Digidentity

CAB Manual

SERMI

Title	CAB Manual – SERMI
Date	2 June 2026
Author	Client Service Manager
Version	2026-v1

Revisions

Version	Date	Author	Changes Made (*)
2023-v1	7 Aug 2023	Client Service Manager	Initial version
2023-v1.1	12 Sep 2023	Client Service Manager	Added a support email template (see chapter 3.7). Adjusted UID requirements for support requests (see chapter 3.6).
2023-v1.2	3 Nov 2023	Client Service Manager	Corrected typo: QR-code validity changed from 14 to 28 days (see chapter 4.1). Added 'Lemon Turtle' error code (see chapter 4.2).
2023-v1.3	9 Nov 2023	Client Service Manager	Added IO_UID and RSS_UID to support template (see chapter 3.7).
2023-v1.4	8 Dec 2023	Client Service Manager	Added information in chapter 4.3 — General Information & Tips.
2024-v1	1 May 2024	Client Service Manager	Added error code 'Yellow Pigeon' (see chapter 4.2). Changed text font from 'Buenos Aires' to 'Seaford'. Added bullet list to support email template.
2024-v2	20 Nov 2024	Client Service Manager	Added information in chapter 4.3 — General Information & Tips.
2025-v1	13 Jan 2025	Client Service Manager	Added IO: Public Authority to details of UAT in chapter 2.3.5.
2026-v1	12 May 2026	Client Service Manager	Editorial pass: typos and grammar fixes throughout. Corrected Table of Contents page references (chapters 2.3.7 onward). API documentation URL standardised to connect.digidentity.eu. App Error Codes table: White Whale and Yellow Pigeon split into separate rows. Certificate Reset note clarified: '28-day' QR code validity period.

(*) All changes are marked in grey highlight.

Digidentity

Contents

1 Introduction

Welcome to the Conformity Assessment Body (CAB) Manual for the SERMI Scheme. This comprehensive manual has been created to provide CABs with all the necessary information and procedures required to ensure smooth and efficient operation with Digidentity within the SERMI scheme.

Contents include, but are not limited to, various (technical) aspects of the SERMI scheme, such as the support procedure, registration processes, harnessing APIs, and common troubleshooting techniques.

This document is a living document that will be continually edited and updated. Please see the revisions section for version history and changes.

2 Onboarding

As the official Trust Center (TC) for SERMI, Digidentity is responsible for providing Conformity Assessment Bodies with the necessary tools to fulfil their duties and responsibilities within the SERMI Scheme. This includes providing and managing the digital certificates and authorisation status of the IO employees, and providing to the CAB the necessary tools/software to invite the authorised IOs/RSSs and IO/RSS employees to create mobile security tokens attached to digital certificates.

2.1 APIs

Digidentity offers APIs (Application Programming Interfaces) that allow for seamless integration with existing CAB systems and processes. These APIs provide all the necessary (technical) functionality to CABs as required under SERMI.

2.2 Documentation

For more information on the API connection process and documentation, please visit:

URL
https://connect.digidentity.eu/SERMI/CabApi/

2.3 Procedure

2.3.1 Accreditation and Approval

A Conformity Assessment Body (CAB) must apply for accreditation with their National Accreditation Body (NAB) and for approval by the SERMI Association.

2.3.2 Contact with Customer Success

After applying for accreditation and approval, a CAB can schedule a meeting with Digidentity Customer Success. This meeting serves as the first point of contact where customer success representatives provide onboarding information and outline the necessary procedures to go live.

Contact Details

Availability	Email
Monday to Friday 09:00 – 17:00 (CET)	Sermi@digidentity.com

2.3.3 Contracting

After initial contact with Customer Success, Digidentity will provide a non-disclosure agreement (NDA) and a commercial contract for signature. The NDA must be signed and delivered to Digidentity to proceed to the next stage of implementation.

2.3.4 API Integration

Once the contracting stage is completed, Digidentity's Implementation team will provide the following details:

- OAuth client credentials (client_id, client_secret, API key, and scope)
- A CABUID for the pre-production environment

These will be sent securely via email to the CAB's elected technical contact, along with the CAB API specification.

