Digital Identity (AMOS SS 2022)

Introduction

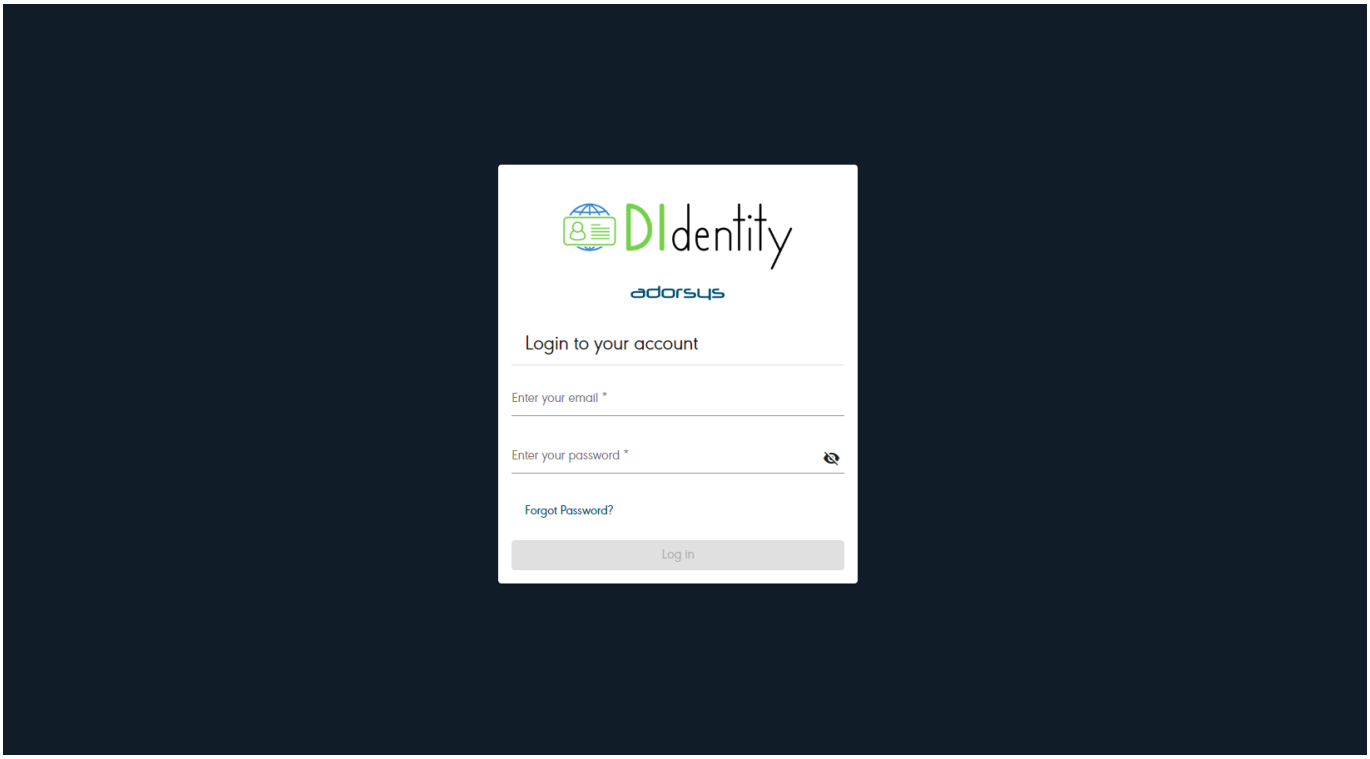
This document helps the user (HR employee) to use the Digital Identity Software and understand the main implemented feature. Hoping that the application itself is intuitive.

User Guide

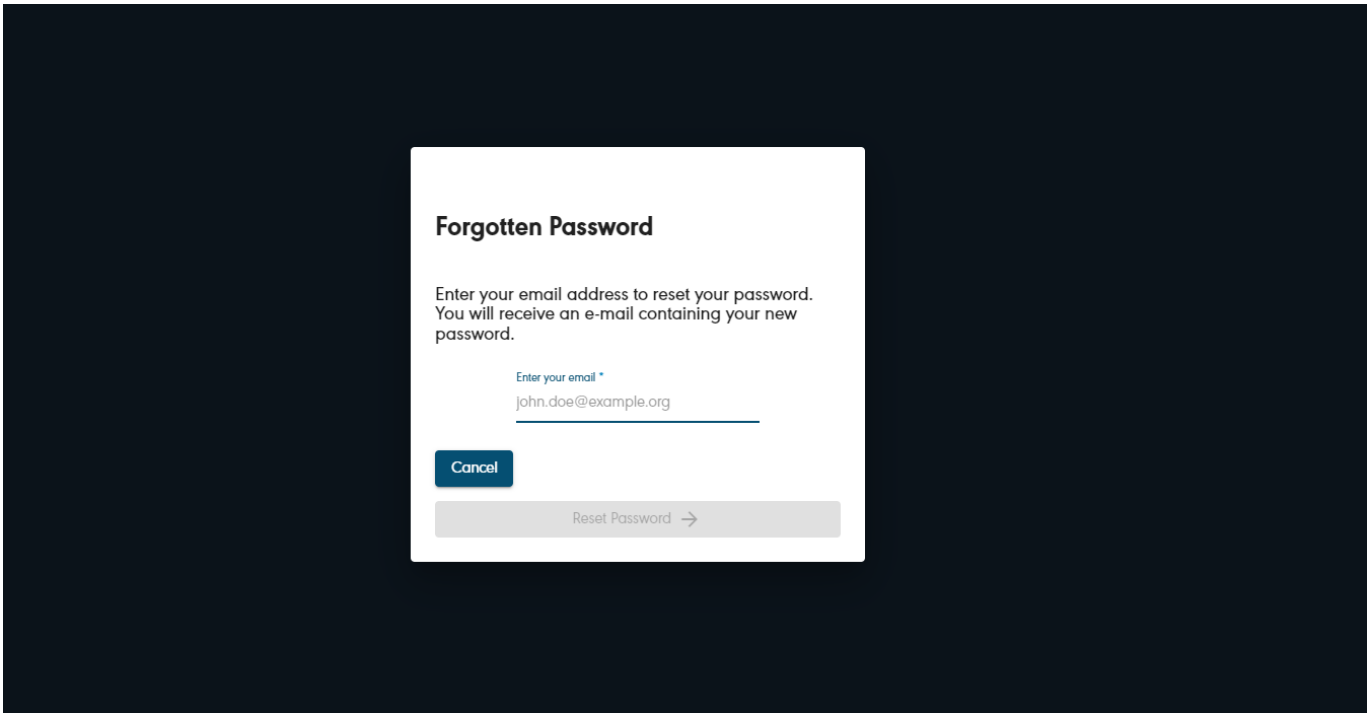
The following views can be found in our application.

Login Page

The login page is used to log in to the software by entering the email and password. It is the first page that appears when launching the application.



- To have access to the different views and functionalities of the application, the user must be logged in and therefore registered.
- after the registration process the user obtains an initial password which will allow him to make his first connection.
- On the login page the user has the possibility to display his password in plain text by clicking on the following icon  .
- In case the user has forgotten his password, he can click on "**Forgot password?**" to obtain a new password via email after entering the email adress of his account. After clicking on it the user gets this pop up:



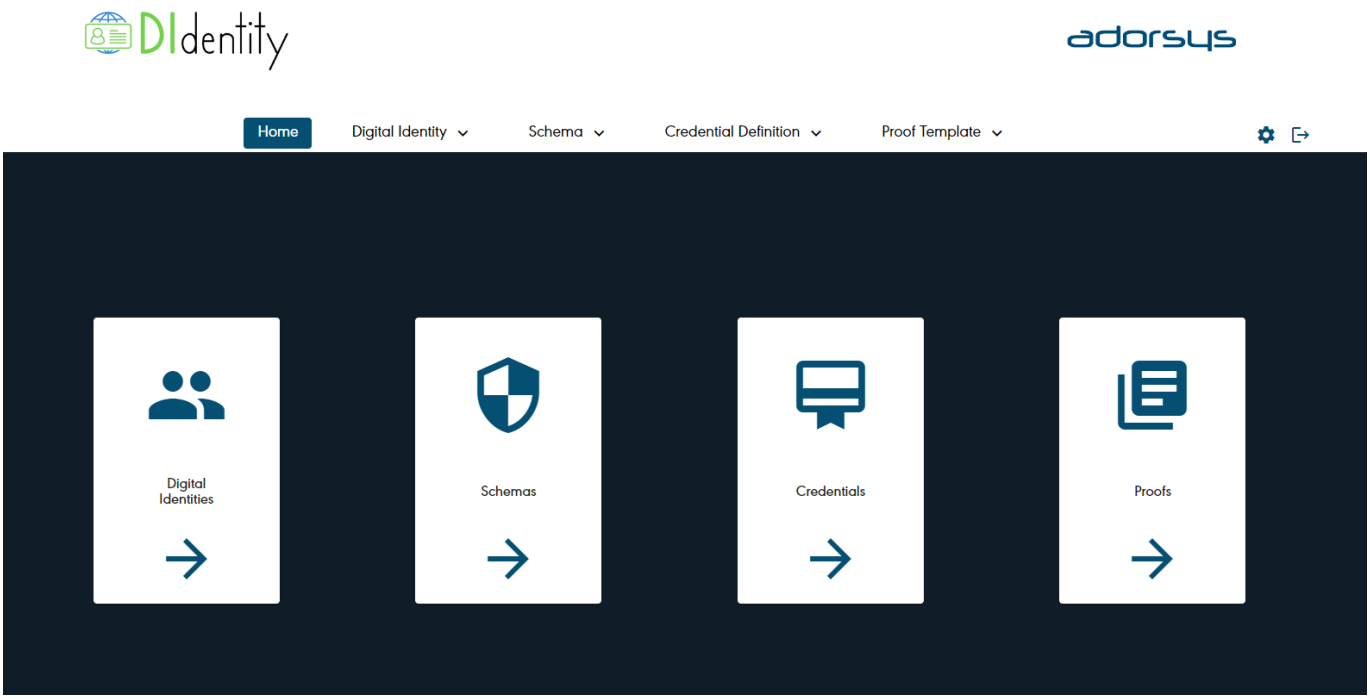
- when the user clicks on login after having filled in the correct login data, he gets redirected to the landing page of the application.

