Validator 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	First draft version publishing	Policies Manager
0.2	July 2020	Updates on the procedures	Policies Manager
0.3	Feb.2021	Layout updates & corrections	Policies Manager
0.4	Feb. 2021	Corrections	Product Owner
1.0	Feb. 2021	Corrections	Product Owner

This document was created and is the property of:

Owner	Author	Date created
certME	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 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 client corresponds to the proofs indicated by the validator, thus by completing the validation process.

This document presents the procedure that a certME Validator uses in order to operate within the certME ecosystem.

1.2 Document name and identification

This document represents the certME Validator Procedures.

The document is available in electronic format within the certME Repository at address https://www.certme.ro/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).

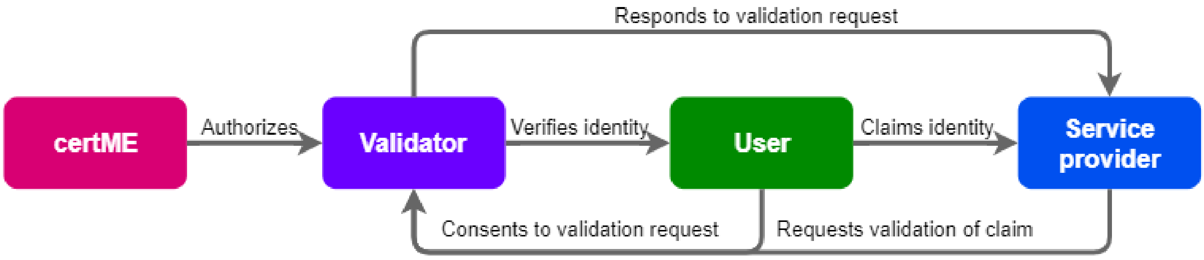

Responds to validation request
certME
Authorizes
Validator
Verifies identity
User
Claims identity
Service provider
Consents to validation request
Requests validation of claim

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 user's 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 Validator Procedures Workflow

The generic workflow for a Validator within the certME ecosystem has the following main steps:

- Validator Enrolment – add the validator into the platform
- User Verification & Enrolment – identity proofing, verification and registration
- User Authorization response to Service Providers
- Management - Support / Updates / End of usage

