Digidentity

SERMI – CAB @ DDY

Process description to issue a digital certificate by a SERMI accredited CAB.

Title	SERMI - CAB @ DDY
Date	21 April 2023
Author	Marcel Wendt
Version	2023-v1
Classification	Public

Digidentity

Revisions

Version	Date	Author	Changes Made (*)
2022-v1	21 April 2023	Marcel Wendt	Initial version

(*) All changes are marked in grey highlight.

Digidentity

Contents

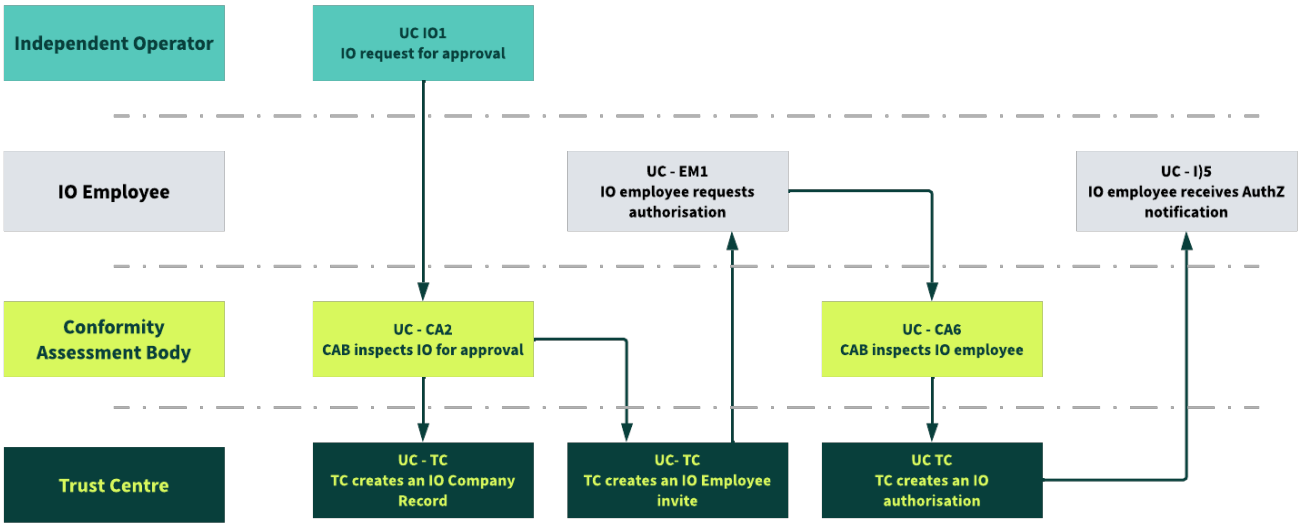
1 Introduction

SERMI was created to fulfill the requirements of several regulations including Regulation (EU) No. 2021/1244, Regulation (EU) No. 2018/858, and Regulation (EC) No. 692/2008. These regulations aim to provide standardised access to technical information, with specific provisions for access to vehicle security features. As a result, the 'EU Forum on Access to Vehicle RMI' was established and issued a report in October 2009 outlining the process and architecture for accessing security-related RMI (Repair Maintenance Information), as well as an accreditation scheme for Independent Operators (IO).

The Conformity Assessment Bodies (CAB) are responsible for the inspection of IO's and their respective IO employees and for issuing approval and authorisation inspection certificates in accordance with the SERMI scheme, and for revoking such certificates. This document outlines the detailed process for a CAB to initiate and authorise digital inspection certificates for employees of Independent Operators to access security-related vehicle RMI in accordance with the Regulation.

This document will describe the relevant use cases between the CAB and the Trust Centre in the following order:

- UC CA1: Setting up a business relationship with Trust Center.
- UC CA2: CAB Inspects IO for approval.
- UC CA8: Informs TC in order to issue a digital certificate.
- UC CA6: CAB inspects IO employee for authorisation.



Digidentity

2 UC CA1. Setting up a business relationship with Trust Center

To participate in the SERMI Scheme, the CAB must establish a contractual agreement with a selected Trust Center. This contract is an appendix to the overall framework agreement between the SERMI association and Digidentity B.V. (Digidentity).

To enable the implementation process, the CAB must sign a Non-Disclosure Agreement (NDA) with Digidentity. This will grant the CAB access to Digidentity's Pre-Production environment, allowing them to begin the actual implementation of the API's.

Please find below the contact details for Digidentity:

Type	Value
Organisation name	Digidentity BV
Address	Waldorpstraat 13-F 2521 CA The Hague The Netherlands
E-mail address for onboarding and non-technical questions	sermi@digidentity.com
Documentation	https://connect.digidentity.com
E-mail address for technical question	eid@digidentity.com
Developer documentation	https://docs.digidentity.com

Digidentity

3 UC CA2. CAB Inspects IO for approval.

To enable the Trust Centre to fulfil its duties, the CAB must provide data from the Independent Operator (IO) to structure the information appropriately. This allows an IO to request authorisation for access to security related RMI data.