2.3.5 User Acceptance Testing

For API connections, a mandatory user acceptance test (UAT) is required before going live. This ensures that CABs can effectively perform their duties and responsibilities within the SERMI Scheme. UAT scenarios include:

Creation of entities

- Creating an IO
- Creating an IOE
- Creating an IO: Public Authority
- Creating an RSS
- Creating an RSSE

Authorisation Management

- Approving an IOE Authorisation
- Revoking an IOE Authorisation
- Approving an RSSE Authorisation
- Revoking an RSSE Authorisation

Support Management

- Reset Certificate

Once a CAB is ready, it can request a UAT by contacting Customer Success. Documentation for the UAT itself will then be supplied to the CAB. For each test scenario, Digidentity will verify that the desired result was obtained. If successful, both parties will provide their signature on the UAT document.

2.3.6 Support Training

After the UAT, Digidentity Customer Success will plan a support training with the CAB. This meeting will outline basic support procedures for Independent Operators, Remote Service Suppliers, and their respective employees. For the full support procedure, please see the chapter 'Support Procedure'.

2.3.7 Go Live

Once the UAT has been signed off by all parties, and the commercial contract has been signed, the CAB can proceed to production. This process is assisted by Digidentity Customer Success and constitutes the final step in the API onboarding process. Once live, the CAB will be able to perform all relevant duties and responsibilities within the SERMI Scheme.

3 Support Procedure

The following section explains the procedures and protocols for support provision between Digidentity and Conformity Assessment Bodies (CABs). The primary purpose of this section is to define a clear and efficient support process for SERMI CABs and to ensure smooth operations and effective communication between parties.

3.1 Roles & Responsibilities

CABs provide first line support to IOs, IO employees, RSSs and RSS Employees on all matters related to the registration process, invitations, authorisations, and daily usage of the SERMI certificate and the Digidentity app.

Digidentity provides second line support to CABs on all escalated matters related to the registration process, invitations, authorisations, and daily usage of the SERMI certificate and the Digidentity app by End Users.

3.2 Availability

Digidentity has a dedicated customer support team on standby to address any escalated issues, queries, or concerns from CABs.

Opening Times
Monday to Friday 09:00 – 17:00 (CET)

3.3 Contact Channels

CABs can reach out to Digidentity via the following channels:

For Support Queries — Email
sermi-support@digidentity.com

3.4 Support Process

3.4.1 First Line Support

Initial Contact: When encountering a technical issue, the End User should contact the relevant CAB for first-line support.

Issue Assessment and Attempted Resolution: The CAB will assess the reported issue and attempt to provide an appropriate solution. The CAB will be equipped to handle most common technical problems through APIs provided by Digidentity.

Documentation: A documentation website will be maintained by Digidentity with frequently asked questions and other relevant support information. This guide also contains a chapter on troubleshooting for commonly experienced issues.

3.4.2 Second Line Support

Issue Escalation: If the CAB is unable to resolve the issue, the user issue can be escalated to Digidentity by the CAB. This process is initiated by sending an email to sermi-support@digidentity.com.

Emails must contain:

- IO_UID/RSS_UID and IOE_UID/RSSE_UID
- Detailed issue description, including any error messages, screenshots, and steps taken before the problem arose.
- Any previous troubleshooting steps executed by the CAB.

Emails must not contain:

- Personal identifiable information (PII), such as personal email address or IO/RSS employee name.

Digidentity support will never ask for any personal information related to the SERMI certificate. Any PII sent by the CAB to Digidentity will be treated as a data breach. Information will be redacted, and the support request will be deleted by Digidentity.

Resolution by Digidentity: Upon receiving the escalated issue, Digidentity will undertake further analysis and action to resolve the issue together with the CAB.

3.5 Support Email Template

The following template must be used to contact the Digidentity customer support team.

Field	Content
UIDs	IO_UID/RSS_UID: [value] | IOE_UID/RSSE_UID: [value]
Device Make/Model	Please provide the device and model information (e.g., iPhone 13 Pro Max).
App Version	Please provide the current app version of the user. This is visible by the user under 'settings' in the app.
Issue Description	▪ Provide a detailed issue description. Include any error messages and steps taken by the user before the problem arose. Which action was the user trying to complete? ▪ Creating a SERMI certificate ▪ Logging into a VM portal ▪ Providing or accepting a chain authorisation ▪ Other, namely: ___
Troubleshooting	Enter any previous troubleshooting steps executed by the CAB (please mention each step).
Screenshots	If available, please include screenshots and screen recordings.

3.6 Security

All CABs are required to communicate an official support email address to Digidentity. This allows Digidentity to verify the legitimacy of an escalated support request by a CAB.

This email address must be:

- Generic (e.g., support@cabname.com).
- Accessible to all relevant CAB helpdesk employees.