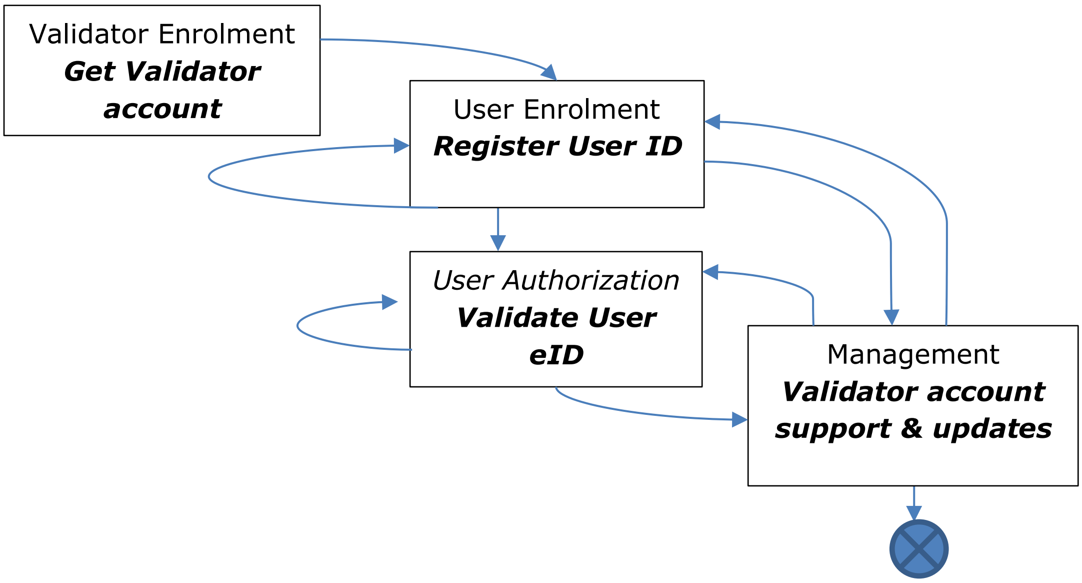


Figure 3-1 Validator workflow

3.1 Validator Enrolment Procedure

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

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

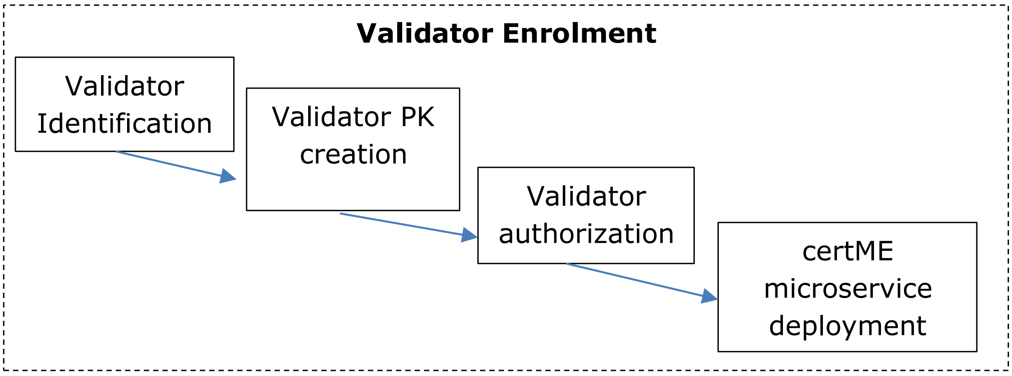


Figure 3-2 Validator Enrolment workflow

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 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 their 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 validator 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.

3.1.2 Validator Identification & Documents Verification

The Validator enrolment process is done by enrolling the company and verifying the documents provided by its legal representative.

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.

3.1.3 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.

3.1.4 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.

3.1.5 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.

3.2 User Verification & Enrolment Procedure

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

1. The face-to-face identification of the user according to the identity documents provided
2. The installation of the certME app on the user mobile device.
3. Acceptance by the user of the certME Privacy Policy and Terms and Conditions
4. The generation of the public/private keys of the user
5. Attributes receipt, confirmation & storage in the certME mobile app
6. User registration & request to issue a certME eID

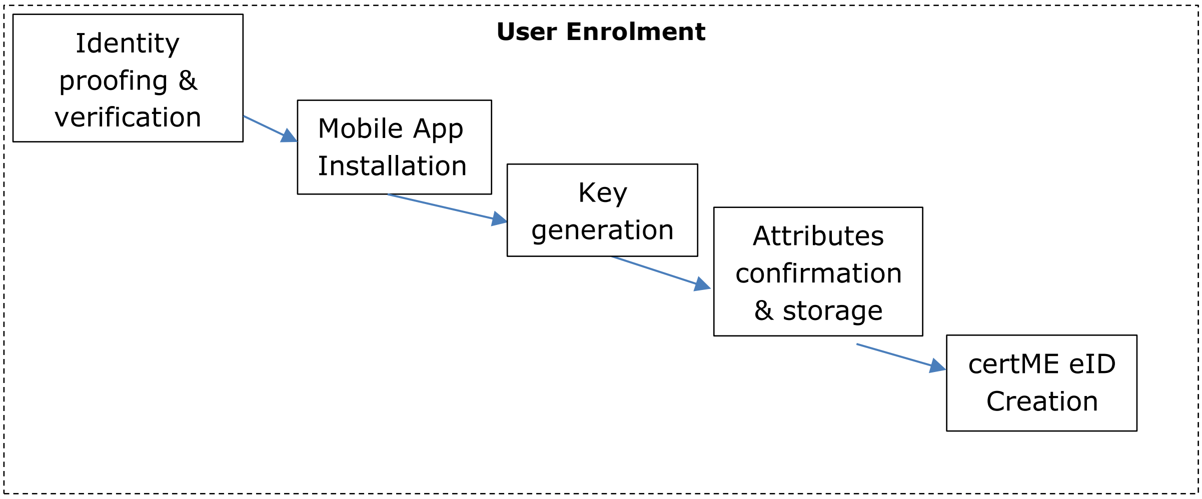


Figure 3-3 User Enrolment workflow

3.2.1 Enrolment Process and Responsibilities

The enrolment process begins with the mobile app installation.
The responsibility of the Validator entity is to collect the required documents and approvals for the subsequent validation of the User's identity and attributes.

