SPID Identification via OIDC

IDHub (OAuth Wrapper) Configuration Guide

Step 1: The company who wants to use SPID for identification purpose must be registered at SPID.

Namirial is registered as such. If the Namirial's registration should be used, mind that Namirial must be the local registration authority when issuing disposables based on the SPID identification.

As a result:

- you have credentials for the SPID connection.

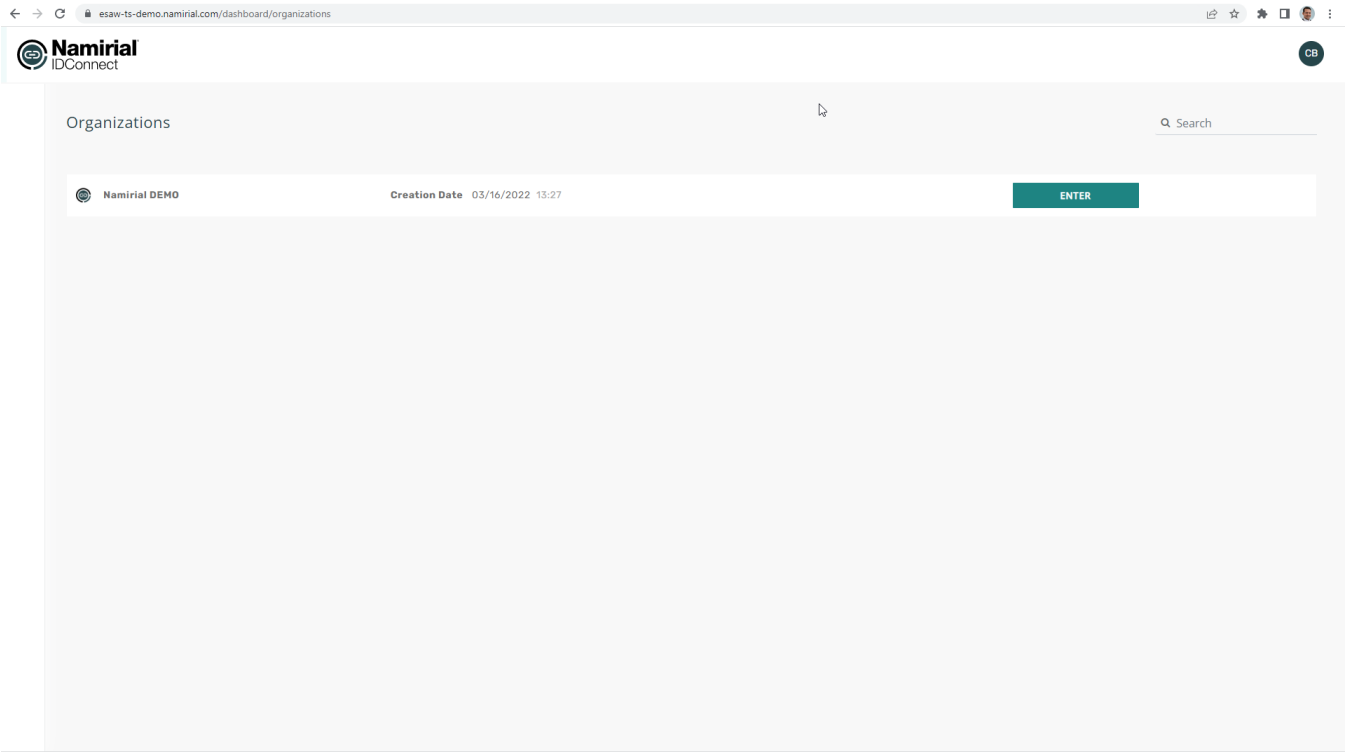
Step 2: configure the IDHub Middleware

This step covers basic configuration for the API connection to SPID in IDHub and registering a new OAuth Application in the IDHub back-end

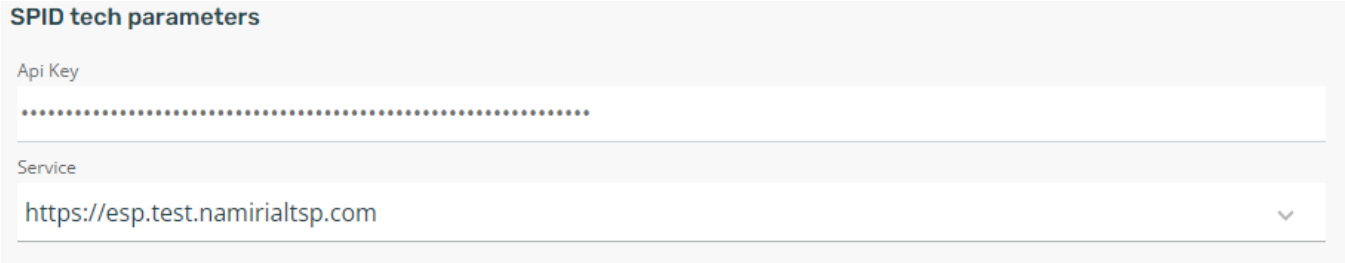
This step is typically performed by Namirial staff.