CABs must communicate this email address to Digidentity during the production onboarding process. This is captured on the CAB onboarding form supplied by Digidentity.

Important (!) Digidentity will only process support requests from an officially communicated email address. All other support requests will not be processed.

3.7 Monitoring

Digidentity maintains a website page which displays the live status of our services. CABs can subscribe to receive updates about service disruptions and planned outages. Digidentity highly recommends all CABs subscribe to this website. This page is available at: https://ddy.statuspage.io

3.8 Incidents

In the event of a service disruption or any other issues, CABs should follow the steps below:

- **Investigate:** Check https://ddy.statuspage.io to confirm if there is an active service disruption or known issue.
- **Contact:** If no issue is reported on the status page, CABs should contact Digidentity support via email: sermi-support@digidentity.com.
- **Incident Details:** Provide a comprehensive report of the issue, including the time of occurrence, any error messages, and steps taken before the problem arose.
- **Follow-up:** A Digidentity support representative will acknowledge receipt of the issue, initiate the necessary steps to resolve the problem, and provide updates until the issue is resolved.

3.9 Escalation Procedures

Should an issue require higher-level attention, the following escalation procedures apply:

- **Escalation Level 1:** If the issue remains unresolved after initial contact with the support team, the support agent will escalate the issue to the Service Desk Team Lead.
- **Escalation Level 2:** If the issue persists or is of a critical nature, it will be escalated to the Customer Success Manager.
- **Escalation Level 3:** In rare circumstances, should the issue remain unresolved, it will be escalated to the Client Service Manager.

3.10 Support Feedback

To continuously improve our services, we welcome feedback from CABs on our support provision. CABs will periodically be contacted by Digidentity to discuss support (common/recurring issues, available information, etc). Planning of these sessions is determined by Digidentity.

3.11 Confidentiality

Digidentity maintains strict confidentiality and adherence to our Privacy Policy. This applies to all information shared by a CAB with Digidentity during the support process. Digidentity does not share support information with third parties.

4 Troubleshooting

This section presents a comprehensive troubleshooting guide, addressing common End User problems, their potential causes, and step-by-step solutions.

4.1 Common Issues

Issue	Description	Solution
Forgotten PIN Code	The IO/RSS employee has forgotten the PIN code for their SERMI certificate.	Use the 'Reset Certificate' API call. This will create a new certificate which can be shared with the IOE/RSSE.
Wrong PIN Code	The IO/RSS employee has entered the wrong PIN code too many times, blocking access to the SERMI certificate.	Use the 'Reset Certificate' API call. This will create a new certificate which can be shared with the IOE/RSSE.
Lost Device	The IO/RSS employee has lost their mobile device with the SERMI certificate.	Ask the End User to download the Digidentity Wallet app on their new device. Use the 'Reset Certificate' API call to create a new certificate for the IOE/RSSE.
QR Code Validity	The QR code in the invitation for the IOE is valid for 28 days. If not redeemed within this period, the QR code will expire and the IOE will be unable to register.	The CAB must send a new invitation to the IO or RSS employee.
Unable to Download the Digidentity Wallet	The Digidentity Wallet has specific device requirements for security reasons. Devices that do not adhere to these requirements are prevented from accessing the app.	Consult the FAQ for current device requirements and verify with the End User. Ask them to check for software updates. If the device does not meet requirements, advise the End User to use a different mobile device.
Unable to Receive or Send Chain Authorisation(s)	The IO Employee is unable to send chain authorisations, or the RSS employee is unable to receive chain authorisations.	Contact Digidentity support (sermi-support@digidentity.com). If there is still an active authorisation link, please share this in the support request.
Unable to Log In at Vehicle Manufacturer's Portal	The IO Employee is unable to log into a VM portal.	Check the status of the End User's authorisation (valid & approved). Check if the End User has a working internet connection. Check that the correct certificate is selected.