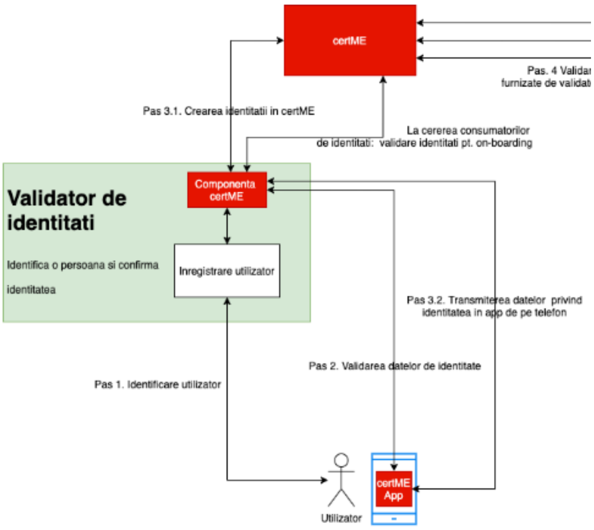

certME
Pas. 4 Validar
furnizate de validat
Pas 3.1. Crearea identitatii in certME
La cererea consumatorilor
de identitati: validare identitati pt. on-boarding
Validator de identitati
Identifica o persoana si confirma identitatea
Componenta certME
Inregistrare utilizator
Pas 3.2. Transmiterea datelor privind identitatea in app de pe telefon
Pas 2. Validarea datelor de identitate
Pas 1. Identificare utilizator
Utilizator
certME App

Figure 3-4 User enrolment

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

After the complete verification of the user's data, the Validator also informs the User about his/her rights and obligations.

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

The Validator operator is responsible for the verification of the following items:

- The claimed identity of the User,
- The claimed attributes of the User,
- The User'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 Validator and the applicable law.

The User is provided with the following information and documents:

- The certME Terms and Conditions which include the Recommended Security Precautions
- The Privacy Policy describing data collection and processing
- The online address for certME eID Terms and Conditions on the certME eID use

By signing the Terms and conditions the User accepts and understand the following:

- His responsibility that the information provided to the Validator is correct, complete, valid and up to date,
- That certME ecosystem maintains a retention period of minimum 10 years from the date of certME eID issuance for all the information related to the registration and enrolment, to the certME eID request and to the certME eID revocation
- That in case the current Validator ceases its activities, this data may be transferred to a third party, with Validator role.

- Acknowledges the rights, obligations and responsibilities of certME and of other Validators, as defined in the User Agreement and by national laws,
- That the User has the obligation to inform certME on any change or event that may affect the validity or the content of the certME eID

3.2.2 certME Mobile App Installation

The certME mobile app is a software application compatible with the Android operating system. The app is available for download on Google Play and can run on smartphones and tablets without restrictions.

The app is installed and operated by the persons being issued the identification means on a mobile device under their control. The usage of the certME mobile app is protected by strong biometric authentication (based on Secure Enclave/Element) enforced by the mobile app.

3.2.3 Key generation

The certME mobile app allows the user to create a public/private keypair. The public key is used to obtain the public blockchain address which serves as an identifier for the certME eID.

The hardware key-store is used to store the private key. The certME mobile app doesn’t work on mobile devices which don’t support hardware key stores.

3.2.4 Identity proofing, verification and registration

The certME user enrolment process is done by face-to-face verification. certME mobile app uses a QR-code based system to securely authenticate and exchange data with the certME validator app.

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

The verification of natural persons’ identity is required when the natural person is the Subject of an electronic means of identification issued by certME at the request of a Validator.

All the documents necessary to identify the natural persons will be presented to the representatives of the Validator in original. Also, the user is required to accept the Terms and conditions for the provision of identification services and this document.

certME or any Validator reserves the right not to perform identity proofing, verification and registration in case there are reasonable indications regarding the validity or accuracy of the documents presented by the Subject (damaged identity card or passport or which does not meet the minimum-security requirements).

To ensure a substantial level of assurance for digital identities delivered under certME service, all user enrolments are done in person and face to face. The validator web app is designed to enforce verification of users by a two-way handshake using QR codes. The user uses his certME mobile app to scan a QR code generated by the certME validator web app. By reading the QR code all attributes’ values introduced by the Validator’s operator from the web app are transferred to the user’s mobile app and displayed for user verification.

3.2.5 Attributes' confirmation & storage

After verifying that the attributes displayed are correct the user confirms the attributes by pressing a button that will generate a QR code containing his confirmation and signature.

If the user does not confirm the attributes, then the identity proofing, verification and registration process is repeated.

The certME validator web app scans the QR code generated by the user's certME mobile app in response to the initial QR.

The app allows the user to store up to 255 attributes. All attributes are stored encrypted within the mobile app.