Creation of first user:

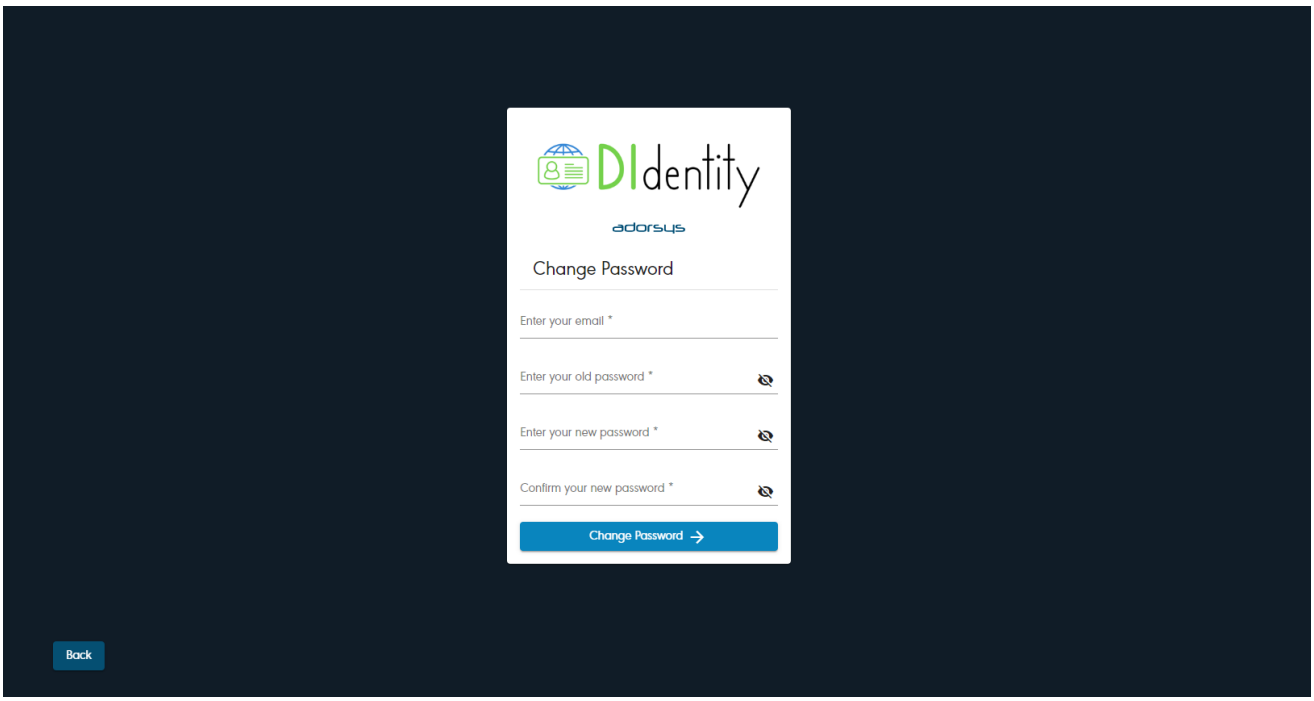
To create a first user account on the empty application click on 'Forgot Password?' and enter the mail of the first HR employee. He gets then an email with a inital password. (That works only once on new, fresh instances of the application)

Home (Landing Page)

After you are logged in to the software, you are redirected to a *landing page* which is the **Home** view of the application where you can see cards that allow quick access to the overview pages of the application. On this view you can also see a navigation menu that allows you to access other views.



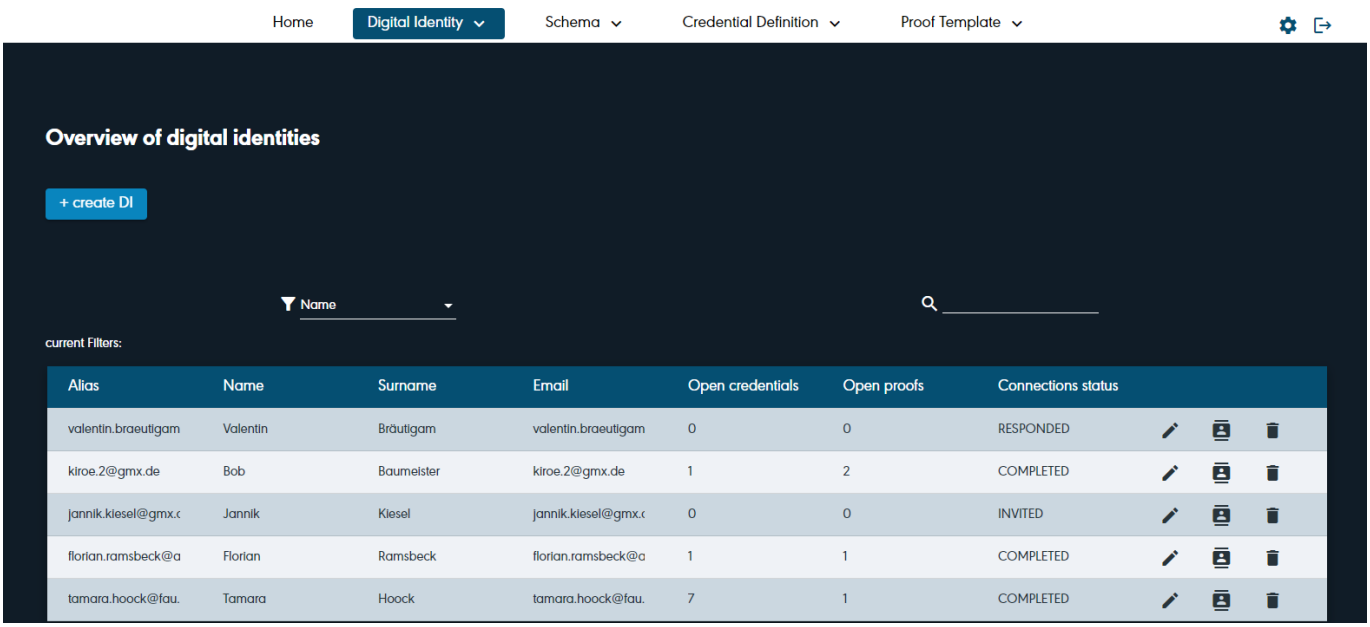
-  implements the change password functionality. After clicking on it the user is redirected to this view where he can set a new password which meets the password criteria (at least each one lower case, upper case and numerical character and at least 8 characters in total):



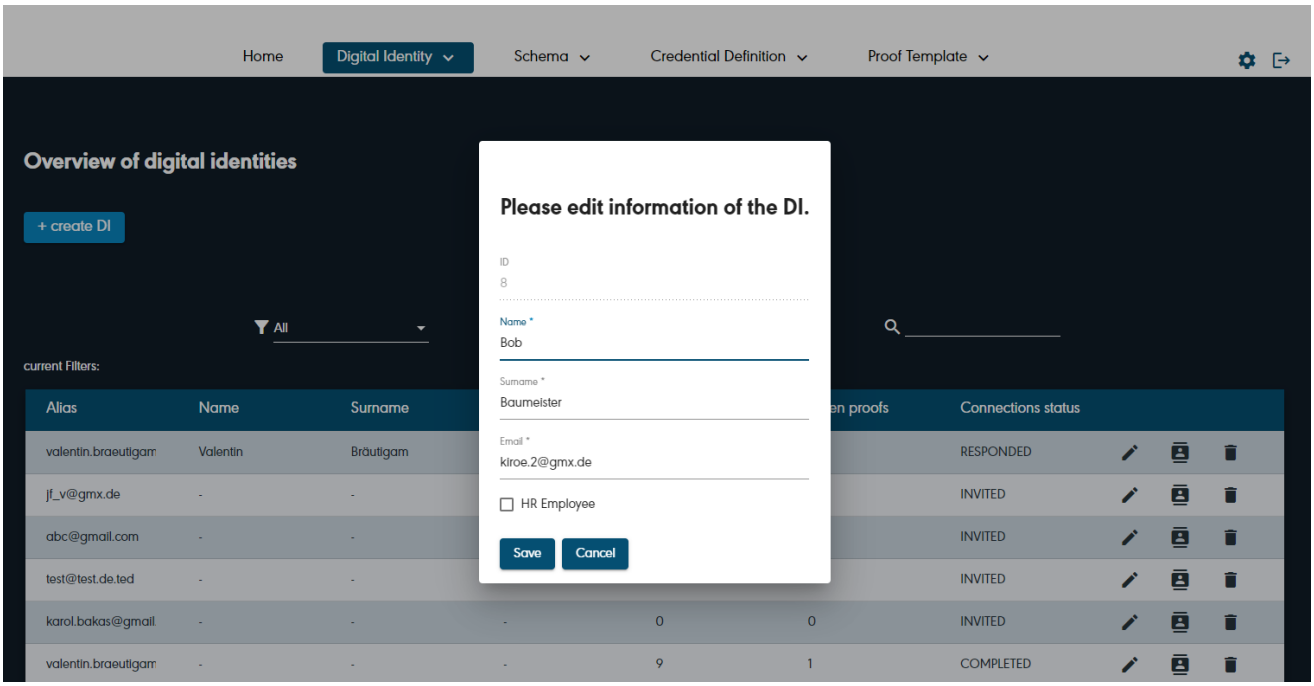
-  is used to log the user out.

Overview of Digital Identities

In this view, you can get an overview of all the created digital identities and open processes. It is also possible here to perform some actions on the existing digital identities like edit or delete them.