For preproduction, the configuration is done on https://esaw-ts-demo.namirial.com/

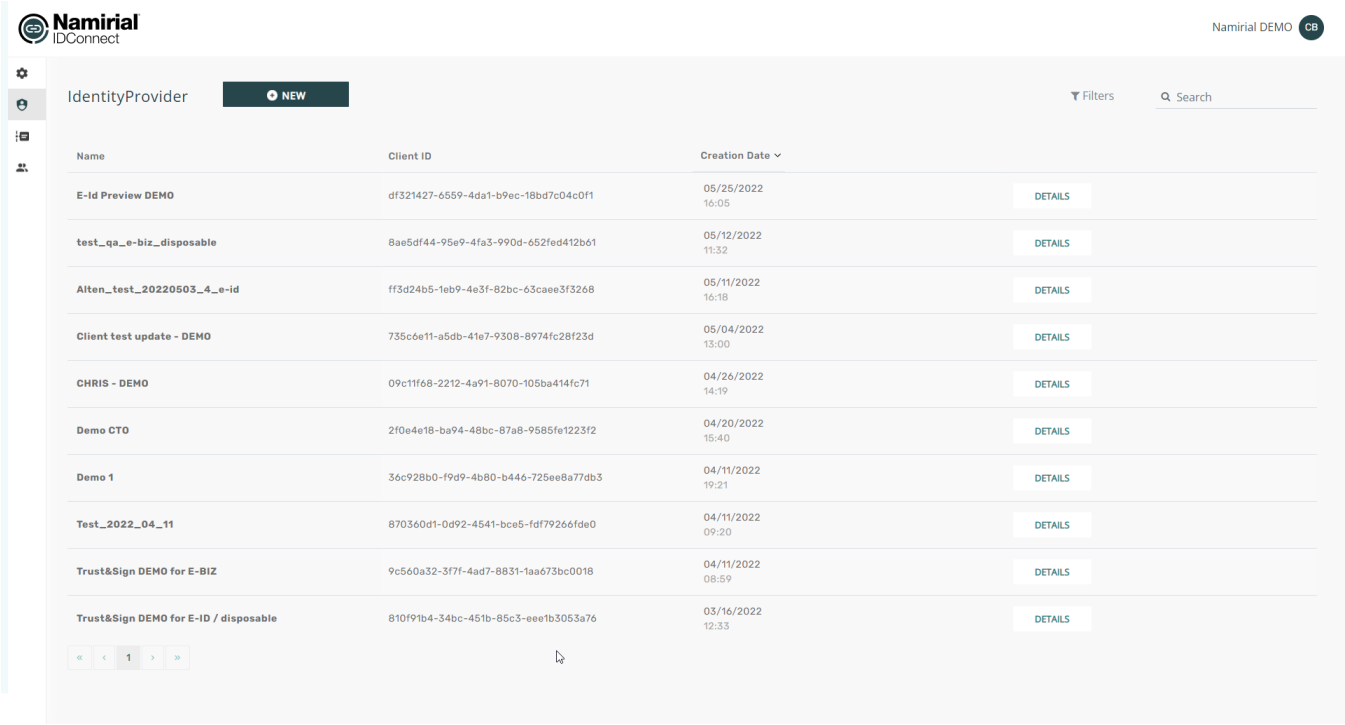
Login: MyNamirial account (but user has to be added to the IDHub backend by an admin first)



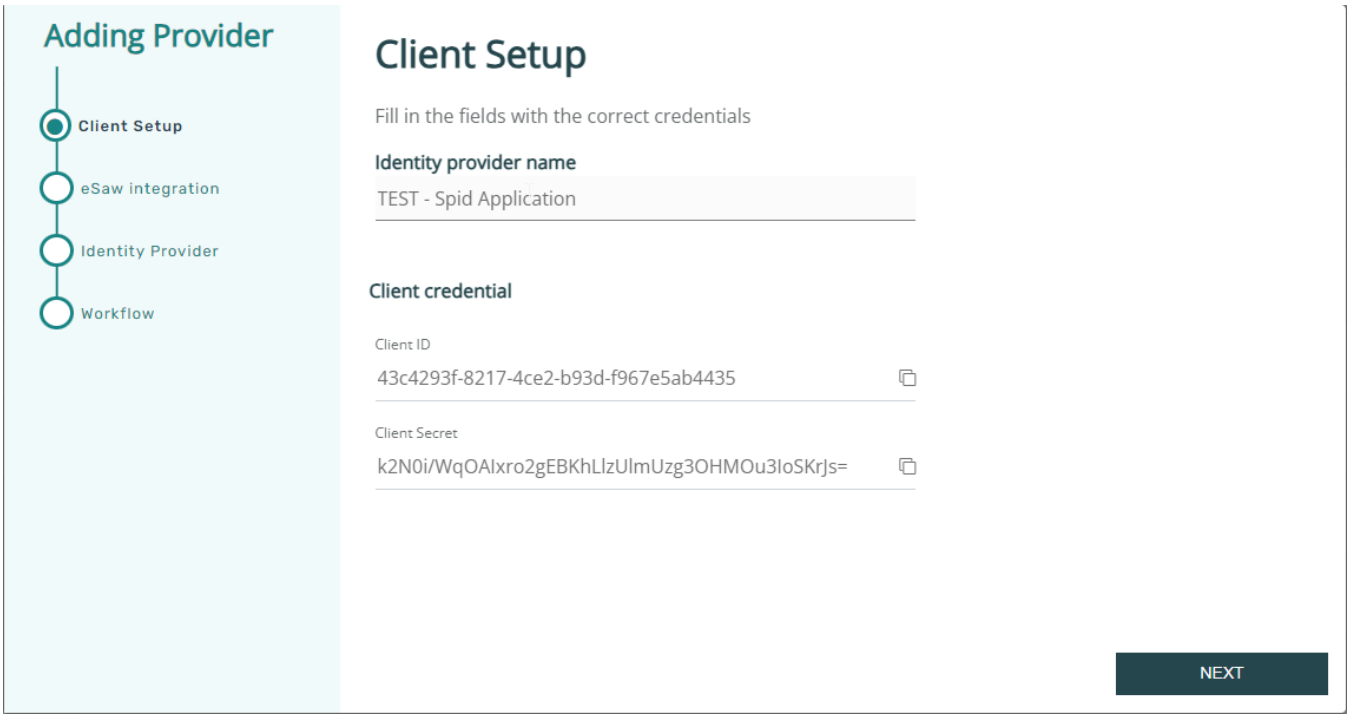
If it's a newly created organization, fill necessary connection data to connect from IDHub to SPID. For the DEMO spid environment e.g.:



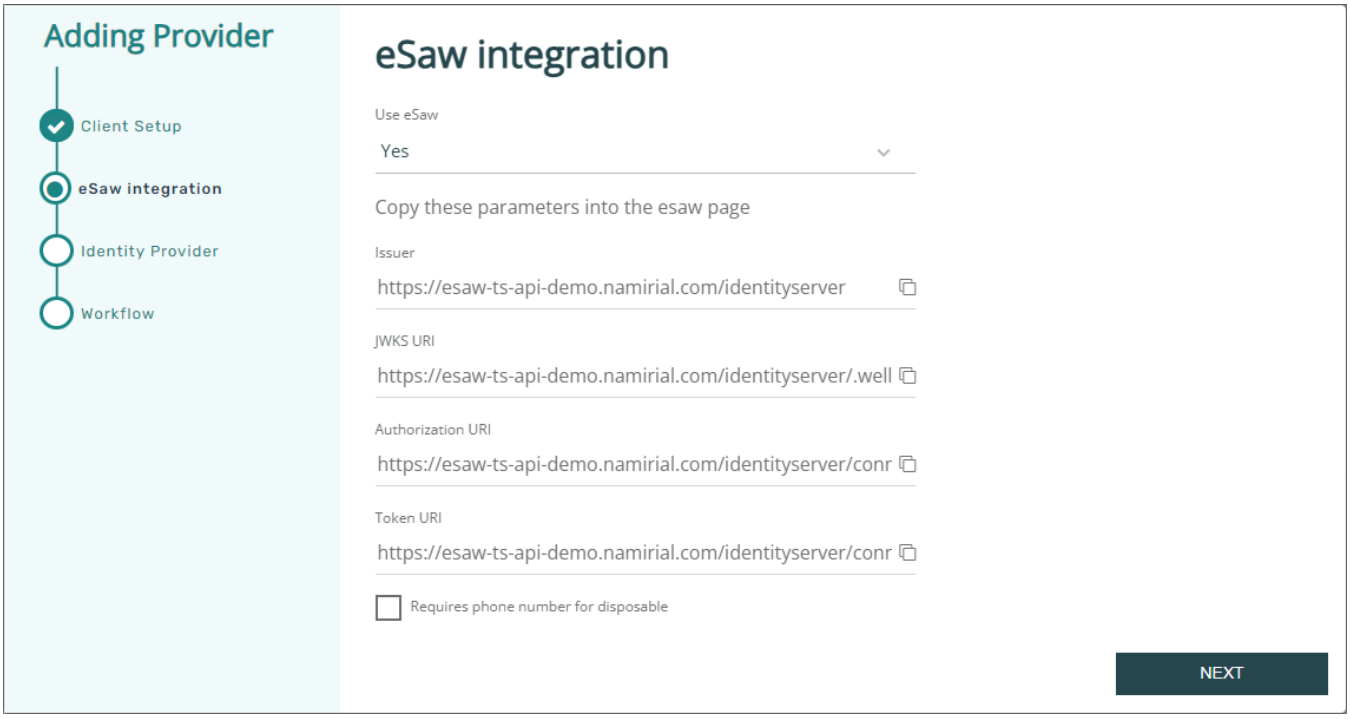
Go to "Identity Providers" and configure your new identity provider for the specific business case.
The identity provider is the specific configuration which eSignAnyWhere later uses, and which knows by configuration which workflow of SPID to be used.



Create a new identity provider:



note down or copy the client id and client secret to your eSAW configuration!

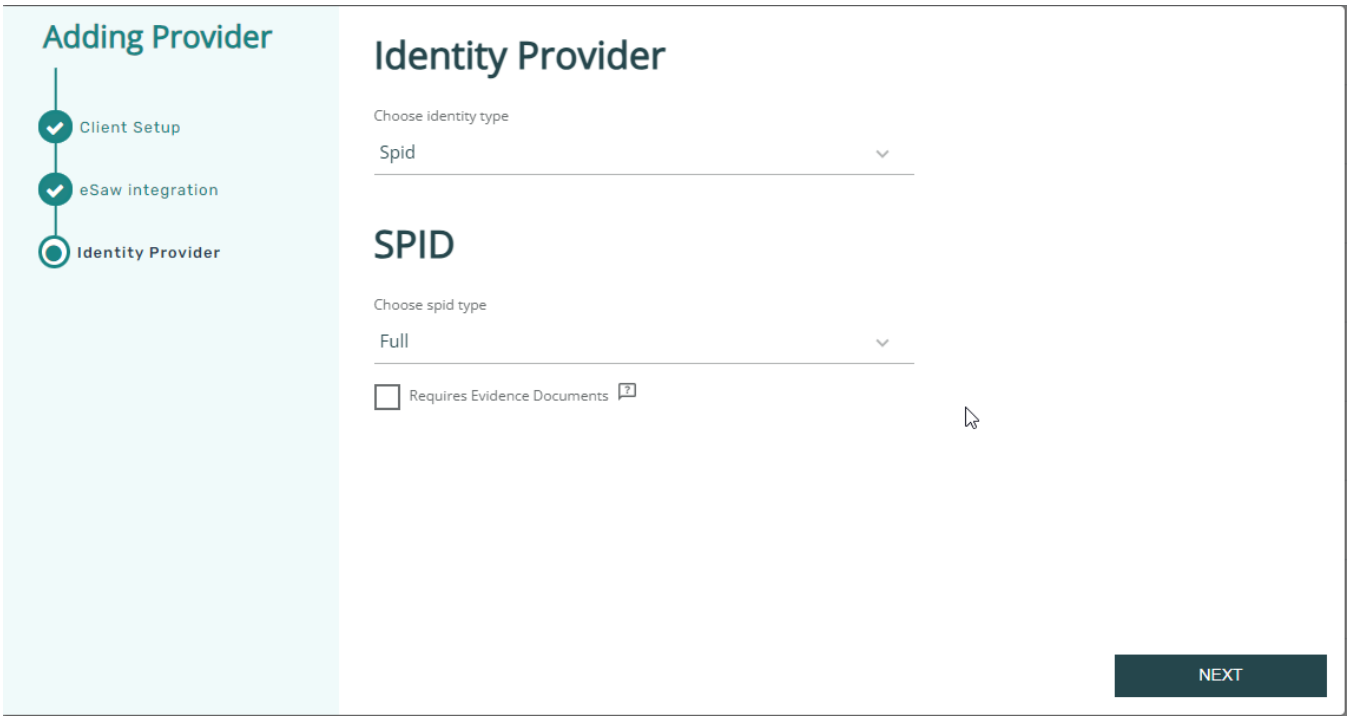


Define that eSignAnyWhere is used. This allows the integration to access data provided by eSignAnyWhere already.

copy these urls, you will need it in your eSAW configuration.

