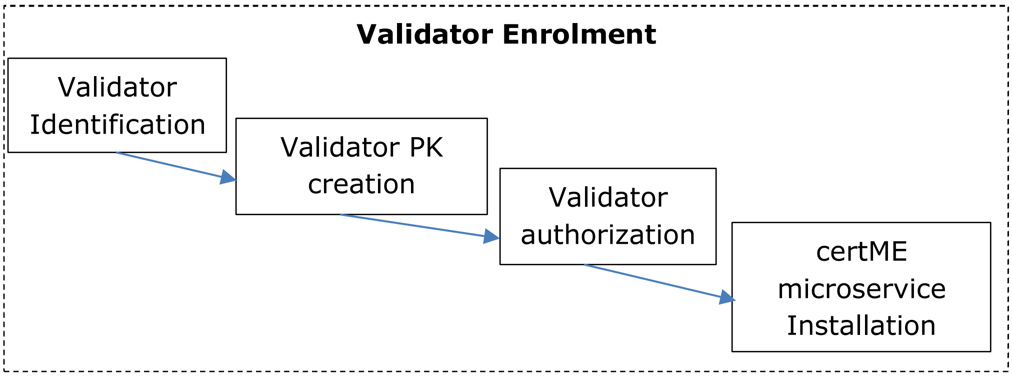

Figure 3-3 Validator Enrolment workflow

3.2.1 Enrolment Process and Responsibilities

The responsibility of the Scheme Manager entity is to collect the required documents and approvals for the subsequent validation of the Validator's identity and attributes.

An officer of the Scheme Manager performs a first verification of the documents and verifies that the collected information is complete and correct.

After the complete verification of the Validator data, the Scheme Manager also informs the Validator about their rights and obligations.

The Scheme Manager verifies and completes the enrolment data. The Validator is responsible for the accuracy of the data that will be incorporated in the certME account . The Scheme Manager is responsible for the correct registration/enrolment of the Validator and for supplying the Blockchain with the correct content for the variable fields in the certME account. The Scheme Manager officer is responsible for the verification of the following items:

- The claimed identity of the Validator,
- The claimed attributes of the Validator,
- The Validator's entitlement to the requested identity

The enrolment process is performed in compliance with the rules and methods described herein and in the internal guidelines and procedures of the Scheme Manager and the applicable law.

The Validator is provided with the following information and documents:

- The Validator agreement
- The Terms and conditions
- Online address for the procedures, notifications or other documents provided by the Validator

By signing the Validator agreement, the Validator accepts and understand the following:

- His responsibility that the information provided to the Scheme Manager is correct, complete, valid and up to date,
- That certME ecosystem maintains a retention period of minimum 10 years from the date of certME account creation for all the information related to the validator account.
- That in case the current Scheme Manager ceases its activities, this data may be transferred to a third party, which will undertake the Scheme Manager role.
- That in case the Validator ceases its activities, all data relating to eIDs for which the Validator has performed the verification and registration must be transferred to the Scheme manager, which will undertake the Validator role for said eIDs.
- Acknowledges the rights, obligations and responsibilities of certME and of partners, as defined in the Validator Agreement and by national laws,
- That the Validator has the obligation to inform certME on any change or event that may affect the validity or the content of the certME validator account

The enrolment process continues with the data generation for the certME account creation and Validator authorization, and ends at the Scheme Manager with the certME microservice and notifications installation.

3.2.2 Validator Identification & Documents Verification

The Validator enrolment process is done by enrolling the company through its legal representative identification and documents verification both for the person and the company.

Identification documents required to verify the identity of individuals must be valid and meet the minimum-security standards. These are included in the certME Acceptable Identity Documents. The verification of natural persons' identity is required when the natural person represents a legal entity that enters into a contractual agreement with certSIGN.

All the documents necessary to identify the natural persons will be presented to the representatives of the Scheme Manager in original and in a legal copy. The documents necessary to identify the legal person will be provided in a legal form in original or certified copies. Also it is required to have the proof of acceptance of the Validator Agreement for the provision of identification services according to this document.

3.2.3 Validator account creation

Specially designated operators of certSIGN having specific roles (System administrator along with 2 Key Admins), generate within a HSM a non-exportable secp256k1 elliptic curve private key (used by the Ethereum blockchain) for the Validator's account. The Validator is issued a X509 certificate which it will use to authenticate to the HSM (via a CryptoServer API) in order to sign blockchain transactions with the private key.

3.2.4 Validator authorization

The private key (present within the HSM) issued in relation to the Validator's account, has a corresponding public key which is used in conjunction with the keccak256 algorithm to obtain the blockchain address of the Validator. The Scheme Manager representatives (DApp Manager role) issue a blockchain transaction containing the Validators blockchain address to add the role of Validator into the smart-contract responsible with the Validator registry.