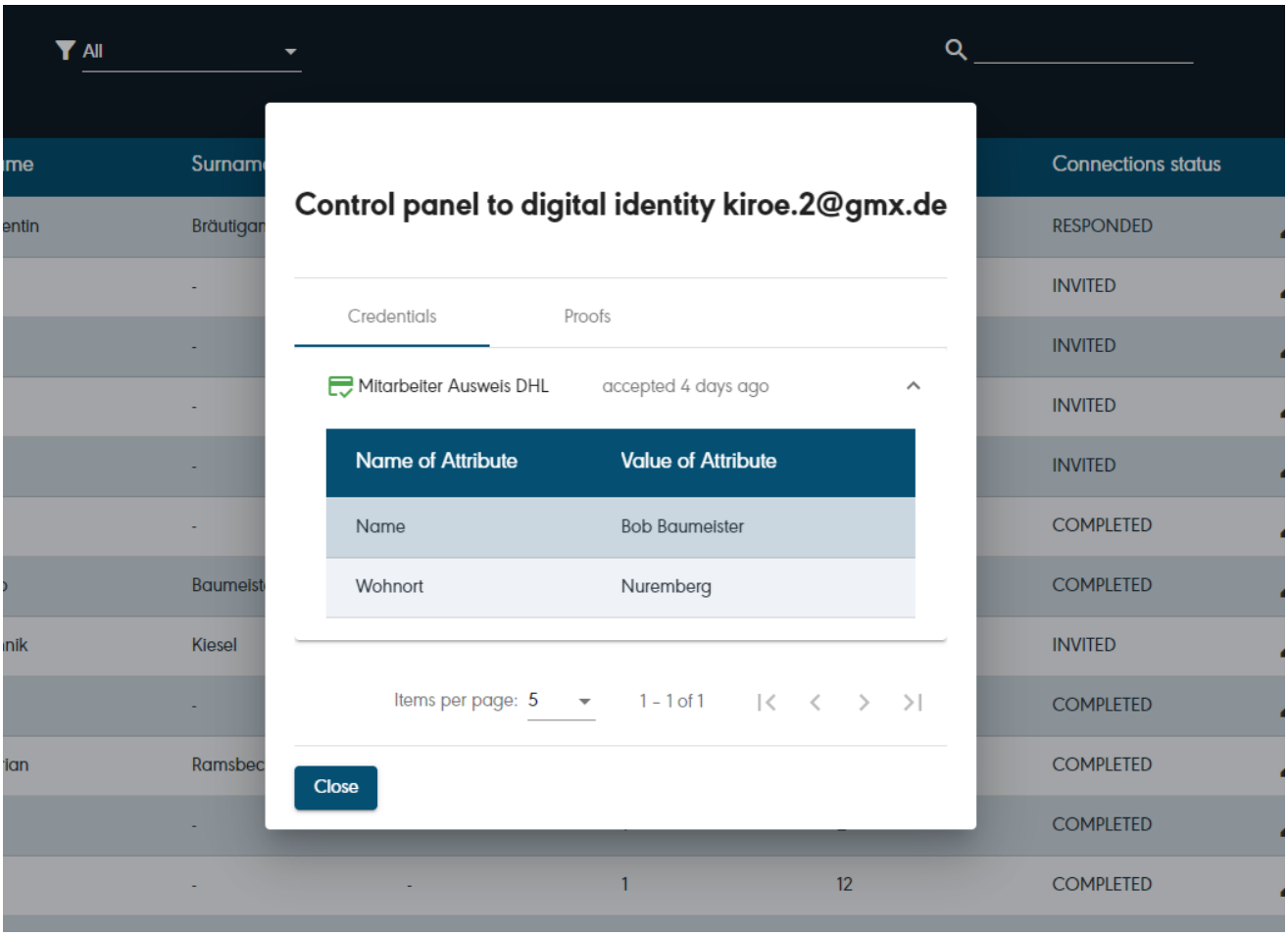


-  implements the edit functionality. By clicking on this icon a pop-up opens and allows the user to modify the information concerning the Digital Identity/Connection.

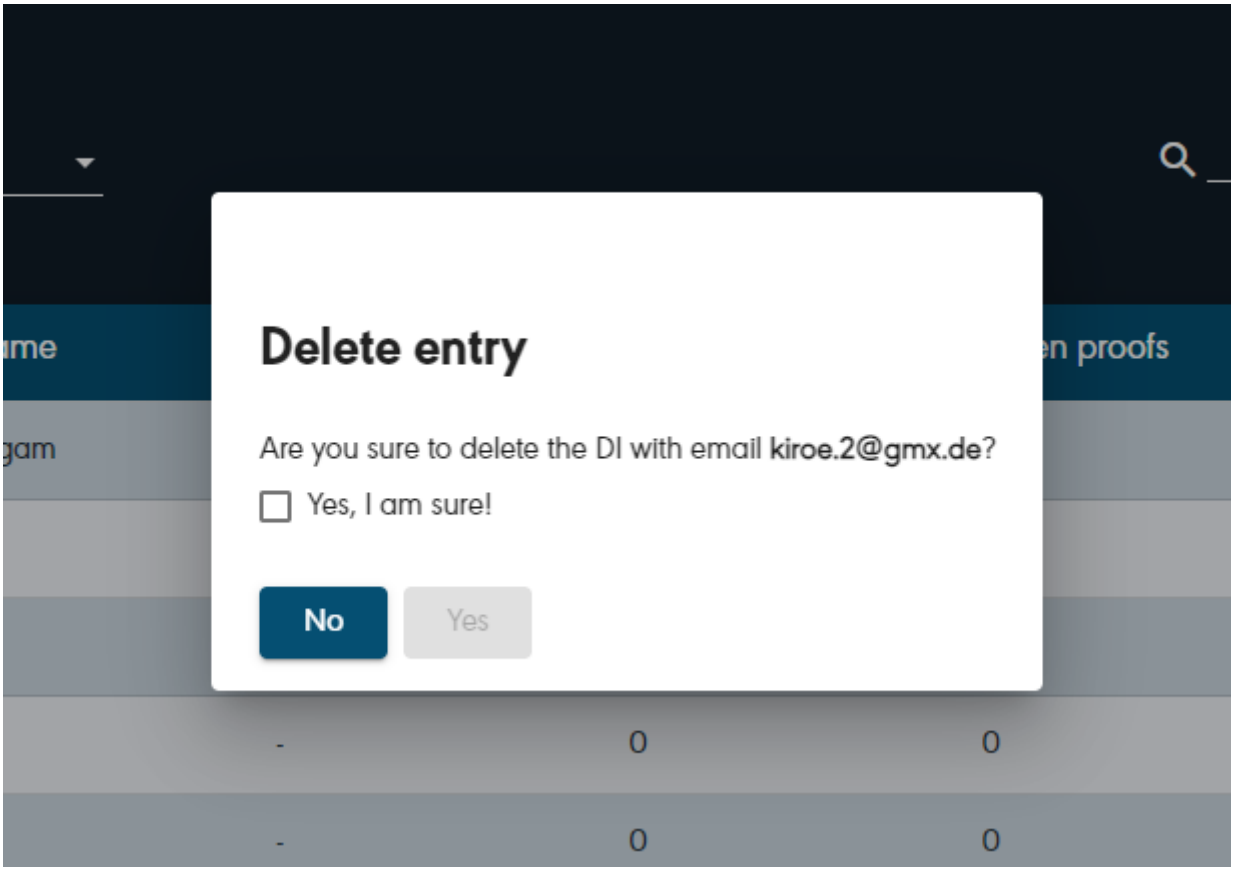


-  By clicking on this icon, a pop-up windows opens which displays a table showing credentials offered and issued, as well as a table showing the proofs requested and received from connections. The credential table has columns that indicate the name of the credential, whether the credential has been

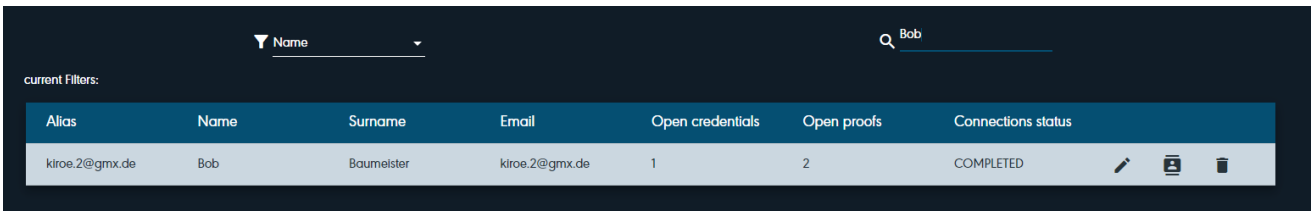
issued or created and the time associated with this operation. For proofs linked to the digital identity it is the same but it indicates whether the proof was requested or received by the connection.



-  can be clicked to delete the Digital Identity/Connection.

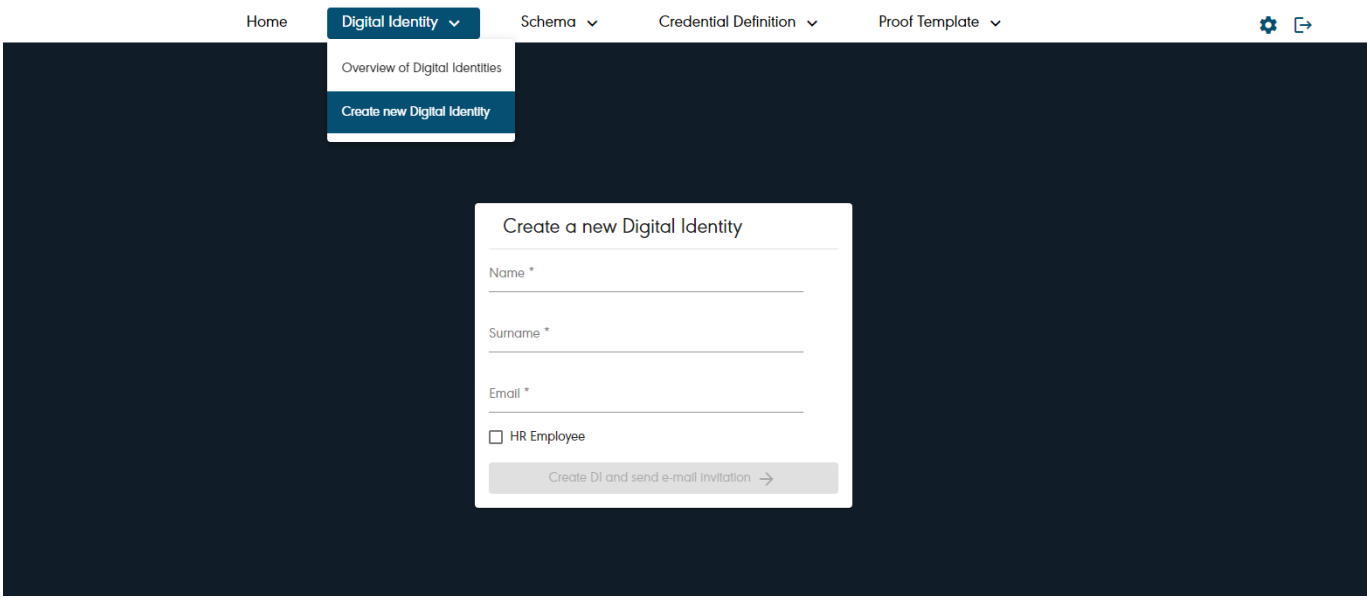


- The user can use filters to search the list of Digital identity. He can select the column of the table he wants to filter by and use the search bar to add the filters.