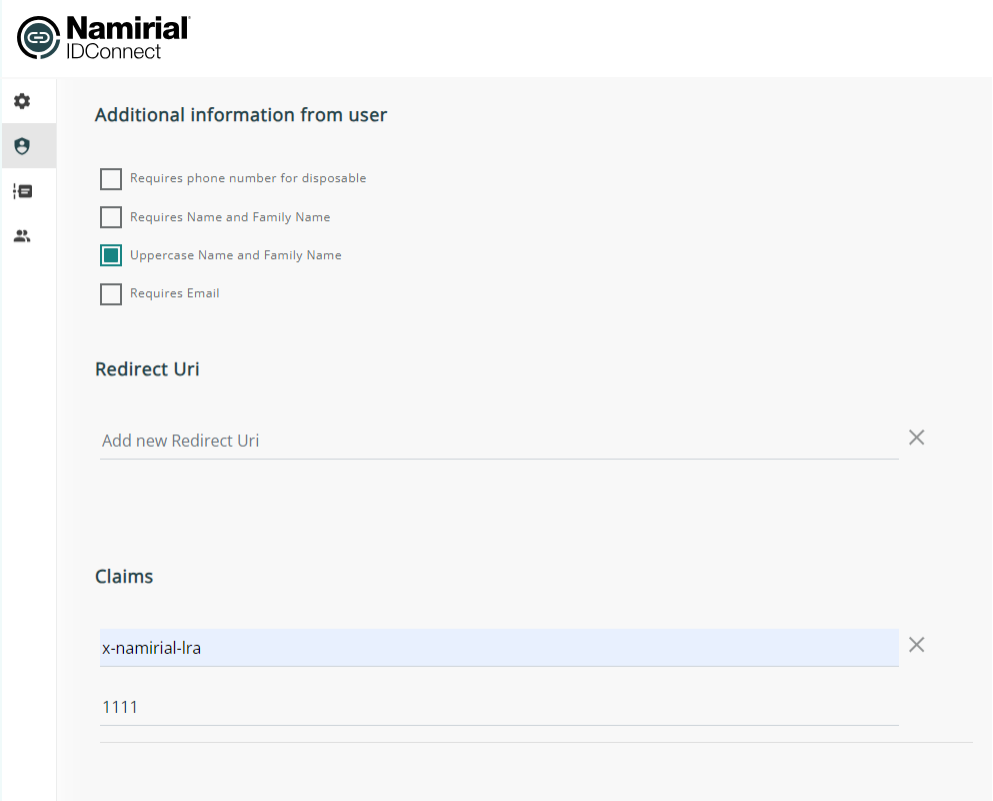
Note that SPID has 2 kind of profiles: SPID FULL and SPID BASE. When using SPID BASE (can be selected on next page), the SPID does not provide a phone number.
When the signer's phone number should not be provided by the sender (in Disposable Certificate Data), but the signer should be asked to enter the phone number himself, select the checkbox "Request phone number for disposable".

In the next page, select Spid as identity type, and choose if the Spid Full or the Spid Base profile should be obtained from Spid.



Complete the wizard and save the just created Identity Provider.

After completing the wizard, define some properties and provide additional static values which the integration needs. This can be e.g. an information of a specific LRA handling to be used:



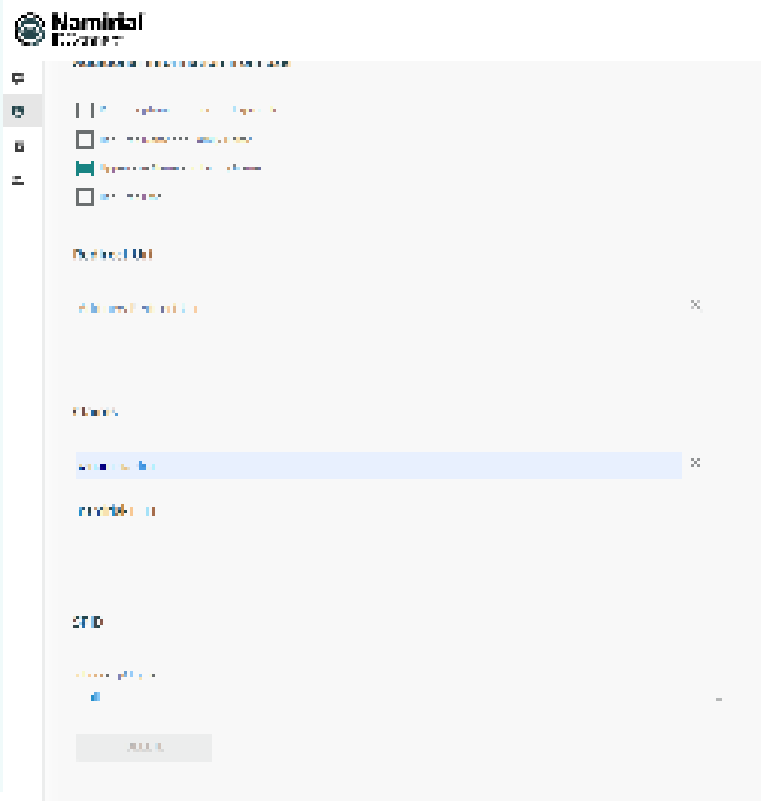
For Spid, ensure to define in the provider also a static claim with a value indicating that the LRA overwriting has to be used.

