# Service Provider Procedures

Document code: [Subject]

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

Document Security Level: **Public**

---

**Important Notice**



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 to procedures | 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 | 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 user corresponds to the proofs indicated by the validator, thus by completing the validation process.

This document present the procedure that a certME Service Provider uses in order to operate within the certME ecosystem.

## 1.2 Document name and identification

This document represents the certME Service Provider 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), S**ervice Provider** (data consumer) and **Validator** (authorized identity verifier and data validator).

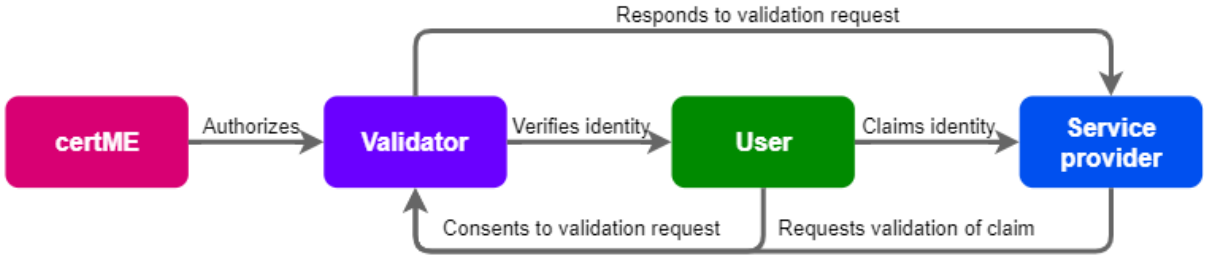


**Figure 2-1 certME ecosystem participants**

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 and interact 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 Service Provider Procedures

The generic workflow for a Service Provider within the certME ecosystem has the following main modules:

- Service Provider Enrollment on certME system
- Authentications Usage for the customers using certME eID
- Management - Support / Updates / End of usage

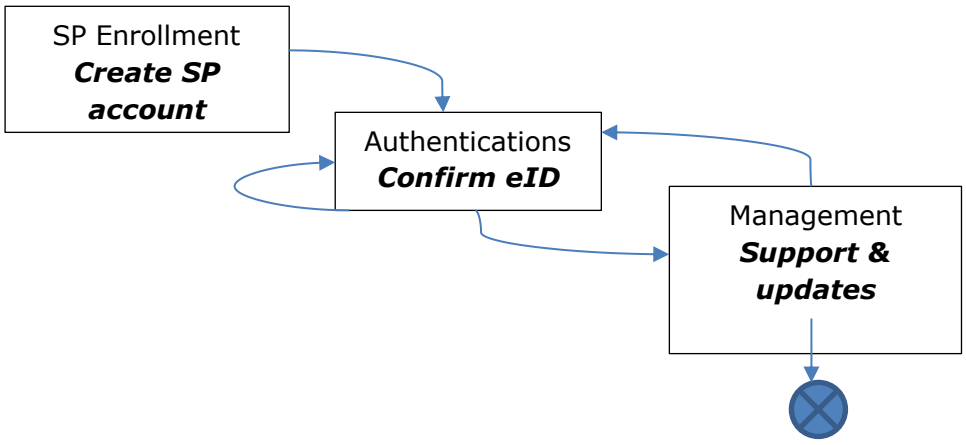


**Figure 3-1 Service Provider workflow**

## 3.1 Service Provider Enrollment 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.

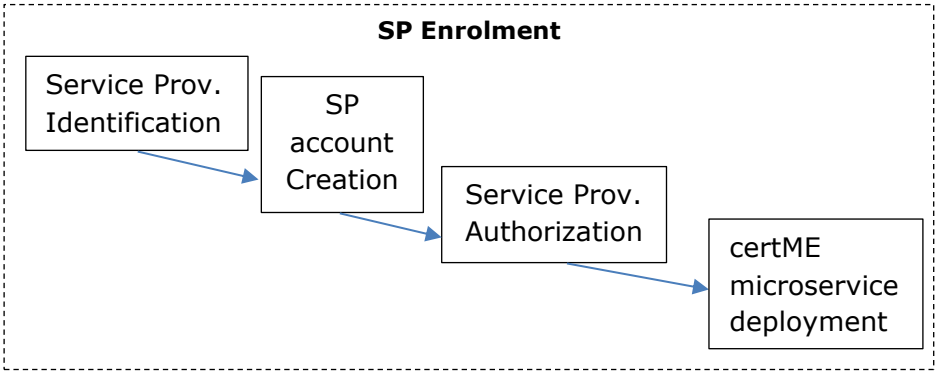


**Figure 3-2 Service Provider Enrolment workflow**

### 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
- Online address for the procedures, notifications or other documents provided by the SM

- 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 Service Provider Authentication Procedure

The authentication of the User with their certME eID is the main process of using certME eID.