Create new Digital Identity

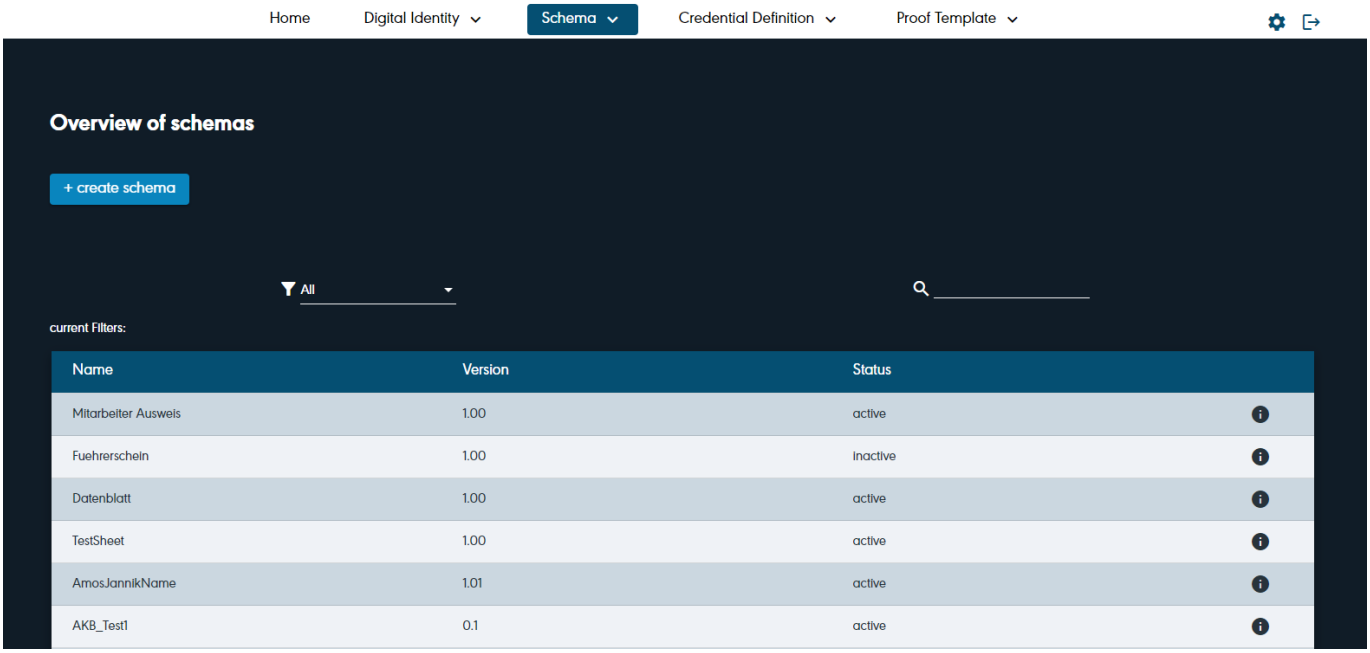
To create a new digital identity the user simply needs to fill in the different input fields in the 'Create New Identity' view with the valid data. The required data is the name, surname and email of the employee whose digital information is to be created. This data gets stored and is later used for identity verification in case of a HR employee.



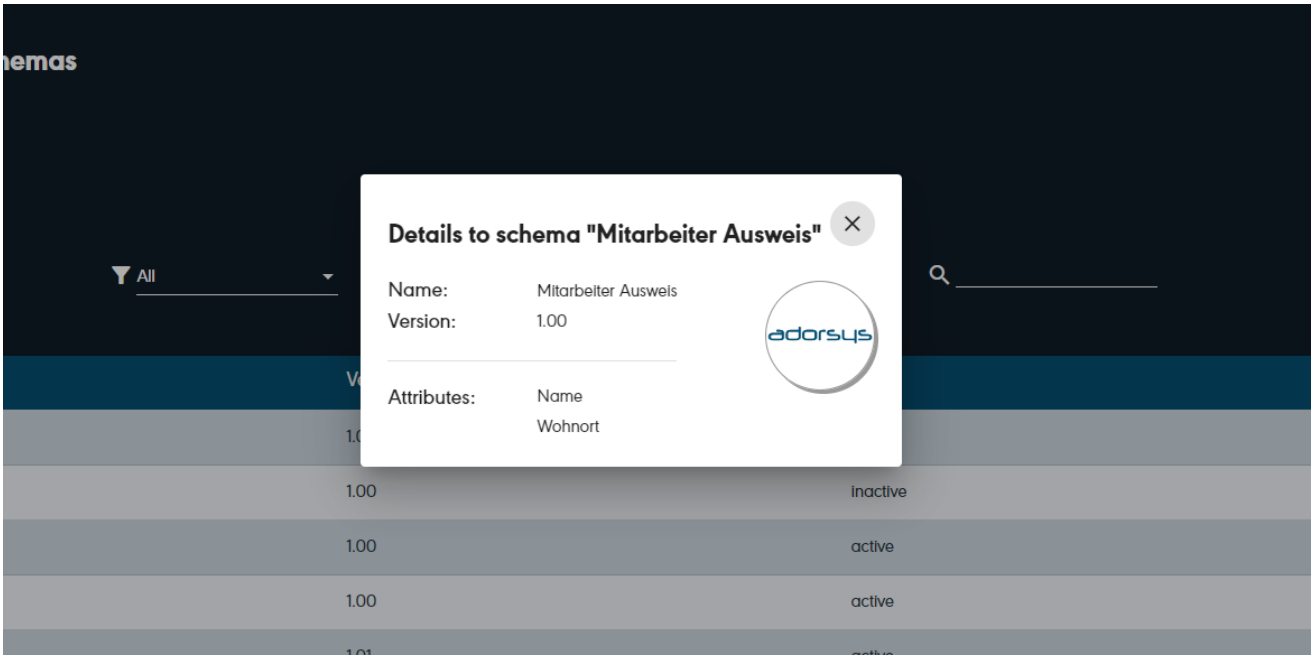
During the creation of a digital identity/connection the user can specify if it belongs to an HR employee by clicking in the checkbox tagged with 'HR employee' and in this case the employee belonging to this digital identity will receive an additonal email to the one with connection information and the QR code. This second email contains an initial password which allows him to use the DIdentity software as an HR employee and to manage the digital identities in the application.

Overview of Schemas

This view shows all created schemas including their version and status. The status can be 'active' or 'inactive' which indicates whether the schema is in use and therefore if credential definitions can be created from it.



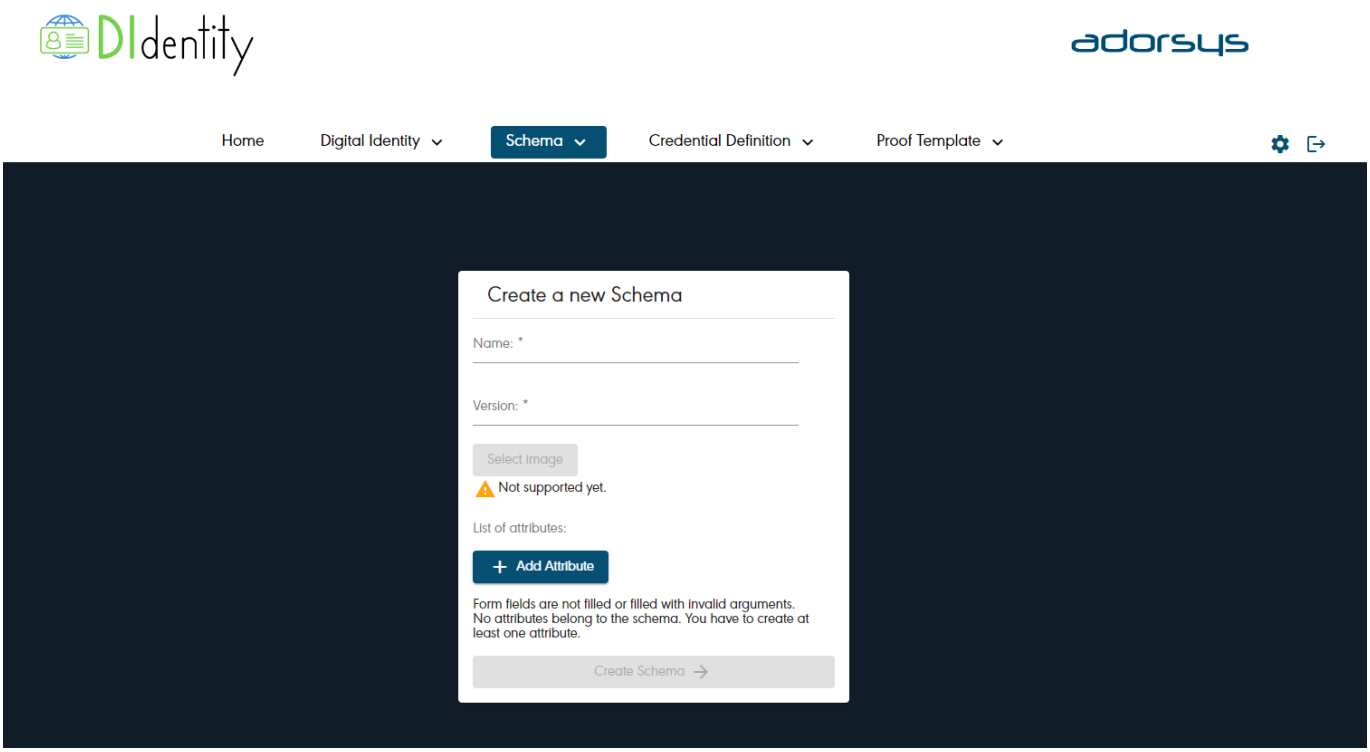
- To get more details about a schema the user can click on  . Additional information is for example an connected image and the attributes of the schema.



- It is also possible to filter in the list of schemas similar to filtering in the overview of digital identities.

