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.
 - Step 2: configure the IDHub Middleware
 - Step 3: Configure eSignAnyWhere Identity Provider Configuration
 - The IDHub Identity Provider middleware is hosted by Namirial SpA.
- Server side configuration on SIGNificant Server Platform
- Usage
- Screenshots

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)

\leftrightarrow \rightarrow	C esaw-ts-demo.namirial.com/dashboard/organizations			🖻 🖈 🖬 🌘 🗄				
0	Namirial DConnect							
	Organizations		¢	Q Search				
	Namirial DEMO	Creation Date 03/16/2022 13:27	ENTER					

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

SPID tech parameters

Api Key	
Service	
https://esp.test.namirialtsp.com	~

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.

© [Namirial Donnect Namirial DEMO						
¢ 0	IdentityProvider • NEW			▼ Filters Q Search			
10 	Name	Client ID	Creation Date V				
	E-Id Preview DEMO	df321427-6559-4da1-b9ec-18bd7c04c0f1	05/25/2022 16:05	DETAILS			
	test_qa_e-biz_disposable	8ae5df44-95e9-4fa3-990d-652fed412b61	05/12/2022 11:32	DETAILS			
	Alten_test_20220503_4_e-id	ff3d24b5-1eb9-4e3f-82bc-63caee3f3268	05/11/2022 16:18	DETAILS			
	Client test update - DEMO	735c6e11-a5db-41e7-9308-8974fc28f23d	05/04/2022 13:00	DETAILS			
	CHRIS - DEMO	09c11f68-2212-4a91-8070-105ba414fc71	04/26/2022 14:19	DETAILS			
	Demo CTO	2f0e4e18-ba94-48bc-87a8-9585fe1223f2	04/20/2022 15:40	DETAILS			
	Demo 1	36c928b0-f9d9-4b80-b446-725ee8a77db3	04/11/2022 19:21	DETAILS			
	Test_2022_04_11	870360d1-0d92-4541-bce5-fdf79266fde0	04/11/2022 09:20	DETAILS			
	Trust&Sign DEMO for E-BIZ	9c560a32-3f7f-4ad7-8831-1aa673bc0018	04/11/2022 08:59	DETAILS			
	Trust&Sign DEMO for E-ID / disposable	810f91b4-34bc-451b-85c3-eee1b3053a76	03/16/2022 12:33	DETAILS			
	« < 1 > »	La					

Create a new identity provider:

Adding Provider	Client Setup	
Client Setup	Fill in the fields with the correct credentials	
I	Identity provider name	
eSaw integration	TEST - Spid Application	
Identity Provider		
Workflow	Client credential	
C	Client ID	
	43c4293f-8217-4ce2-b93d-f967e5ab4435	
	Client Secret	
	k2N0i/WqOAlxro2gEBKhLlzUlmUzg3OHMOu3loSKrJs=	6
		NEXT

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

Adding Provider	eSaw integration
Client Setup	Use eSaw Yes v
eSaw integration	Copy these parameters into the esaw page
Identity Provider	lssuer
Workflow	
	https://esaw-ts-api-demo.namirial.com/identityserver/.well 🗇
	Authorization URI
	https://esaw-ts-api-demo.namirial.com/identityserver/conr 🗋
	Token URI
	https://esaw-ts-api-demo.namirial.com/identityserver/conr 🗋
	Requires phone number for disposable
	NEXT

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.

Adding Provider	Identity Provider		
Client Setup	Choose identity type Spid	~	
Identity Provider	SPID		
	Choose spid type Full	~	
	Requires Evidence Documents 📝	ß	
			NEXT

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:

	Namirial DConnect	
٠	Additional information from user	
•	Requires phone number for disposable Requires Name and Family Name Uppercase Name and Family Name Requires Email	
	Redirect Uri	×
	Claims	
	x-namirial-Ira	×
	1111	

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-Ira-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)

le Namirial Const							
ę.							
0	I Providence of the second sec						
	and the second s						
	New York Control of the Street Street						
-							
	Perfect Out						
	Allows Patrick Co	×,					
	Charles .						
	and a first the	×					
	rudik u						
	STID						
	store play a	_					
	-	_					
	ALL 1.						

Finally, press the save button.

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

©	Namirial Namirial DEMO						
¢ 0	Processes		т	▼ Filters Q Search Doc Name			
ła	Extract to csv						
*	User	Envelope ID	Document Name	Creation Date 🗸	Status		
	Simon Seller	41f72fd7-a871-435f-bbbf-68feaceee357	Car Rental Agreement (2) (2).pdf	05/30/2022 14:27	(Waiting	>	
	Andrea Bisello	bfd2b2ae-d028-4ad3-8028-cf82fc28ca4f	copia9.pdf	05/30/2022 10:06	Accepted	>	
	Andrea Bisello	319aa7cb-f852-4f2c-9883-72b0972cae2f	copia2.pdf	05/27/2022 12:41	Accepted	>	
	Andrea Bisello	ea9e5c43-00a7-45cd-a680-803e31a8e623	copia2.pdf	05/27/2022 12:13	Pending	>	
	الس Andrea Bisello	6b2024e4-2742-4636-b70e-5a243c6ed3a2	copia1.pdf	05/27/2022 10:12	Accepted	>	
	Paul Robert Spadoni	7a8a93c6-cfcf-4984-bb43-f0522fbef938	test.pdf	05/25/2022 16:52	Accepted	>	
	Marco Mortini	a2d69722-338d-4d9e-b503-aa9d80178dd3	pdf per test.pdf	05/23/2022 13:20	Accepted	>	
	Marco Mortini	07abfbdf-4b00-4ed4-a2cd-5b9662e12bfe	pdf per test.pdf	05/23/2022 08:18	Accepted	>	
	Marco Mortini	c07366ed-4ae6-4783-a5fd-43d7f7cd6d6b	pdf per test.pdf	05/23/2022 08:06	Accepted	>	
	Marco Mortini	b9ba9506-c768-4341-b947-7ac1897c669d	pdf per test.pdf	05/20/2022 16:12	⊘ Accepted	>	
	Processes 1 - 10 of 83						
	≪ < 1 2 3 4 →	3					