When the User accesses a Service Provider's 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.

### First authentication

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.

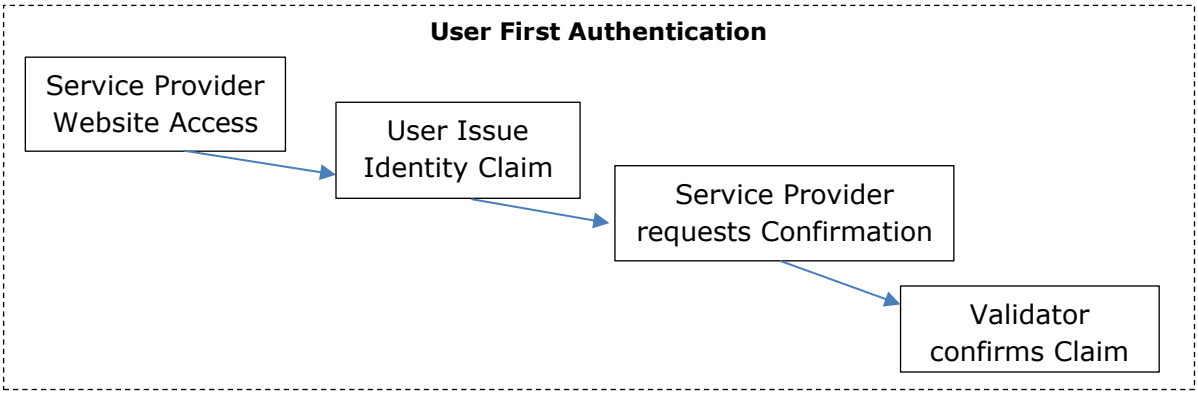


Figure 3-4 First Authentication Workflow

### Subsequent authentications

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

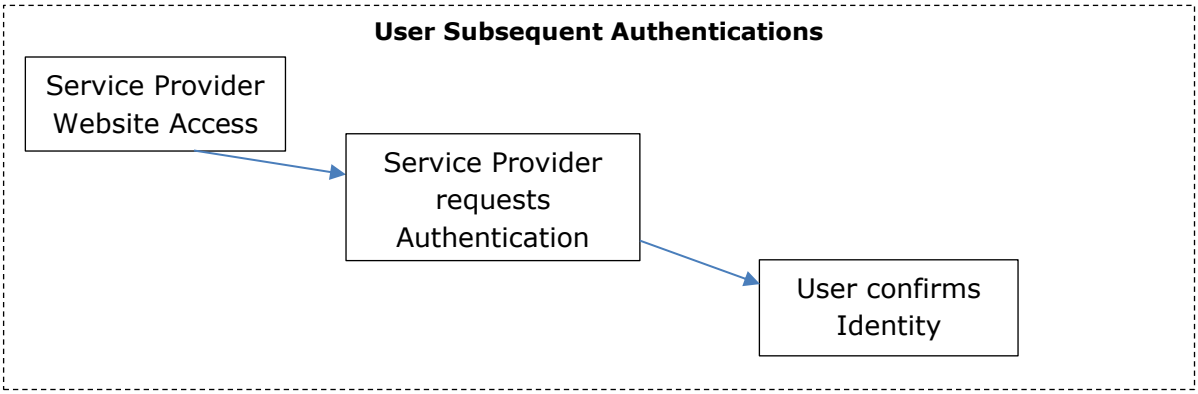


Figure 3-5 Subsequent Authentications Workflow

### 3.2.1 User 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.

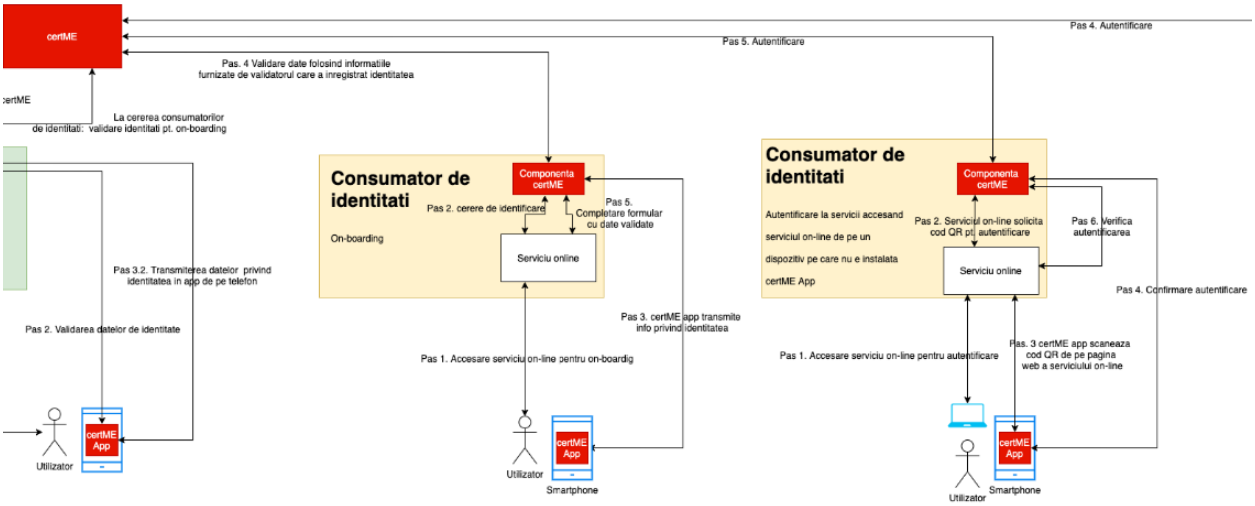


**Figure 3-6 User Authentication**

### 3.2.2 User Attributes Confirmation

Any validation of the level of assurance of user data requested by a service provider to a consortium member 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 consortium members 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.