recommended configuration:

claim name: x-namirial-lra-handing

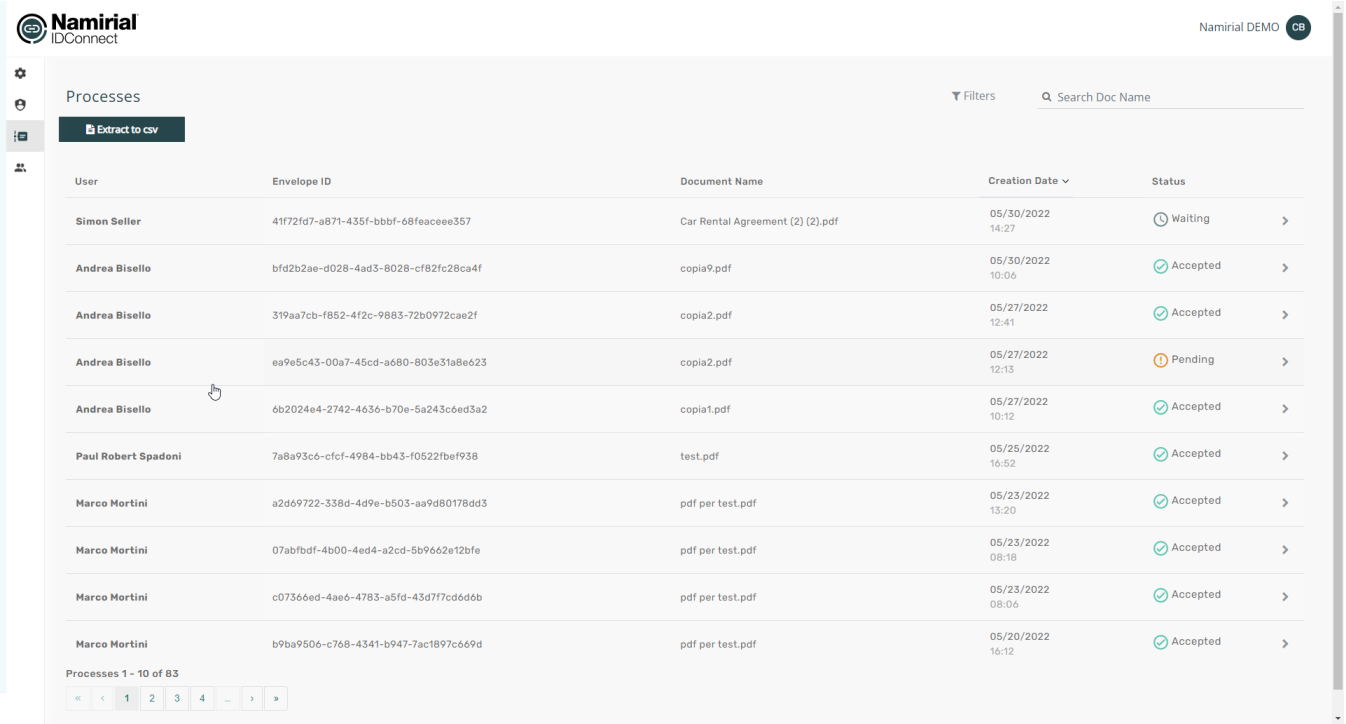
value: namirial-<LRA-Number>

(a specific LRA number will be necessary, even if in any case Namirial will be the LRA, because it will require "technical LRAs" per customer to distinguish and invoice correctly the disposable certificates)



Finally, press the save button.

In the processes tab, you see ongoing and completed identification processes (i.e. instances of identification).



Step 3: Configure eSignAnyWhere Identity Provider Configuration

The IDHub Identity Provider middleware is hosted by Namirial SpA.

Prototype version **hostet by Namirial SpA,** is working with DEMO environment, therefore on the prototype following redirect URI is configured: https://demo.esignanywhere.net/SawViewer/HttpHandlers/AuthHandler.ashx

Example of a Mapping updates the disposable certificate data and verifies the holder name:

Parameter		Value	Field Mapping Configuration			Comment
			Field Property Path	Mode	Data Field	
Provider Name		e.g. "SPID"				Will be shown in eSAW to select the authentication/identification method, and will be shown to the signer in authentication method selection.
Client Id		(use the client ID created in step 2. It should have been provided by Namirial sales or presales team)				
Client Secret		(use the client secret created in step 2. It should have been provided by Namirial sales or presales team)				
Scope		openid profile email spid				
Authorization URI		https://esaw-ts-api-demo.namirial.com/identityserver/connect/authorize				
Token URI		https://esaw-ts-api-demo.namirial.com/identityserver/connect/token				
Logout URI						
JSON Web Token (JWT) Configuration						
	JWKS URI	https://esaw-ts-api-demo.namirial.com/identityserver/.well-known/openid-configuration/jwks				
	Issuer	https://esaw-ts-api-demo.namirial.com/identityserver				
	Add 'nonce' parameter	Off				
	Validate audience	On				
	Validate issuer	On				
	Validate lifetime	On				
	Field Mapping		given_name	Validate	Recipient First Name	Note that this is a validation rule to ensure that the signer is the one which the sender defined. The typing of the name defined by the sender has to be IDENTICAL to the name returned by SPID. In IDHub, you can also define that you always get UPPERCASE names.
	Field Mapping		family_name	Validate	Recipient Last Name	Note that this is a validation rule to ensure that the signer is the one which the sender defined. The typing of the name defined by the sender has to be IDENTICAL to the name returned by SPID. In IDHub, you can also define that you always get UPPERCASE names.