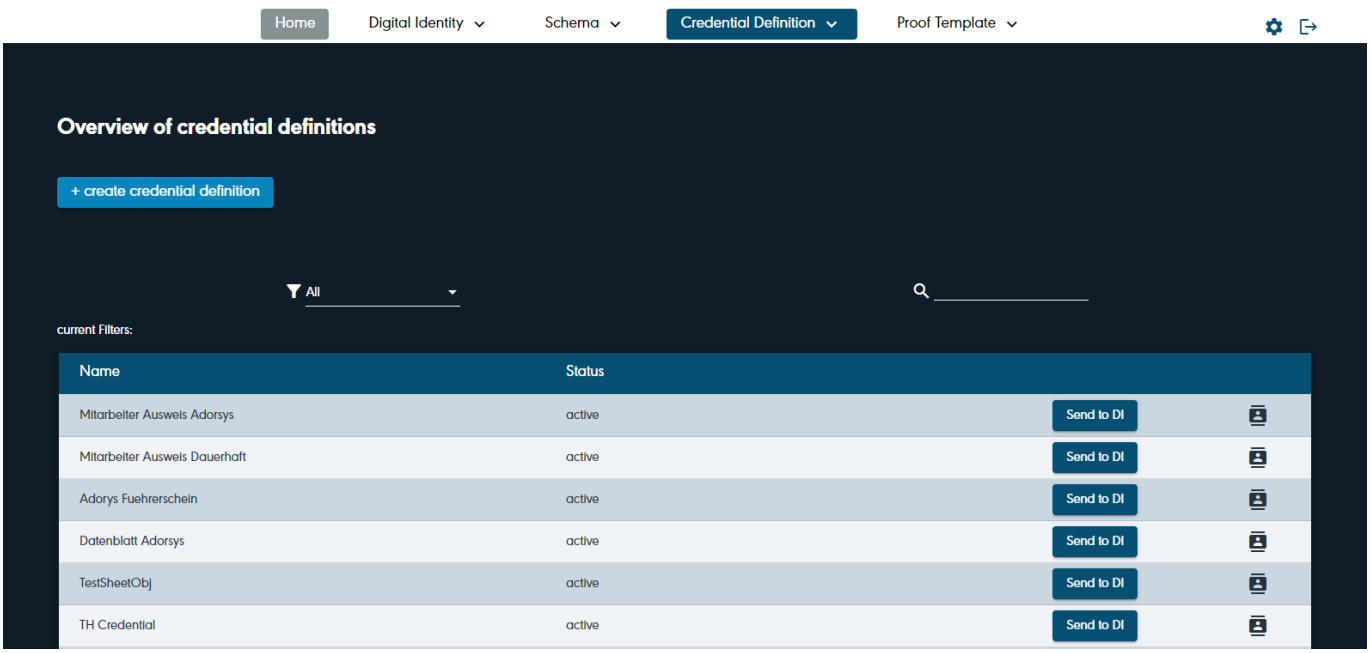
Create new Schema

The *creation of schemas* is possible via the **create schema** view. To create a schema the user must fill in the following data: the name, version and image (*unfortunately the image is not yet supported*) associated with this schema. There is also the possibility to add attributes by clicking on 'add attribute' and typing in a name. A schema has to contain at least one attribute to be created.

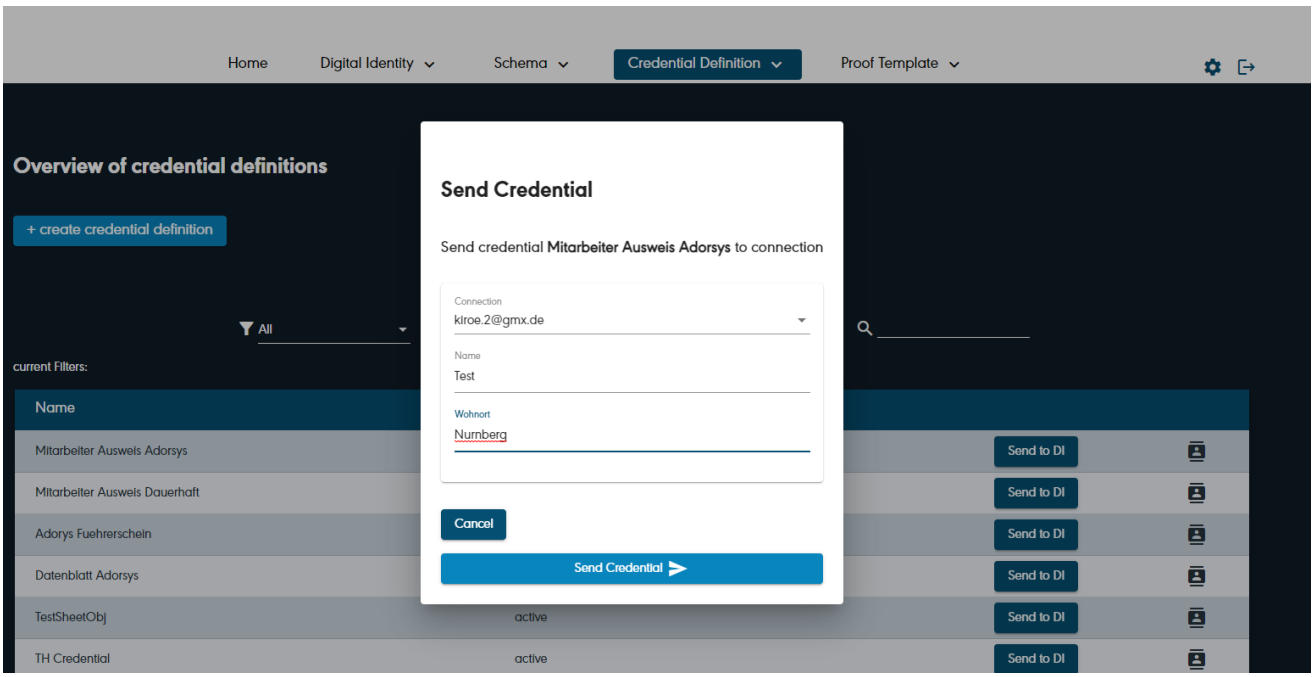


Overview of Credential Definitions

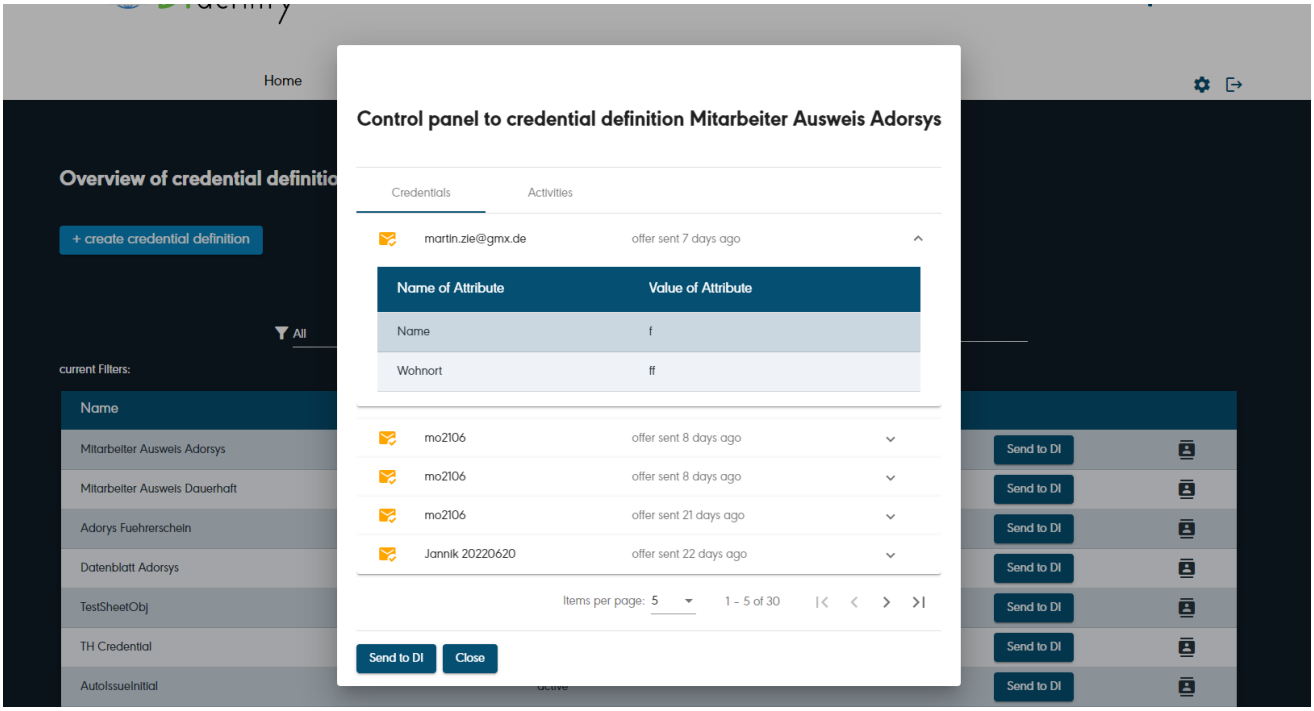
This view shows all created credential definitions.



- In this view the user can send a credential defined by one of the created credential definitions to a digital identity by clicking on the "**Send to DI**" button and choosing the digital identity to which he would like to send it and by filling in the requested attributes.



