Proof website, domain, and network ownership

1st February 2025

FOSDEM 2025, DNS track

Project "Open Console"

Mark Overmeer

Architect
Developer

Nguyễn Phương **Thảo**

Community
Finances

Arnhem, The Netherlands

Presentation overview

1) OpenWebSearch.EU / OpenSearchFoundation
2) What is "Open Console"?
3) Collecting proofs
    - email ownership
4) Accessing Services
5) Website, Domain, and IP-range ownership

OpenWebSearch.EU

Open WebSearch .eu

- EU NGI funded, 8.5M€, 2022-2026
- https://openwebsearch.eu
- Started by
  The Open Search Foundation
  https://opensearchfoundation.org

osf open search foundation

~15 partners
uni & research:

UP

CERN

Radboud University
Nijmegen, the Netherlands

DLR

UNIVERSITÄT
LEIPZIG

CSC

lrz Leibniz-Rechenze
der Bayerischen Akademie der Wissenschaften

OpenWebSearch.EU

- 4 larger projects, >50 papers
- Smaller grants, like Open Console
- Publication of a crawled data-set, 3B URLs ~ 14TB index

CommonCrawl 2.6B/394TB per 2 months.

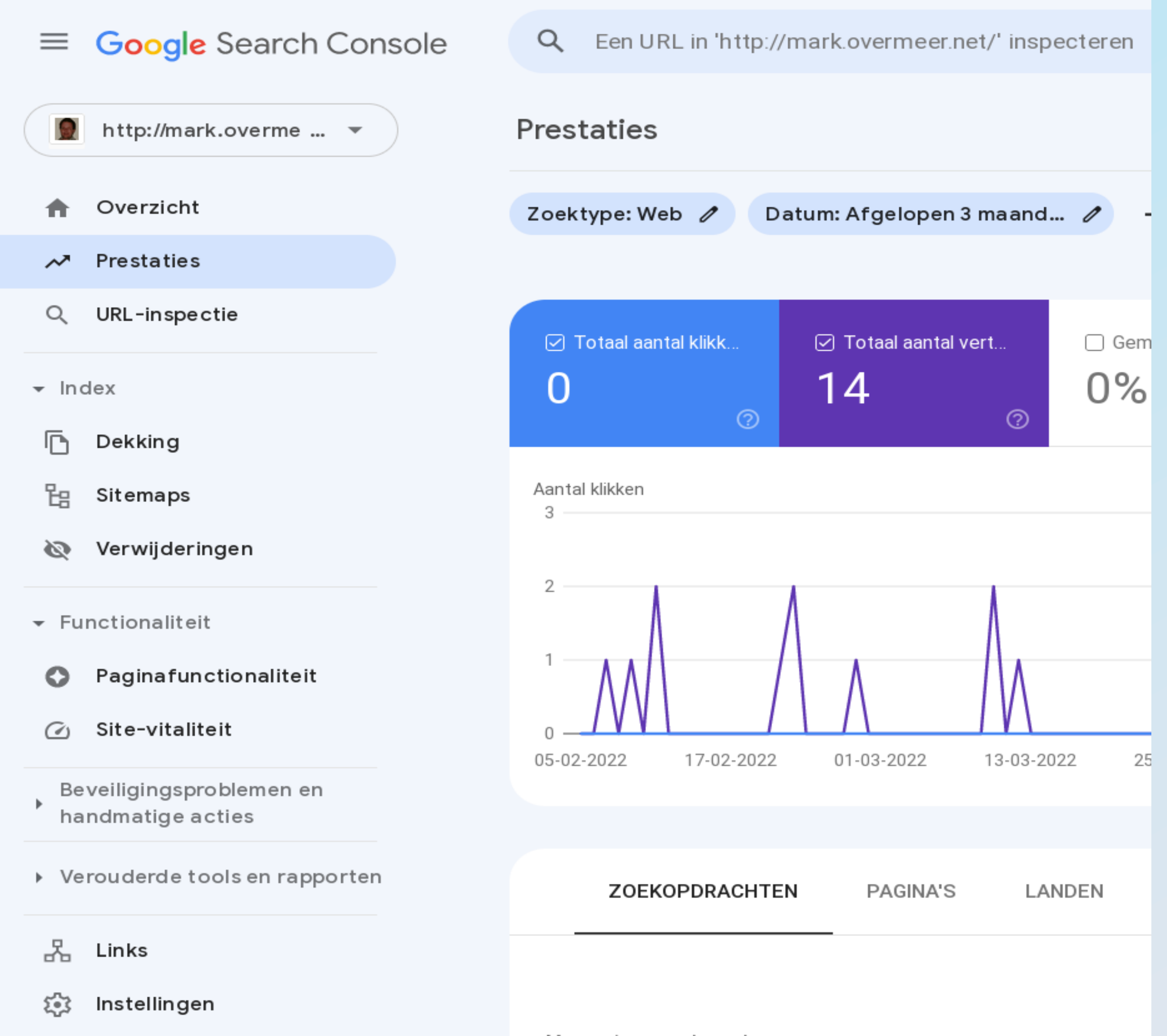
- Many task forces (OSF)
  - applications
  - economy
  - education
  - ethics
  - legal
  - tech
- OSSYM Conferences