### 3.2.3 Validator Confirmation

The authentication is complete when the service provider receives proof from a consortium member 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.

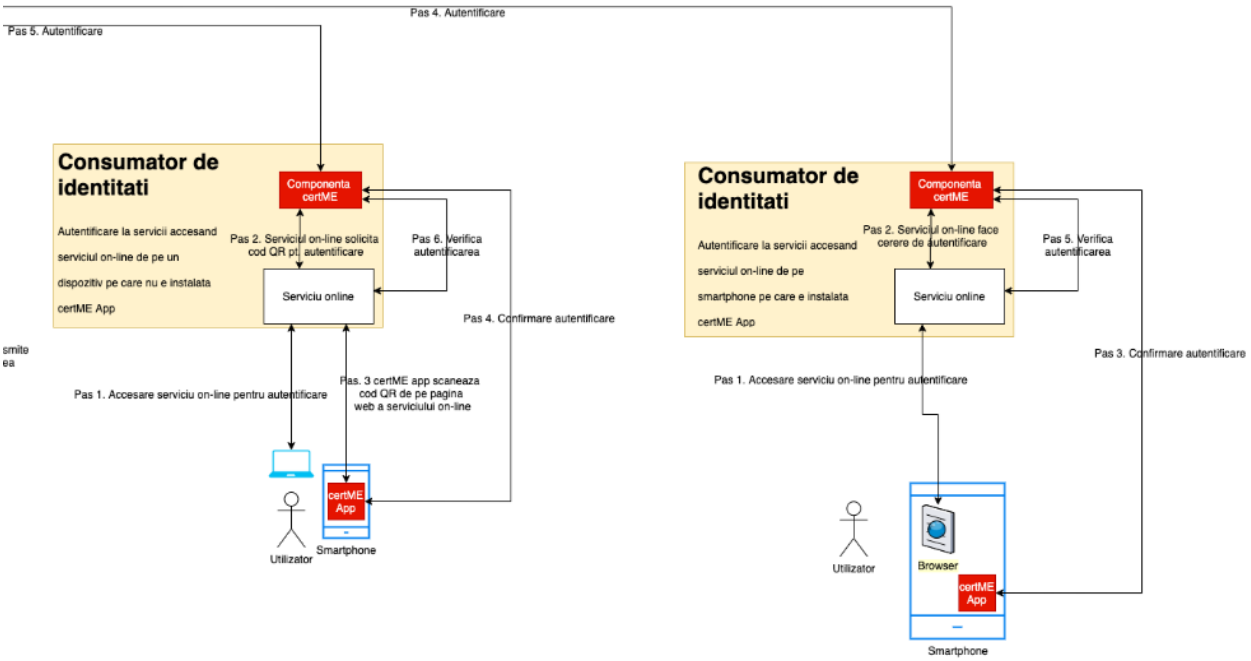


**Figure 3-7 Authentication on laptop/smartphone**

## 3.3 Management Procedures

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

- Support on requests sent to the Scheme Manager
- Support on Customer requests sent to the Service Provider

### 3.3.1 Support on requests sent to the Scheme Manager

The Scheme Manager will inform immediately the Service Provider on the resolution for the requests that are related to the suspension, reactivation or deletion of the SP certME account.

The Service Provider may respond with arguments to the claim and may ask for a clarification on the resolution.

### 3.3.2 Support on Customer requests sent to the Service Provider

If the request content is related to the certME eID, the Service Provider may forward the request to the Scheme Manager.