3.2.5 Validator installation of the certME microservice

certSIGN provides a software component to the Validator to install it on their system.

The microservice uses the X509 digital certificate issued to the legal representative of the Validator in order to authenticate to certME CryptoServer and sign blockchain transactions with his private key stored in HSM.

3.3 Management Procedures on Service Providers

The management procedures set contains a few procedures for different situations:

- Support on Service Provider requests
- Suspend a Service Provider's certME account
- Reactivate a Service Provider's certME account
- Delete a Service Provider's certME account

3.3.1 Support on Service Provider requests

The procedure to give support to a Service Provider on request is the following:

1. The responder from the certME Support email informs the Service Provider that we received his request and we will analyze and respond according to the SLA
2. If the request was on the phone the certME support team member should inform the Service Provider that the team will analyze and respond to his request within the SLA time.
3. Analyze the request and classify the emergency and priority according to the internal instructions.
4. Open a certME Support ticket with the request info and assign it to the on duty support team
5. Respond to the Service Provider request with the solution proposed, within the default SLA time according to the emergency & priority of the request.
6. Get the confirmation from the Service Provider if the solution was responding to the request, in order to close it
7. Close the request ticket with the details of the solution process and results.

3.3.2 Suspend a Service Provider's certME account

On a request to suspend an existing certME account the steps are the following:

1. Record the request in a Support ticket with all the initial details
2. Check the requester if it is in the list of valid requestors for this operation
3. Check the details of the suspension request, if the arguments are valid

4. In case any validation of the request parameters is not clear escalate the issue
5. Suspend the certME account for the Service Provider according to the internal instructions, within the SLA
6. Check the success of the suspension task
7. Report the suspension to the requester
8. Fill the suspension ticket with the details and close it

3.3.3 Reactivate a Service Provider's certME account

On a request to reactivate a suspended certME account the steps are the following:

1. Record the request in a Support ticket with all the initial details
2. Check the requester if it is in the list of valid requestors for this operation
3. Check the details of the reactivation request, if the arguments are valid
4. In case any validation of the request parameters is not clear escalate the issue
5. Reactivate the certME account for the Service Provider according to to the internal instructions, within the SLA
6. Check the success of the reactivation task
7. Report the reactivation to the requester
8. Fill the reactivation ticket with the details and close it

3.3.4 Delete a Service Provider's certME account

On a request to delete an existing certME account the steps are the following:

1. Record the request in a Support ticket with all the initial details
2. Check the requester if it is in the list of valid requestors for this operation
3. Check the details of the delete request, if the arguments are valid
4. In case any validation of the request parameters is not clear escalate the issue
5. Delete the certME account for the Service Provider according to to the internal instructions, within the SLA
6. Check the success of the delete task
7. Report the deletion to the requester
8. Fill the delete ticket with the details and close it

3.4 Management Procedures on Validators

The management procedures set contains a few procedures for different situations:

- Support on Validator requests
- Suspend a Validator's certME account
- Reactivate a Validator's certME account

3.4.1 Delete a Validator's certME account Support on Validator requests

The procedure to give support to a Validator on request is the following:

1. The automatic responder from the certME Support email inform the Validator that we received his request and we will analyze and respond according to the SLA
2. If the request was on the phone the certME support team member should inform the Validator that the team will analyze and respond to his request within the SLA time.
3. Analyze the request and classify the emergency and priority according to the internal instructions.

4. Open a certME Support ticket with the request info and assign it to the on-duty support team
5. Respond to the Validator request with the solution proposed, within the default SLA time according to the emergency & priority of the request.
6. Get the confirmation from the Validator if the solution was responding to the request, in order to close it
7. Close the request ticket with the details of the solution process and results.

3.4.2 Suspend a Validator's certME account

On a request to suspend an existing certME account the steps are the following:

1. Record the request in a Support ticket with all the initial details
2. Check the requester if it is in the list of valid requestors for this operation
3. Check the details of the suspension request, if the arguments are valid
4. In case any validation of the request parameters is not clear escalate the issue
5. Suspend the certME account for the Validator according to the internal instructions, within the SLA
6. Check the success of the suspension task
7. Report the suspension to the requester
8. Fill the suspension ticket with the details and close it

3.4.3 Reactivate a Validator's certME account

On a request to reactivate a suspended certME account the steps are the following:

1. Record the request in a Support ticket with all the initial details
2. Check the requester if it is in the list of valid requestors for this operation
3. Check the details of the reactivation request, if the arguments are valid
4. In case any validation of the request parameters is not clear escalate the issue
5. Reactivate the certME account for the Validator according to to the internal instructions, within the SLA
6. Check the success of the reactivation task
7. Report the reactivation to the requester
8. Fill the reactivation ticket with the details and close it

3.4.4 Delete a Validator's certME account

On a request to delete an existing certME account the steps are the following:

1. Record the request in a Support ticket with all the initial details
2. Check the requester if it is in the list of valid requestors for this operation
3. Check the details of the delete request, if the arguments are valid
4. In case any validation of the request parameters is not clear escalate the issue
5. Transfer all eID registration, suspension, reactivation, revocation physical reports and eID validation codes to the certME Validator entity.
6. Delete the certME account for the Validator according to the internal instructions, within the SLA
7. Check the success of the delete task
8. Report the deletion to the requester
9. Fill the delete ticket with the details and close it

3.5 Management Procedures on Users

The management procedures set contains a few procedures for different situations:

- Support on User certME eID
- Suspend a User's certME eID
- Reactivate a User's certME eID
- Revoke a User's certME eID

3.5.1 Support on User requests

The procedure to give support to a User on request is the following:

1. The automatic responder from the certME Support email inform the User that we received his request and we will analyze and respond according to the T&C
2. If the request was on the phone the certME support team member should inform the User that the team will analyze and respond to his request according to the T&C.
3. Analyze the request and classify the emergency and priority according to the internal instructions.
4. Open a certME Support ticket with the request info and assign it to the on-duty support team
5. Respond to the User request with the solution proposed, within the default response time according to the emergency & priority of the request.
6. Get the confirmation from the User if the solution was responding to the request, in order to close it
7. Close the request ticket with the details of the solution process and results.

3.5.2 Suspend a User's certME eID

On a request to suspend an existing certME eID the steps are the following:

1. Identify the blockchain address of the certME eID based on the eIDAS MDS attributes provided by the requester
2. Record the request in a Support ticket with all the initial details (action required, blockchain address of eID)
3. Check the requester if it is in the list of valid requestors for this operation
4. Record eIDAS MDS attributes in the suspension report along with requester attributes (if different from user), ticket number and timestamp.
5. In case any validation of the request parameters is not clear escalate the issue
6. Suspend the certME eID for the User according to the internal instructions
7. Check the success of the suspension task
8. Report the suspension to the requester
9. Fill the suspension ticket with the details and close it

3.5.3 Reactivate a User's certME eID

On a request to reactivate an existing certME eID the steps are the following:

1. Identify the blockchain address of the certME eID based on eIDAS MDS attributes of the user
2. Record the request in a Support ticket with all the initial details (action required, blockchain address of eID)
3. Check the requester if it is in the list of valid requestors for this operation
4. Record eIDAS MDS attributes in the reactivation report along with requester attributes (if different from user), ticket number and timestamp.

5. In case any validation of the request parameters is not clear escalate the issue
6. Reactivate the certME eID for the User according to the internal instructions.
7. Check the success of the reactivation task
8. Report the reactivation to the requester
9. Fill the ticket with the details and close it

3.5.4 Revoke a User's certME eID

On a request to revoke an existing certME eID the steps are the following:

1. Identify the blockchain address of the certME eID based on eIDAS MDS attributes of the user
2. Record the request in a Support ticket with all the initial details (action required, blockchain address of eID)
3. Check the requester if it is in the list of valid requestors for this operation
4. Record eIDAS MDS attributes in the revocation report along with requester attributes (if different from user), ticket number and timestamp.
5. In case any validation of the request parameters is not clear escalate the issue
6. Revoke the certME eID for the User according to the internal instructions
7. Check the success of the revocation task
8. Report the revocation to the requester
9. Fill the revocation ticket with the details and close it

3.6 Attributes Management

On a request to add/activate/inactivate attributes supported by the platform, the steps are the following:

1. Record the request in a Support ticket with all the initial details
2. Check the requester if it is in the list of valid requestors for this operation
3. Check the details of the request, if the arguments are valid
4. In case any validation of the request parameters is not clear escalate the issue
5. Add/ activate/inactivate the attributes according to the internal instructions
6. Check the success of the task
7. Report the result to the requester
8. Fill the ticket with the details and close it

3.6.1 Add new certME eID attributes

To add a new possible attribute to the certME eID platform the steps are:

1. Authenticate with the certME DApp manager private key on the Scheme Manager website app
2. Select the add attributes from the app menu
3. Add each attribute name and value
4. Confirm to the updates and Save
5. Inform the Validators on the updates

3.6.2 Activate a certME eID attribute

To activate an existing attribute of the certME eID platform the steps are:

1. Authenticate with the certME DApp manager private key on the Scheme Manager website app
2. Select the attribute from the app menu
3. Activate the attribute
4. Confirm the update and Save
5. Inform the Validators on the update

3.6.3 Inactivate a certME eID attribute

To inactivate an existing attribute within the certME eID platform the steps are:

1. Authenticate with the certME DApp manager private key on the Scheme Manager website app
2. Select the attribute from the app menu
3. Inactivate the attribute
4. Confirm the update and Save
5. Inform the Validators on the update