	Field Mapping		identification_type	Update	Disposable Certificate Identification Type	
	Field Mapping		document_type	Update	Disposable Certificate Document Type	
	Field Mapping		identification_number	Update	Disposable Certificate Identification Number	
	Field mapping		phone_number	Update	Disposable Certificate Phone Number	
	Field Mapping		issuing_country	Update	Disposable Certificate Document Issuing Country	
	Field Mapping		issued_by	Update	Disposable Certificate Issued By	
	Field Mapping		document_number	Update	Disposable Certificate Document Number	
	Field Mapping		identification_country	Update	Disposable Certificate Identification Country	
	Field Mapping		issued_on	Update	Disposable Certificate Document issued On	
	Field Mapping		expiry_date	Update	Disposable Certificate Document Expiry Date	

Server side configuration on SIGNificant Server Platform

(For On-Premise, this can be done by the customer. For SaaS, it has to be requested at Namirial Cloud Operations Team)

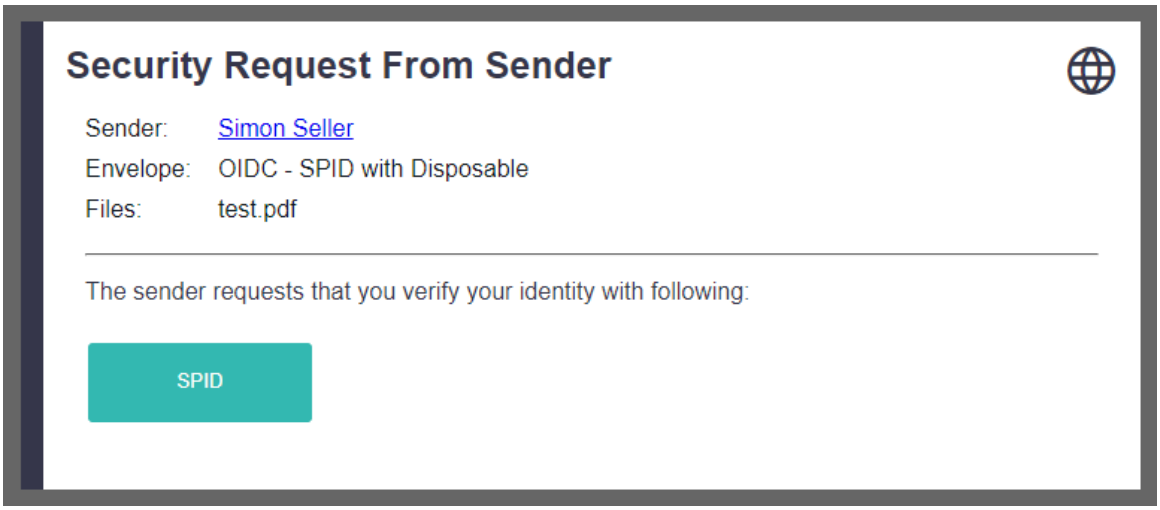
Define, for the specific LRA, the mapping from LRA ID identifier to the full set of "LRA override configuration".
(this is expected to be released in August. Further details will be provided shortly)

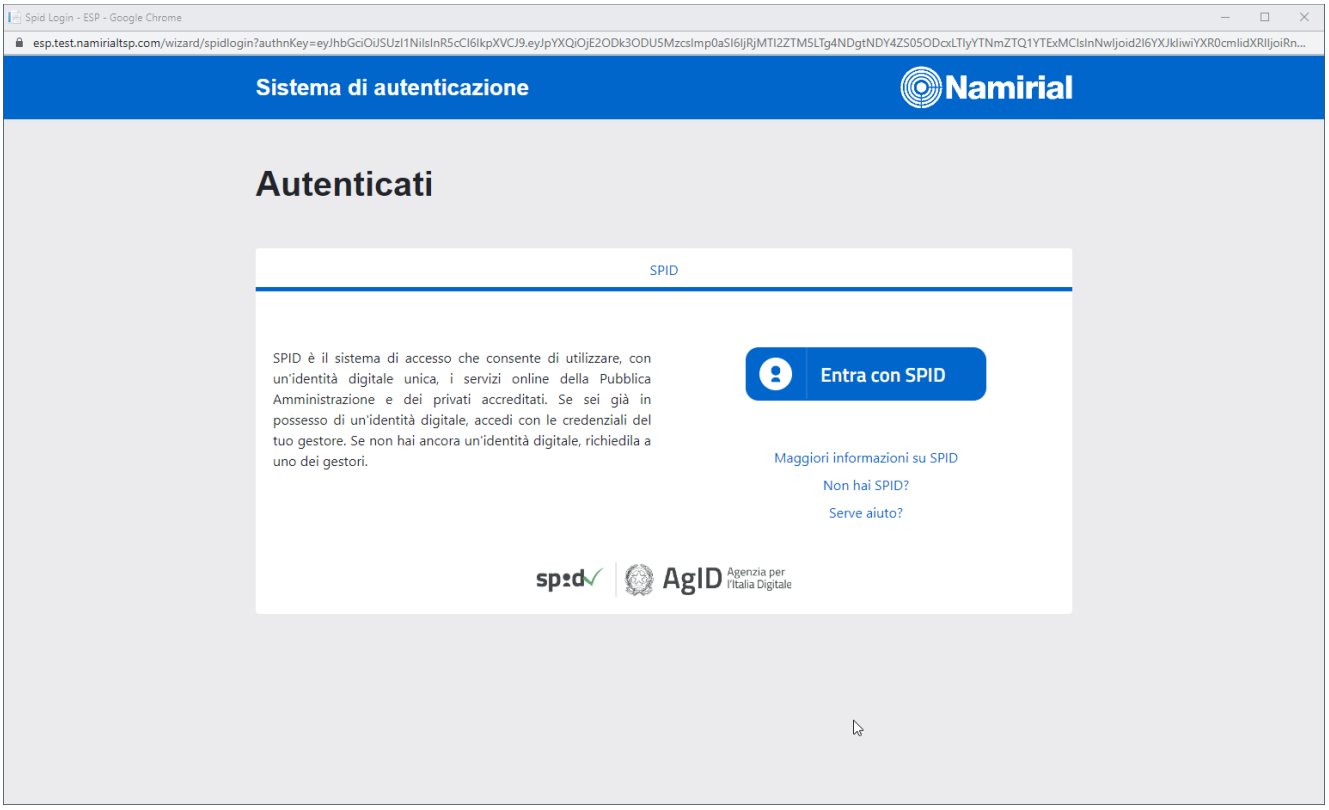
Usage

- Create a new envelope
- Select the document(s) to be signed
- Open the Authentication/Identification section
- Add the OAuth Identification method "SPID"
- If indicated, place in the Designer page a signature field and select the signature method "Disposable Certificate".