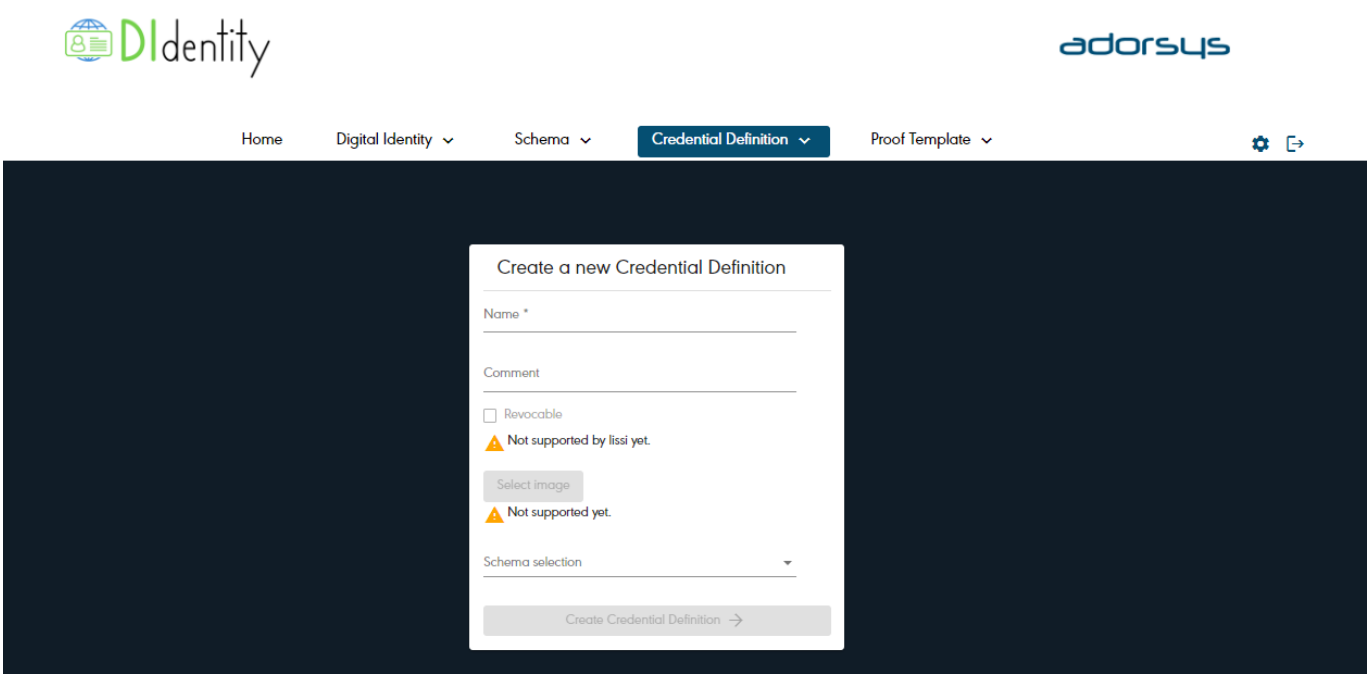
- By clicking on this icon  a pop-up opens and a table is displayed showing all actions of the credential definition with respect to digital identities.



- Filtering is also possible in this list of credential definitions similar to filtering in the overview of digital identities.

Create new Credential Definition

To create a credential definition the user can use the 'create credential definition' button on the credential definition overview page or simply use the menu item in the navigation bar.

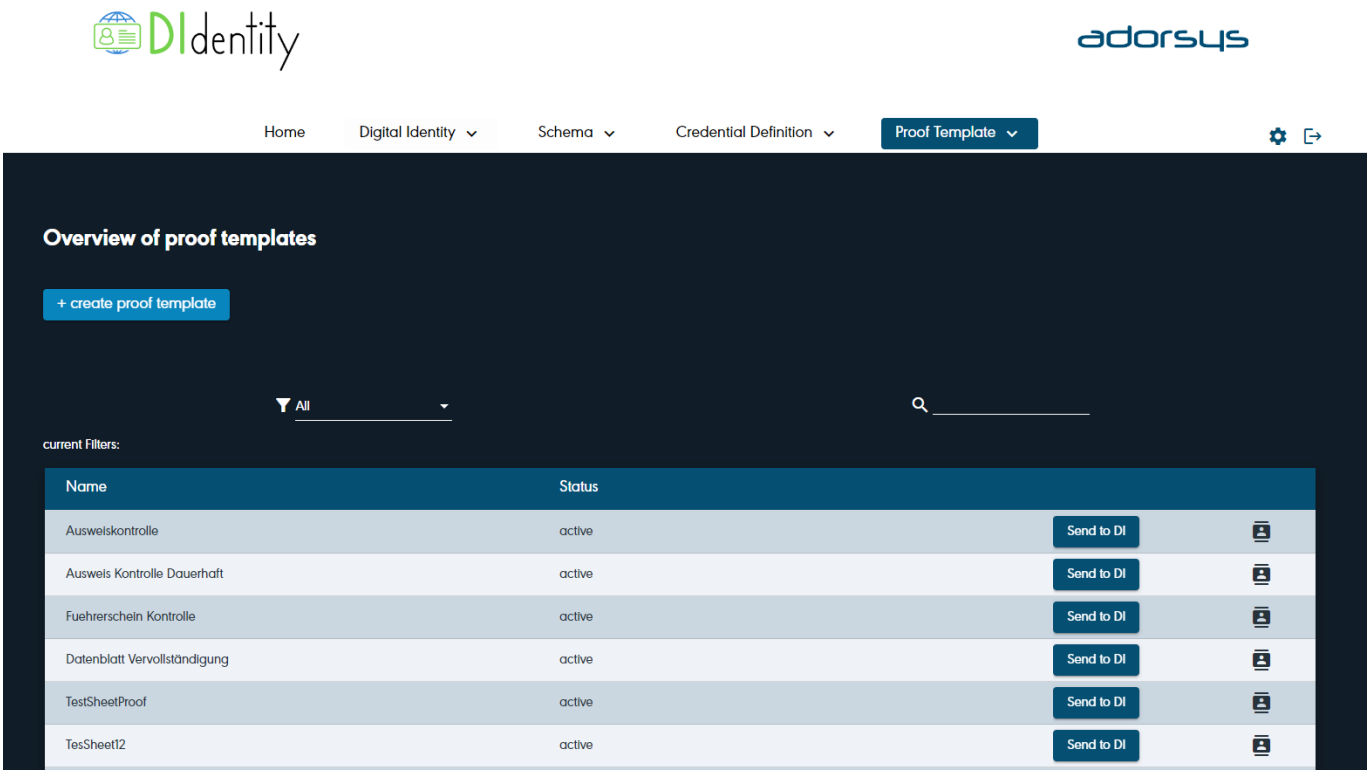


The user has to enter a name for the new credential definition, optionally enter a comment, select whether the credential definition is revocable using the checkbox (*unfortunately it is not supported by lissi yet*) and finally

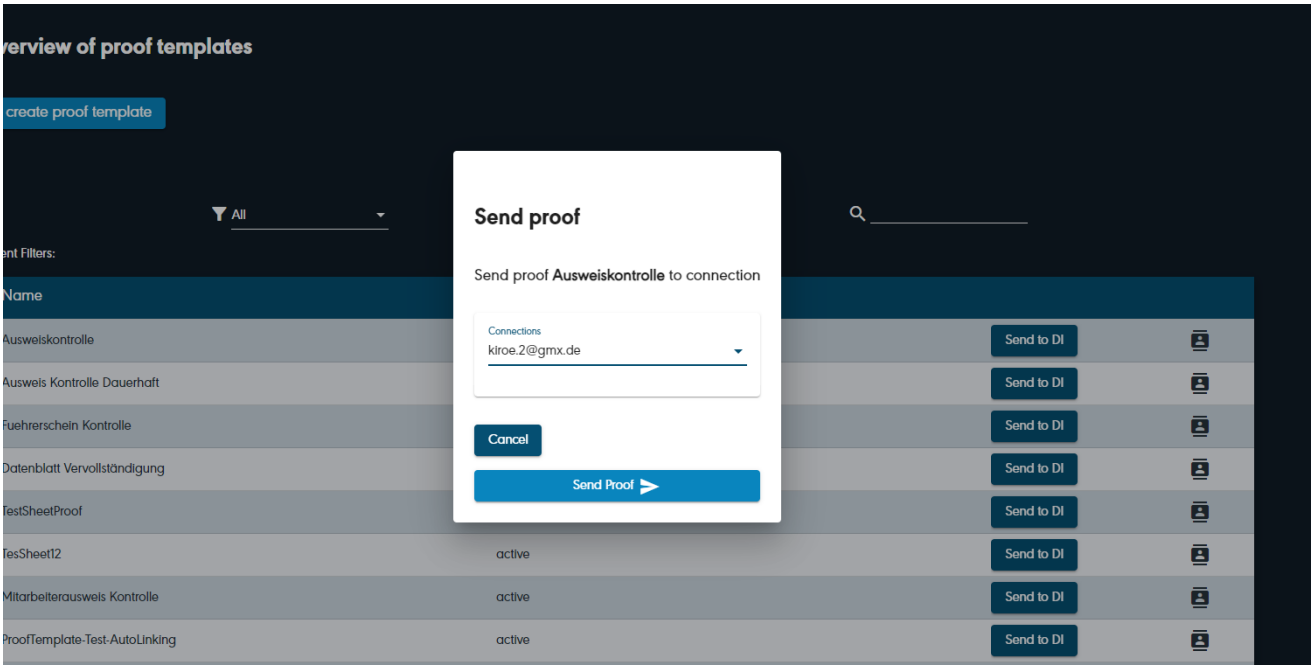
associate a schema with the new credential definition. The credentials defined by this credential definition will later contain the attributes of the selected schema.