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://demous.net/SawViewer/HttpHandlers/AuthHandler.ashx

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

P	arameter	Value	Field Mapping Configuration		uration	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.
Cli	ent Id	(use the client ID created in step 2. It should have been provided by Namirial sales or presales team)				
Cli	ent Secret	(use the client secret created in step 2. It should have been provided by Namirial sales or presales team)				
Sc	оре	openid profile email spid				
Au UR	thorization	https://esaw-ts-api-demo.namirial.com /identityserver/connect/authorize				
То	ken URI	https://esaw-ts-api-demo.namirial.com /identityserver/connect/token				
Lo	gout URI					
JS To Co	ON Web ken (JWT) nfiguration					
	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.
						וו סטוידעו, 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 Up _type	Ipdate Disposable Certificate Identification Type
Field Mapping	document_t Up ype	Ipdate Disposable Certificate Document Type
Field Mapping	identification Up _number	Jpdate Disposable Certificate Identification Number
Field mapping	phone_num Up ber	Jpdate Disposable Certificate Phone Number
Field Mapping	issuing_cou Up ntry	Ipdate Disposable Certificate Document Issuing Country
Field Mapping	issued_by Up	Ipdate Disposable Certificate Issued By
Field Mapping	document_n Up umber	Jpdate Disposable Certificate Document Number
Field Mapping	identification Up _country	Ipdate Disposable Certificate Identification Country
Field Mapping	issued_on Up	Ipdate Disposable Certificate Document issued On
Field Mapping	expiry_date Up	Ipdate 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 (i) phone number input page is shown.

Sender: Sin Envelope: Of Files: tes The sender red	Request From Sender mon <u>Seller</u> DC - SPID with Disposable st.pdf uests that you verify your identity with foll	owing:					
Spid Login - ESP - Google Chrome esp.test.namirialtsp.com/wizard/spidlog	in?authnKey=ey/hbGciOiJSUz11NilsInR5cCl6lkpXVCJ9.ey/pYXQiOjE2ODk3ODU5Mz	csimp0aSi6ijRjMTi2ZTM5LTg4NDgtNDY4ZS05ODcxLTyYTNmZTQ1YTExh	– 🗆 🗙 ACIsInNwijoid2l6YXJkliwiYXR0cmlidXRIIjoiRn				
	Sistema di autenticazione Sistema di autenticazione Sistema di autenticazione						
	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?					
	sp±d√ 🎡 A	gID Agenzia per Ittalia Digitale					
		G					

Sign in to spid - Google Chrome spid.test.namirial.it/realms/spid/login-actions/authenticate?client_id=https%3A	4%2F%2Fesp.test.namirialtsp.com%2Fwizard&tab_id=8MiZtII7Fp8	- L X	
Namirial Sptd S		English ▼	
SPID request access da https://esp.test.namirialtsp.com/wizard			
	BMMCRS	6	
 ٦	Cancel Remaining time for authentication: 04:13 minutes sp:d√	•	
Sign in to spid - Google Chrome		- 🗆 X	
Samirial sped®	сэнойончоээээссанэваарэн сарэсааснен цаннирэлоэнийс ихс езрисерналтанархолнийс ихсанаахаа цаналтийн үр	English ▼	
SPID request access da https://esp.test.namirialtsp.com/wizard			
To log in with level 2 security, you need to OTP App ID: 1462365 Cancel Remaining time for authentication: 03:11 minutes	o enter the temporary OTP code. Request the sending of the OTP code via Namirial		
To log in with level 2 security, you need to OTP App ID: 1462365 Cancel Remaining time for authentication: 03:11 minutes Do you want to add a new OTP If you want to set up a new OTP generator	o enter the temporary OTP code. Request the sending of the OTP code via Namirial generator?		



🚱 Namirial IdentityServer - Google Chrome			- 🗆 X	
esaw-ts-api-demo.namirial.com/identityserver/Account/Login?ReturnUrl=%2Fidentityserver%2Fconnect%	62Fauthorize%2Fcallback%3Fresponse	_type%3Dcode%26client_id%3D810f91b4-34bc-451b-85c3-eee1b3053a76%26redirect_uri%3Dhttps%253A%252F%252Fdemo.esignany	where.net%252FS 🖿	
Namirial DEMO				
		0		
Waiting for approval				
	The process is waitir	ing for the approval of an operator		
	Envelope ID	41f72fd7-a871-435f-bbbf-68feaceee357		
	User Status Date	Simon Seller 5/30/2022		
	Start Date	5/30/2022		
Ø-	⊘	O		
Process Sta	arted In Progress	Waiting for approval Approved		
	ß			
		Powered By	Namirial	