Screenshots

> The screenshots below show an example use case of using SPID Full. In this case, the phone number is retrieved from the SPID data, so no phone number input page is shown.


Security Request From Sender
Sender: Simon Seller
Envelope: OIDC - SPID with Disposable
Files: test.pdf
The sender requests that you verify your identity with following:
SPID


Spid Login - ESP - Google Chrome
esp.test.namirialtsp.com/wizard/spidlogin?authnKey=eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE2ODk3ODU5MzcsImp0aSI6IjRjMTI2ZTM5LTg4NDgtNDY4ZS05ODcxLTIyYTNmZTQ1YTExMCIsInNwIjoid2l6YXJkIiwiYXR0cmlidXRlIjoiRn...
Sistema di autenticazione
Namirial
Autenticati
SPID
SPID è il sistema di accesso che consente di utilizzare, con un'identità digitale unica, i servizi online della Pubblica Amministrazione e dei privati accreditati. Se sei già in possesso di un'identità digitale, accedi con le credenziali del tuo gestore. Se non hai ancora un'identità digitale, richiedila a uno dei gestori.
Entra con SPID
Maggiori informazioni su SPID
Non hai SPID?
Serve aiuto?
spid
AgID Agenzia per l'Italia Digitale

Sign in to spid - Google Chrome

spid.test.namirial.it/realms/spid/login-actions/authenticate?client_id=https%3A%2F%2Fesp.test.namirialtsp.com%2Fwizard&tab_id=BMiZtIl7Fp8

Namirial spid

English ▼

SPID request access da
https://esp.test.namirialtsp.com/wizard

Username

BMMCRS[redacted]

Password

••••••••••••••••••••

☐ Show password

Login by SPID

Cancel

Remaining time for authentication: 04:13 minutes

spid AgID Agenzia per l'Italia Digitale

Sign in to spid - Google Chrome

spid.test.namirial.it/realms/spid/login-actions/authenticate?execution=c0a471c5-f6d8-4899-9eed-3ad65912895e&client_id=https%3A%2F%2Fesp.test.namirialtsp.com%2Fwizard&tab_id=BMiZtIl7Fp8

Namirial spid

English ▼

SPID request access da
https://esp.test.namirialtsp.com/wizard

To log in with level 2 security, you need to enter the temporary OTP code. Request the sending of the OTP code via Namirial OTP App