Overview of Proof Templates

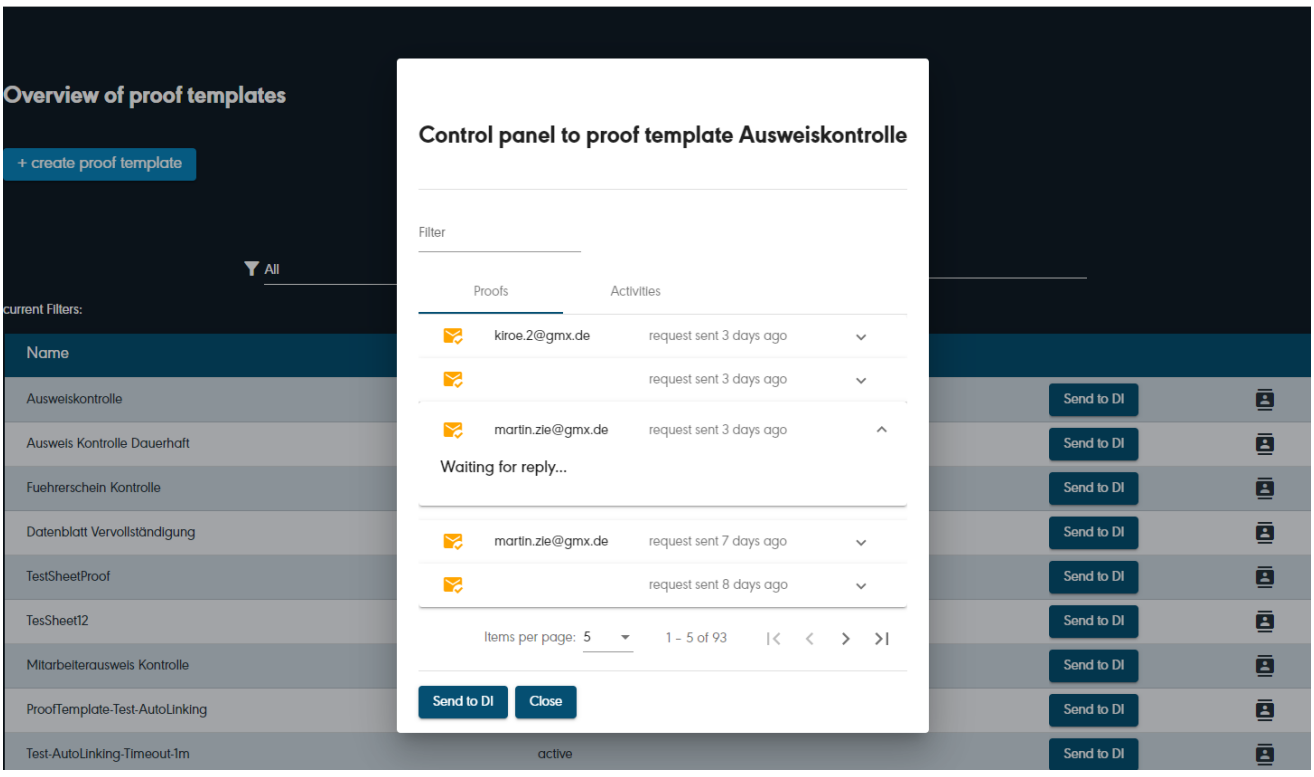
This view presents all the proof templates that have been created and stored.



- In this view the user can send a proof to a digital identity by clicking on the "**Send to DI**" button and choosing the digital identity to which he would like to send a proof.



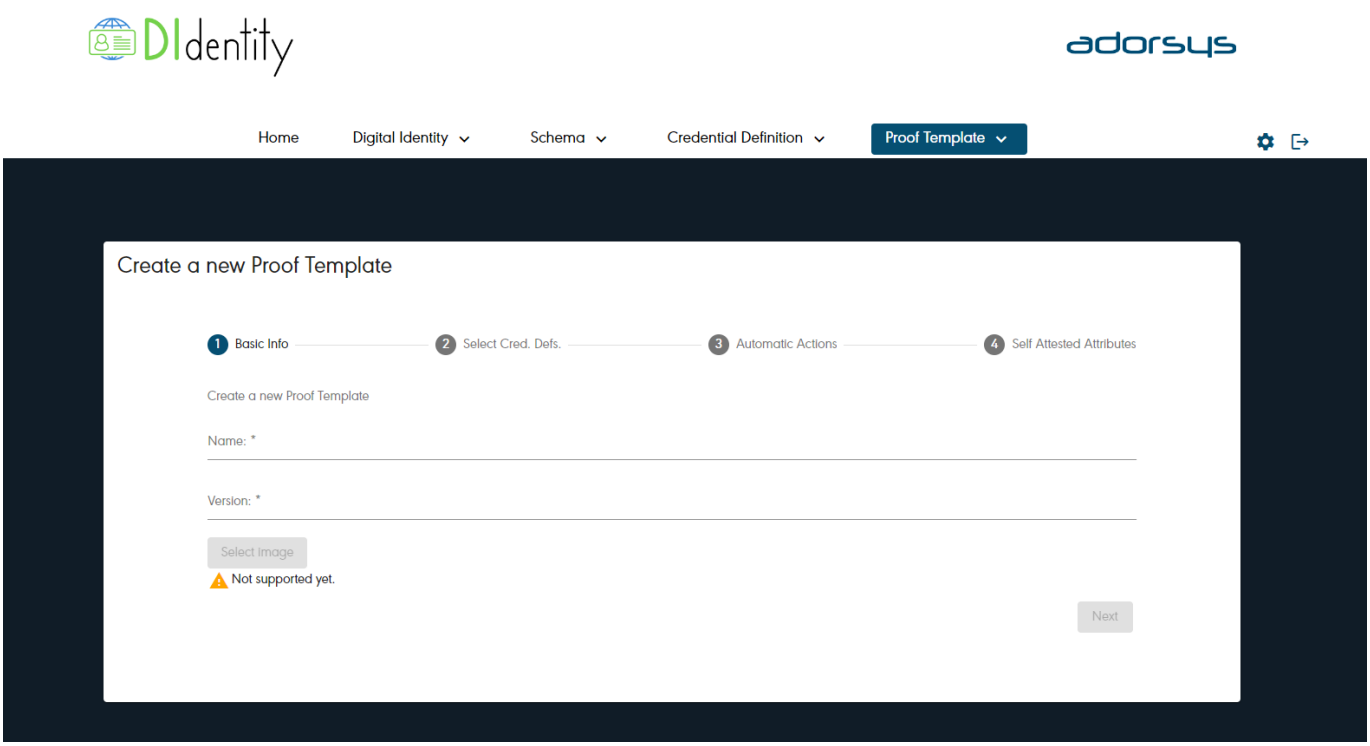
- The user can in this view also have a detailed overview of all the digital identities to which the proof has been sent and also the activities belonging to this proof template by clicking on this icon  .



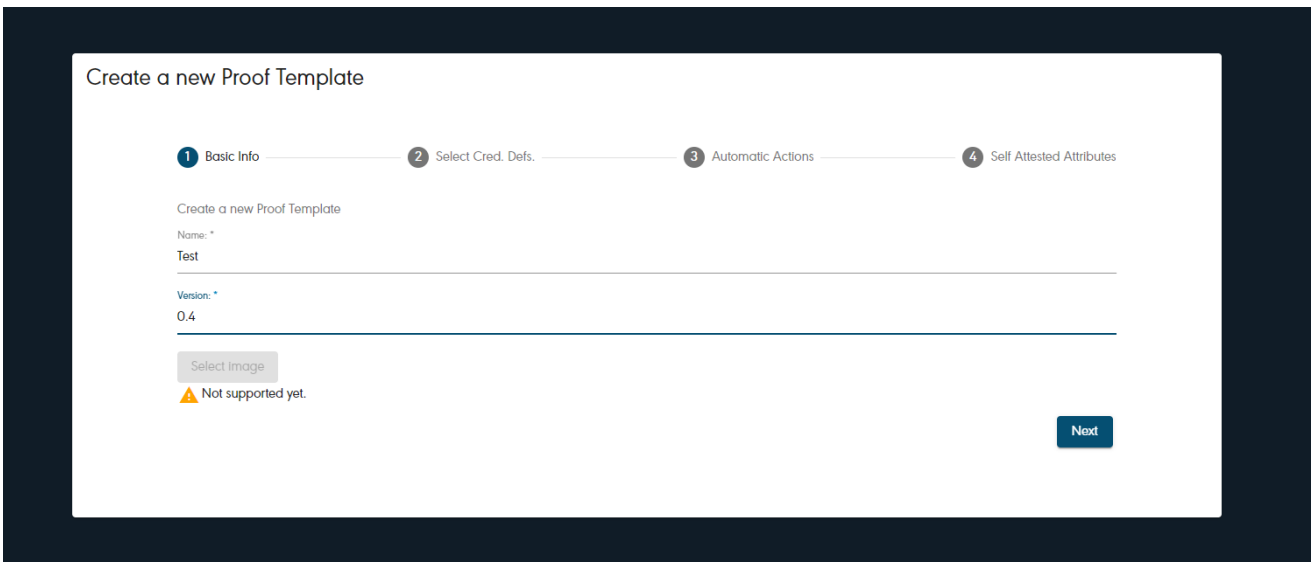
- Filtering is also possible in this list of proof template similar to filtering in the overview of digital identities.

Create new Proof Template

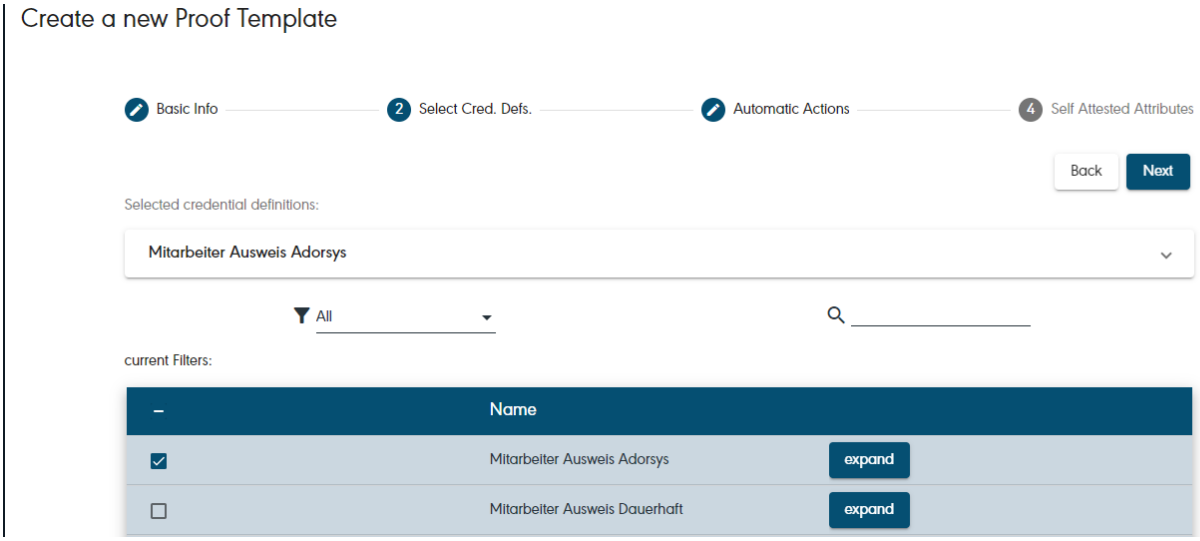
This page allows the user to create a new proof template. To create a new proof template the user has to follow 4 steps.