The following attributes are required:

Field	Description
cab_uid	Contains a value generated by the SERMI organisation which shall be unique to an accredited CAB. This value shall have a maximum of 64bits.
io_uid	Contains a value generated by the CAB which represents the IO/RSS legal name, the address and the VAT or unique official business identification number. <IO LEGALNAME>/<IO ADDRESS>/<IO VAT NUMBER> Example: THE BEST GARAGE/WALDORPSTRAAT13FTHEHAGUE2521CA/VAT:NL819696079B01
rss_uid	If the organisation functions as a Remote Service Supplier (RSS), the following attributes should be utilised, which have the same structure as the IOUID.
organization_name	Name of the IO or RSS
street	Street name of the IO or RSS
house_number	House number of the IO or RSS
postcode	Postcode of the IO or RSS
city	City of the IO or RSS
country_code	The ISO 3166 country code of the IO or RSS
vat_number	The VAT number of the IO/RSS should be provided. If the IO or RSS does not possess a VAT number, an alternative unique number must be chosen according to the following format: < ISO-3166-1-COUNTRY-CODE OF THE CAB >/8 DIGITS/2 check DIGITS>

There are two ways in which this data can be delivered both manual as via the Digidentity API.

3.1 Manual provisioning of IO data

To provision an Independent Operator into the system, an e-mail must be sent to Digidentity's Customer Success team. The aforementioned attributes can be sent to the following e-mail address: sermi@digidentity.com with the subject description "**Create IO**".

Digidentity will respond with the results of the onboarding within two business days.

This provision route is only permitted during the initial phase of the SERMI project, providing the CAB with the chance to become accredited for the Scheme. However, the API route must be implemented as soon as possible.

3.2 API provisioning of IO data

The API provisioning is the recommended method and must be implemented no later than two months after contract signing.

The attributes can be sent using Digidentity's API call "**Create IO**" with the following URL: http://gate.digidentity-preproduction.eu/sermi/io

The developer documentation is available at: https://docs.digidentity.com/

Digidentity

4 UC CA8. Informs TC in order to issue a digital certificate.

To issue a digital certificate to an IO employee, the following attributes must be sent to Digidentity. It is important to note that all personal information must be pseudonymised.

Field	Description
cab_uid	Contains a value generated by the SERMI organisation which shall be unique to an accredited CAB. This value shall have a maximum of 64bits.
io_uid	Contains a value generated by the CAB which represents the IO/RSS legal name, the address and the VAT or unique official business identification number. <IO LEGALNAME>/<IO ADDRESS>/<IO VAT NUMBER> Example: THE BEST GARAGE /WALDORPSTRAAT13FTHEHAGUE2521CA/VAT:NL819696079B01
rss_uid	If the organisation functions as a Remote Service Supplier (RSS), the following attributes should be utilised, which have the same structure as the IOUID.
loe_uid	Contains a value generated by the CAB which represents the IO/RSS employee identity. This value shall be unique to an authorised user: if a user requests a new digital certificate from the same CAB or another CAB (after a renewal or a revocation), he/she has to be associated to the same UID. The IOEUID/RSSEUID is built as follows: < ISO-3166-1-COUNTRY-CODE OF THE CAB/NAME OF THE CAB/CHARACTER ALPHANUMERIC CODE> This value shall have a maximum of 64bits. Example: NL/ THE BEST GARAGE /1234567890A
rsse_uid	If the organisation functions as a Remote Service Supplier (RSS), the following attributes should be utilised, which have the same structure as the IOEUID.
email	E-mail address from the IO Employee, this e-mail must be unique in our platform.
terms_and_conditions_accepted	Only when the Digidentity T&Cs are accepted (value true) an certificate will be issued. The CAB is responsible to inform the IO Employee with the latest Digidentity T&Cs.

This data can be delivered either manually or through the Digidentity API. It is important to note that once a digital certificate is issued and accepted by an IO employee, it cannot be used until authorisation is approved by the CAB.

4.1 Manual provisioning of IOE data

To provision an IO Employee into the system, an e-mail must be sent to Digidentity's Customer Success team. The attributes can be sent to the following e-mail address: sermi@digidentity.com with the subject description "**Create IO Employee**".

Digidentity will respond with the results of the onboarding within two business days. The result will be a unique URL to be send to the IO Employee to start their onboarding.

This provision route is only permitted during the initial phase of the SERMI project, providing the CAB with the chance to become accredited for the Scheme. However, the API route must be implemented as soon as possible.