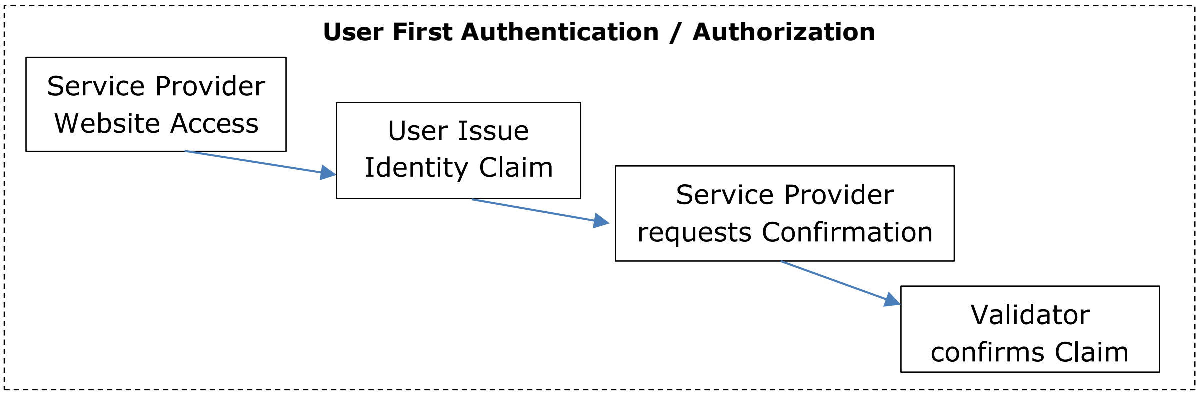
3.2.6 certME eID Creation

Upon completing an identity proofing, verification and registration process, a certME validator signs and issue a transaction to the blockchain, containing the above-mentioned blockchain address of the user and a list of encrypted proofs of identity verification.

certME eID is created when the smart contract confirms the transaction and records the address in the eID registry.

3.3 Validator identity claim confirmation procedure

The authentication of the User with his certME eID is the main process of using certME eID. When the User access a Service Provider Website or app for the first time, he provides his certME eID, the necessary data attributes and his consent. The Service Provider use the blockchain Smart Contract to ask for User attributes validity and the Validator, through the Smart Contract, confirms the validity of the identity claim made by the User.



User First Authentication / Authorization

Service Provider Website Access

User Issue Identity Claim

Service Provider requests Confirmation

Validator confirms Claim

Figure 3-5 User First Authentication Workflow

Subsequent authentications of the User to the Service Provider Web page or app rely on a unique token signed by the User with his certME eID, and do not require the Validator's participation.

3.3.1 Authentication Request

Service providers using the certME identity scheme run a micro service, henceforth called the certME authenticator app.
To receive a certME eID and related data attributes from users, the certME authenticator app is accessible to the certME mobile app users via REST API. To authenticate to the service provider, a user sends his/her person identification data to the certME authenticator app REST API using his mobile app. Communications are protected by two layers of authentication and encryption (TLS and ECIES). The user's mobile app receives the URL to the REST API and a session ID either via QR code from the service provider's website or via arguments from the service provider's mobile app.
The user can authenticate to a service provider using his certME mobile app either by showing a QR code on the screen that the service provider can scan or by securely sending his data via REST API over TLS.
All transactions whereby the user's data is sent and received, can only be done by the user using the data stored on his certME mobile app. Transactions cannot work if they are not signed by the user with his private-key.

3.3.2 User identity claim confirmation

Any validation of the level of assurance of user data requested by a service provider to a validator must also be consented to and signed by the user with his private-key via the certME mobile app. The smart contract that brokers the identity validation between user, service provider and validator does not allow validators to submit proofs of data authenticity and level of assurance, if the user signature and consent is missing.

The certME authenticator app facilitates communications with the blockchain for the service provider. The certME authenticator app is integrated with the service provider's software infrastructure via a REST API. Upon receiving data from a certME mobile app, the microservice generates an identity claim validation request and submits it to a smart-contract on the blockchain. The certME authenticator app constantly monitors the smart-contract for responses to identity claim validation requests. Proofs are extracted from the responses provided by validator apps and used to determine the authenticity and level of assurance of the identity data received from certME mobile app.

3.3.3 Validator Confirmation

The authentication is complete when the service provider receives proof from a validator that confirms the authenticity and level of assurance of data provided by the user.

The certME validator app micro service constantly monitors the blockchain for identity claim validation requests submitted by service providers. If a request is related to a user enrolled by the micro-service owner, the micro-service automatically responds to the request by submitting to the blockchain the necessary proofs that the service provider can use to determine the authenticity and level of assurance of data received from a certME mobile app user.

3.4 Validator Management Procedures on Users

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

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

3.4.1 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.

3.4.2 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

3.4.3 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

3.4.4 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