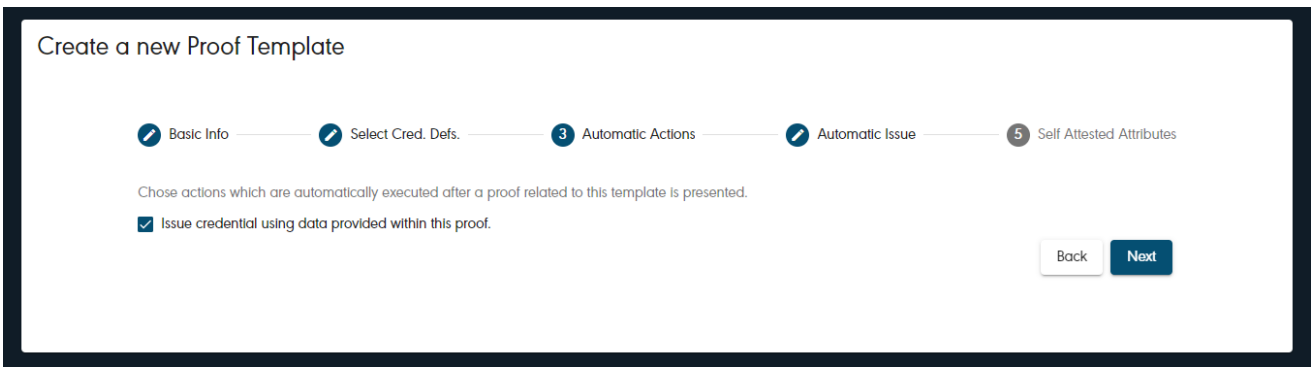
- For the first step the HR employee should enter the name and version of the proof template he would like to create. If the requested format of the input is met the button "**Next**" will be activated and by clicking on it the user will be directed to the next step (Select Cred. Defs).



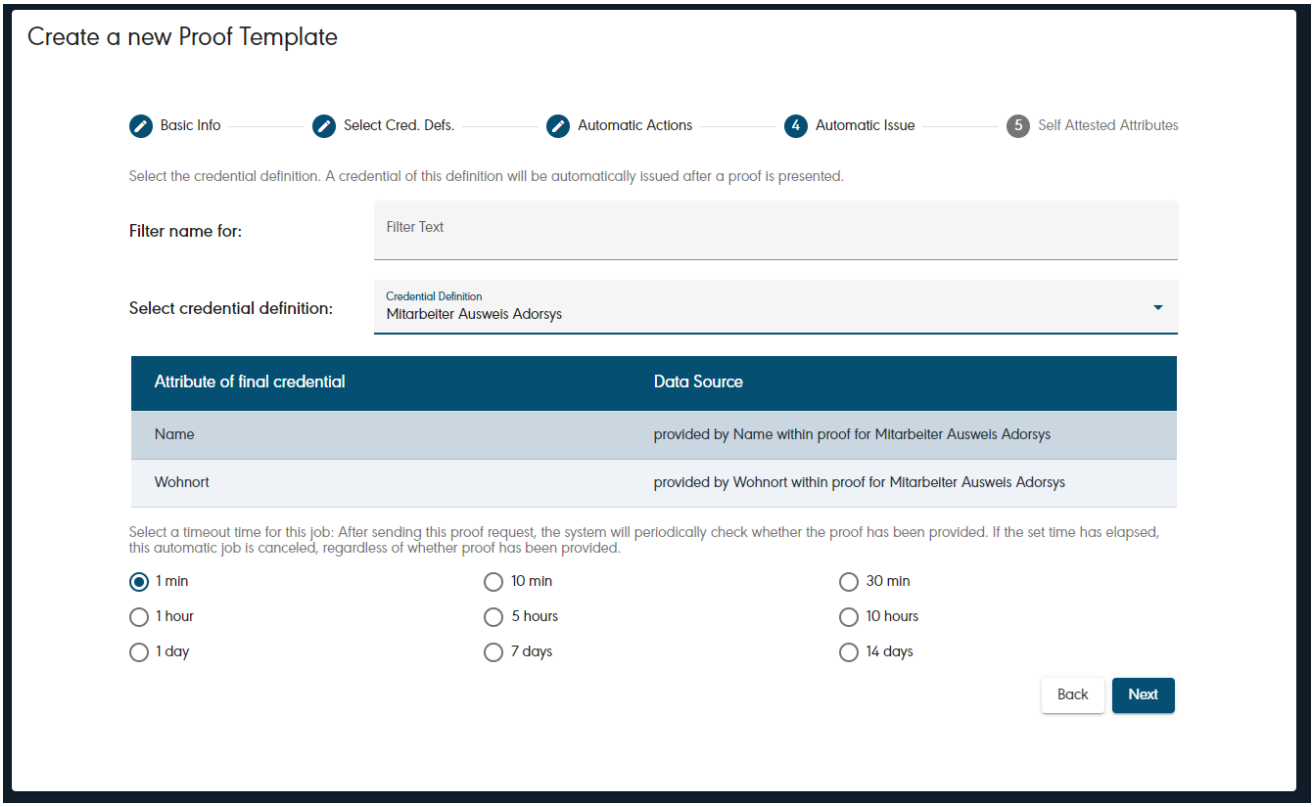
- From the second step it is possible to return to the previous step by clicking on **Back**. In step two it is possible to select the credential definitions needed for the creation of the proof template. To continue with the next step at least one credential definition has to be selected. For each attribute of the schema defined in the credential definition additionally a filter predicate can be applied, e.g. the value has to be greater than 10 (The options for predicates are >, <, >= and <= compared to a value). For accepting the proof later the predicate condition has to be fulfilled.



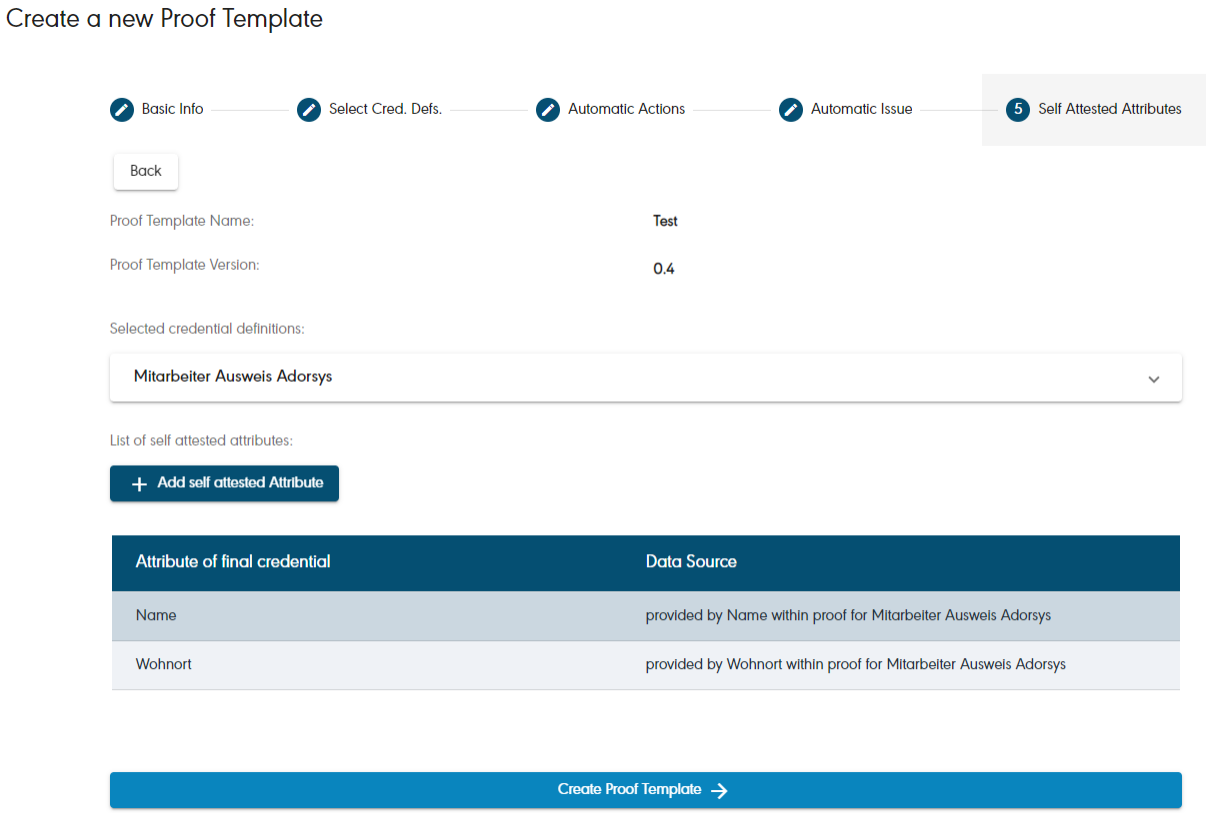
- The third step allows the user to specify an action to be automated. It is possible here to specify to automatically issue the credential from the accepted proof. This will be done after the proof request has been answered in the lissi wallet application. To use this option you must have selected in the previous step exactly one credential definition since this option is not yet possible for more than one credential definition. When the automatic issuance feature is activated, there is an additional step which is added and which is used to configure the credential which will be automatically issued each time the proof is presented.



Activating the checkbox and clicking 'next' leads to a page where the user can select a second credential definition. The second credential will be issued after the proof has been provided by the user. This can be used to provide credentials with attributes filled out by the owner of the digital identity (self-attested attributes). To find the credential definition quicker there is a filter function. After selecting the credential definition the attributes and data sources of all selected credential definitions show up. For each attribute the data comes from the selected credential definition in step 2. Lastly, the user can select a timeout which is initially set to 1 minute. The timeout defines the time the automated issue process of this proof template is provided. After sending this proof request, the system will periodically check whether the proof has been provided. If the time set in the timeout has elapsed, this automatic job is canceled, regardless of whether proof has been provided.



- In the last step we have a general overview over all the data that has been entered for the creation of the proof. Additionally the user has the possibility of adding self-attested attributes. A self-attested attribute is optional and can be added to a job to request more and especially free fillable data from the user of the lissi app. Clicking on the **Create Proof Template** button completes the creation process. Afterwards the proof is created and can be send to a digital identity.



- For a meaningful use of proof templates, the user should have two credential definitions, one created before and one, which is automatically generated on the basis of the lissi app user data. Afterwards, the user should create a proof template, which defines the linking between the credential definitions. Now the user can create a proof request by clicking the button **Send to DI** on the proof templates overview page. The proof request will be sent to the lissi app of the DI and can be sent back with the attributes or declined. The request will automatically expire after the timeout has expired.