4.2 API provisioning of IOE data

The API provisioning is the recommended method and must be implemented no later than two months after contract signing.

The attributes can be sent using Digidentity's API call "**Create IO Employee**" with the following URL: http://gate.digidentity-preproduction.eu/sermi/ioe

The developer documentation is available at: https://docs.digidentity.com/

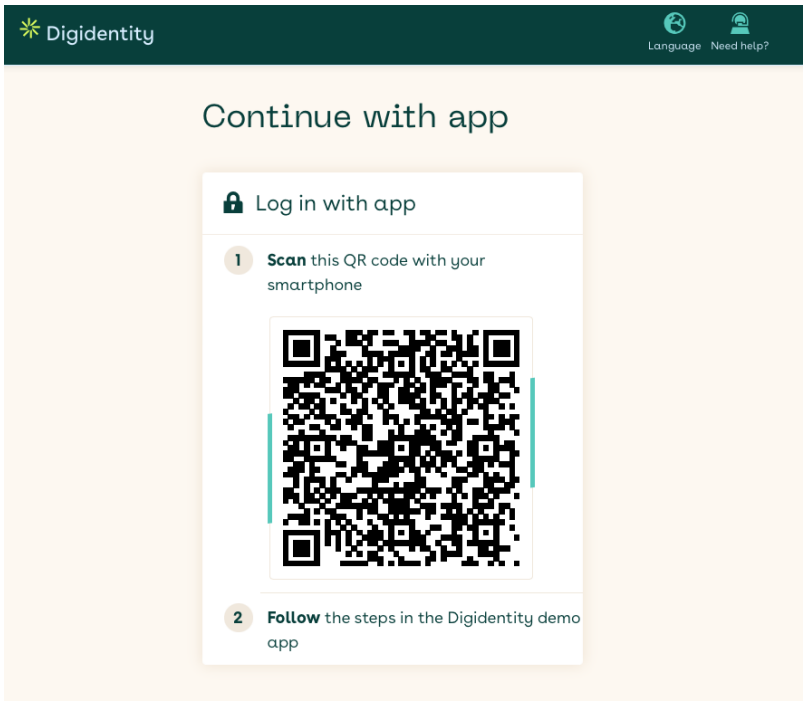
4.3 Sending the invitation manually

CAB sends the invitation to the IO/RSS staff member through the TC, requesting them to establish a digital identity with a digital certificate, utilising a personalised.

The result from both 4.1 as 4.2 will be a unique onboarding URL that could like:

https://open.digidentity-preproduction.eu/Epsy9eJW1eRgQLmQ8

The QR code is displayed to the IO employee through the URL.



Once the QR code is scanned using a smartphone's camera, the Digidentity App is automatically downloaded, and an account is created. The IO Employee is only required to generate a 5-digit PIN and enter it twice.

Please note that the QR code can only be used once.

5 UC CA6. CAB inspects IO employee for authorisation

Once an IO and one or more IOEs have been created on the Digidentity platform, the CAB must approve the digital certificate.

Field	Description
cab_uid	Contains a value generated by the SERMI organisation which shall be unique to an accredited CAB. This value shall have a maximum of 64bits.
io_uid	See the definition in article 5
rss_uid	If the organisation functions as a Remote Service Supplier (RSS), the following attributes should be utilised, which have the same structure as the IOUID.
Ioe_uid	See the definition in article 5
rsse_uid	If the organisation functions as a Remote Service Supplier (RSS), the following attributes should be utilised, which have the same structure as the IOEUID.
action	Approve or reject
reason	Reason why a rejection is submitted.

There are two ways in which this data can be delivered both manual as via the Digidentity API.

5.1 Manual approval of an IO Employee certificate

To provision an Independent Operator into the system, an e-mail must be sent to Digidentity's Customer Success team. The attributes can be sent to the following e-mail address: sermi@digidentity.com with the subject description "**Authorise IO Employee**".

Digidentity will respond with the results of the onboarding within two business days.

This provision route is only permitted during the initial phase of the SERMI project, providing the CAB with the chance to become accredited for the Scheme. However, the API route must be implemented as soon as possible.

5.2 API approval of an IO Employee certificate

The API provisioning is the recommended method and must be implemented no later than two months after contract signing.

The attributes can be sent using Digidentity's API call "**Authorise IO Employee**" with the following URL: http://gate.digidentity-preproduction.eu/sermi/ioe/authorization

The developer documentation is available at: https://docs.digidentity.com/

5.3 IO employee receives AuthZ notification.

When the action "Approve" or "Revoke" is triggered on the Digidentity platform, the IO Employee will automatically receive an e-mail regarding the corresponding action. This e-mail will confirm whether they have been granted access to the security related RMI data or if access has been denied.