Namirial OTP App | ID: 1462365

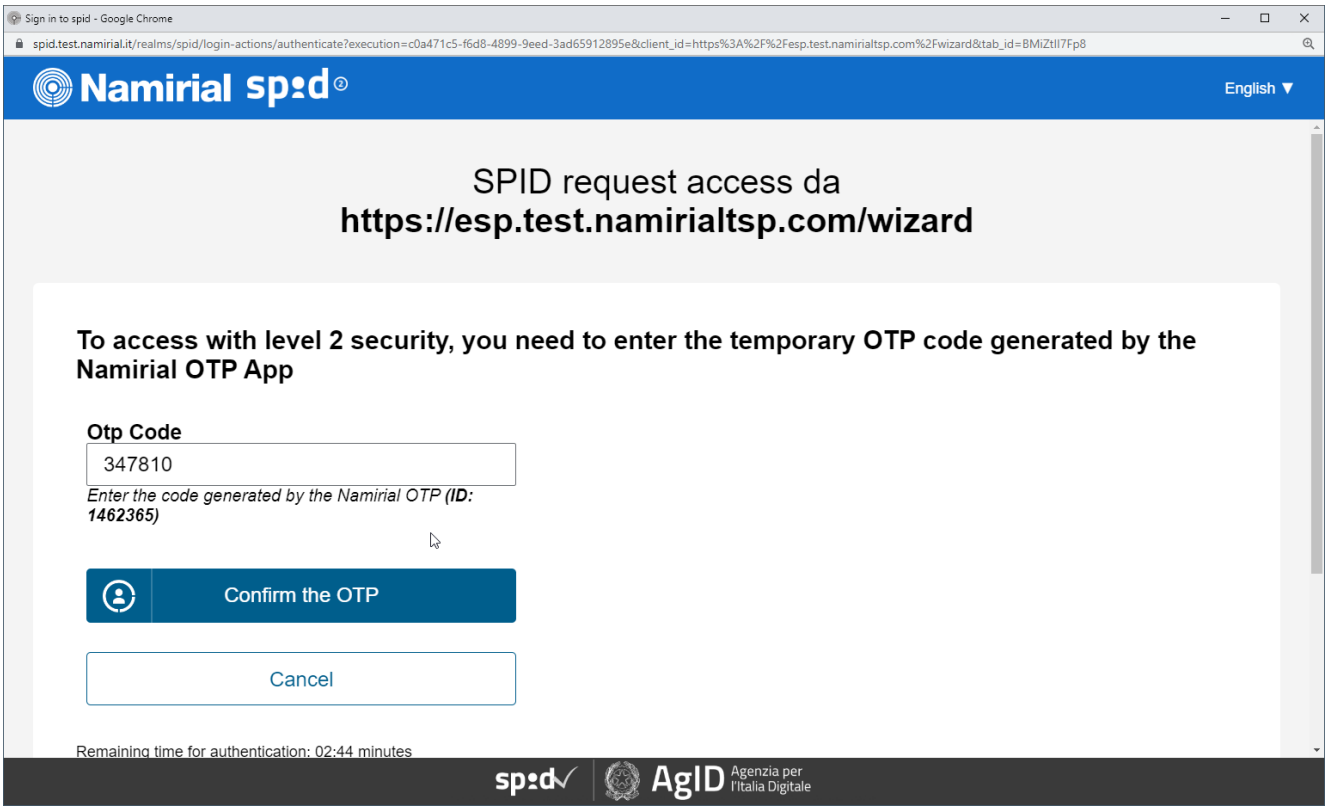
Cancel

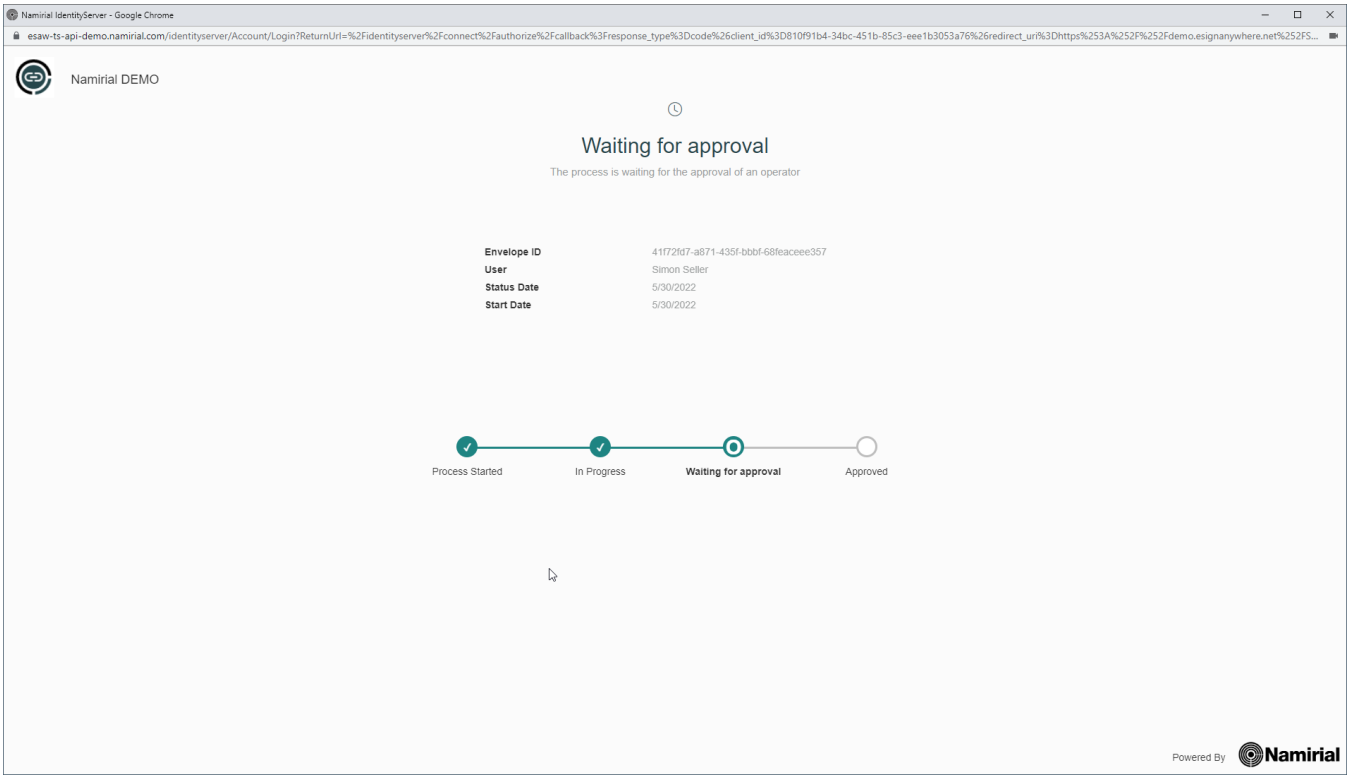
Remaining time for authentication: 03:11 minutes

Do you want to add a new OTP generator?

If you want to set up a new OTP generator, click here

spid AgID Agenzia per l'Italia Digitale


Sign in to spid - Google Chrome
spid.test.namirial.it/realms/spid/login-actions/authenticate?execution=c0a471c5-f6d8-4899-9eed-3ad65912895e&client_id=https%3A%2F%2Fesp.test.namirialtsp.com%2Fwizard&tab_id=BMiZtIl7Fp8
Namirial spid
English
SPID request access da
https://esp.test.namirialtsp.com/wizard
To access with level 2 security, you need to enter the temporary OTP code generated by the Namirial OTP App
Otp Code
347810
Enter the code generated by the Namirial OTP (ID: 1462365)
Confirm the OTP
Cancel
Remaining time for authentication: 02:44 minutes
spid
AgID Agenzia per l'Italia Digitale


Namirial IdentityServer - Google Chrome
esaw-ts-api-demo.namirial.com/identityserver/Account/Login?ReturnUrl=%2Fidentityserver%2Fconnect%2Fauthorize%2Fcallback%3Fresponse_type%3Dcode%26client_id%3D810f91b4-34bc-451b-85c3-eee1b3053a76%26redirect_uri%3Dhttps%253A%252F%252Fdemo.esignanywhere.net%252FS...
Namirial DEMO
Waiting for approval
The process is waiting for the approval of an operator
Envelope ID 41f72fd7-a871-435f-bbbf-68feaceee357
User Simon Seller
Status Date 5/30/2022
Start Date 5/30/2022
Process Started
In Progress
Waiting for approval
Approved
Powered By Namirial