4.2 App Error Codes

Error Code	Dialog in App	Explanation	Solution
Orange Dolphin	No Internet Connection — Looks like your device is not connected to the internet. Check your connection, switch between mobile data and wifi, and try again.	No internet connection. Accessing a website should not work either. Common causes: airplane mode, or no Wi-Fi/4G/5G connection.	Ensure the End User is connected to the internet. Advise switching between mobile data and Wi-Fi. Once confirmed, ask them to tap 'Try again'.
Purple Kangaroo	Could not connect — Your device is connected to the internet, but the Digidentity	Backend unavailable while the device has internet. May be caused by a VPN, proxy,	Ensure connection. Advise switching between mobile data and Wi-Fi. Ask the End User to disable

Error Code	Dialog in App	Explanation	Solution
	app is unable to reach the server.	backend outage, or slow connection timeout.	any active VPN connections. Then tap ‘Try again’.
Green Tiger	Could not connect — The Digidentity app is unable to reach the server due to an issue on our end. Please come back later or contact customer service. (Error message text must be extracted/redacted before sharing externally.)	Backend returning unexpected responses. Known causes include internal errors, decryption errors, filesystem full, migration failure, or keystore exception.	Standard troubleshooting: update the app, close and restart, select the correct certificate, switch connection, reboot device, disable VPN, update OS. If unresolved, contact Digidentity Support.
Maroon Parrot	Unsupported device — Digidentity cannot guarantee the integrity of the certificate because your device is not supported/secure.	Device is jailbroken (iOS) or rooted (Android). Full-screen block on all app usage.	The device must be unjailbroken/unrooted to proceed. Otherwise, the End User must use a device that is not jailbroken or rooted.
White Whale	Something went wrong — Sorry for the inconvenience. Please try again. If the issue persists, come back later or contact customer service.	Generic default error for unclassified issues.	Standard troubleshooting: update the app, close and restart, select the correct certificate, switch connection, reboot device, disable VPN, update OS. If unresolved, contact Digidentity Support.
Yellow Pigeon	Something went wrong — Sorry for the inconvenience. Please try again. If the issue persists, come back later or contact customer service.	Secondary generic error, captured separately from White Whale so support can distinguish frequency and patterns.	Standard troubleshooting: update the app, close and restart, select the correct certificate, switch connection, reboot device, disable VPN, update OS. If unresolved, contact Digidentity Support.
Lemon Turtle	You don’t have the required services to continue and cannot register them yourself. Contact our helpdesk for more help.	User without a SERMI certificate has attempted to log into a VM portal. The SERMI certificate is invite-only and can only be acquired through invitation by the CAB.	Verify the user is in a country where SERMI is implemented. Check if the user has a valid SERMI certificate in their app (visible as a SERMI branded card). If not, assist them in acquiring one. If unresolved, contact Digidentity Support.

4.3 General Information & Tips

Tip / Information	Description	Recommendation
Expectation Management — IOE	The IO employee cannot access security-related RMI until the CAB approves the IO Employee’s authorisation. Approval can be given after the invitation with QR code is sent.	Create information material for the IO employee explaining the invitation and approval process. Clarify that authorisation is only granted after successful inspection by the CAB, even if registration is complete.

Tip / Information	Description	Recommendation
Expectation Management — RSSE	The RSS employee cannot receive chain authorisations from an IO employee until the CAB approves the RSS employee's authorisation. Approval can be given after the invitation with QR code is sent.	Create information material for the RSS employee explaining the invitation and approval process. Clarify that authorisation is only granted after successful inspection by the CAB.
Personal Information	Why can't an IOE/RSSE see their personal details in the Digidentity Wallet? Digidentity is the Trust Center (TC) for SERMI. Within the SERMI scheme, the TC is not permitted to know the IOE/RSSE's identity — only the CAB can hold this information. A SERMI account in the Wallet never contains personal information (name, email, date of birth); only the unique identifier (UID) is visible.	Digidentity is the Trust Center (TC) for SERMI and is not permitted to know the IOE/RSSE's identity. Inform users that only their UID is visible in the wallet. Their identity remains anonymous to Digidentity.
Additional Account(s)	If an IOE/RSSE downloads the Digidentity Wallet before scanning the CAB's QR code invitation, they may accidentally create a Digidentity account. When they later scan the QR invitation, the Wallet will notify them that a new SERMI account is being created ('different user'), resulting in two accounts.	The IOE/RSSE can still register for the SERMI certificate (log out and continue). The non-SERMI account can optionally be deleted via the switch icon in the top right corner. Users should always confirm they are deleting the correct account and should never delete accounts with services they still need.
Certificate Reset	Each IOE or RSSE is entitled to a maximum of three free resets within their 5-year authorisation period. After the third reset, additional requests will be subject to a fee, invoiced to the CAB.	Use the certificate reset when the user loses access to their certificate or does not activate it within the 28-day QR code validity period. The reset generates a new QR code for the user to reactivate their certificate.