@Google

Google Search Console

- Site usage
- Crawl optimization
- Crawl feedback
- Take-downs

Major competitive advantage



Een URL in 'http://mark.overmeer.net/' inspecteren

http://mark.overme ...

Prestaties

Zoektype: Web

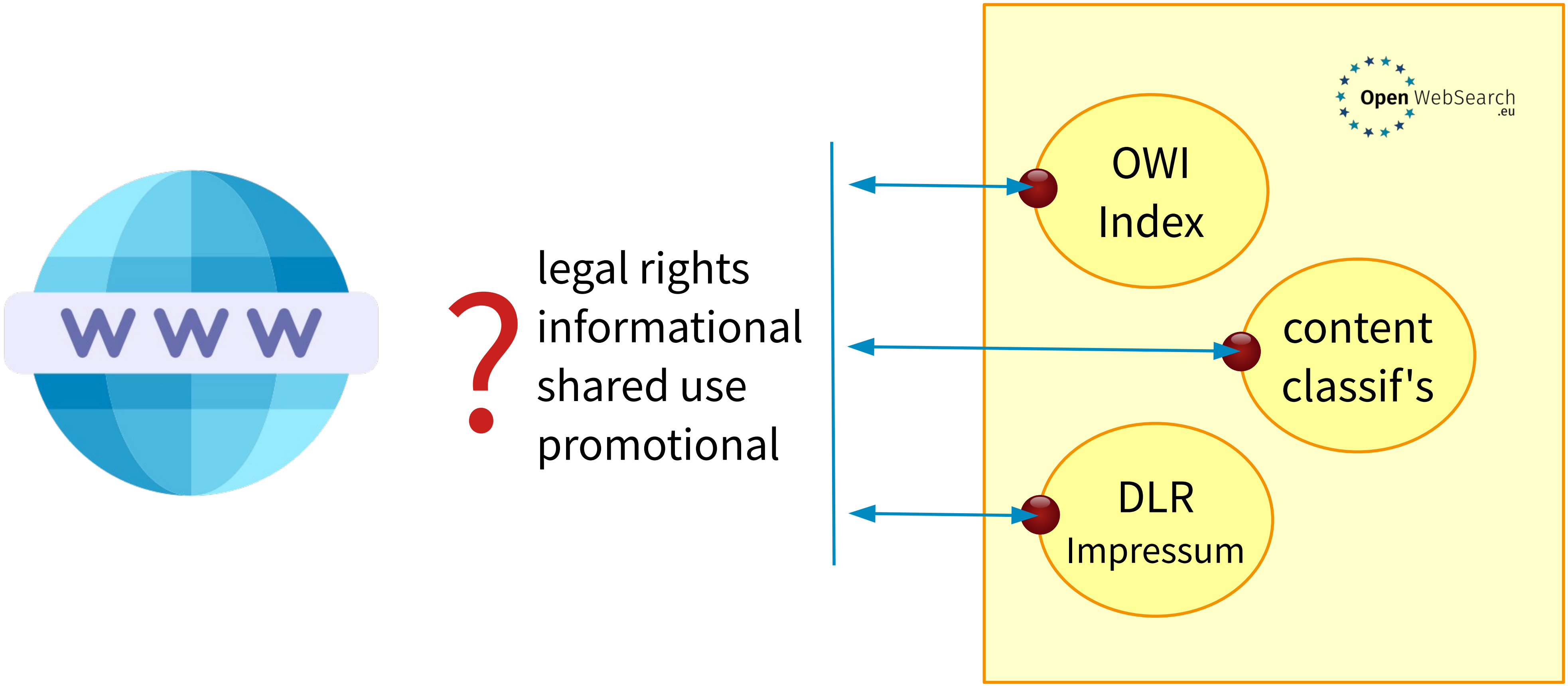
Datum: Afgelopen 3 maand...

☑ Totaal aantal klikk... 0

☑ Totaal aantal vert... 14

□ Gem 0%

Positioning in OWS



?

legal rights
informational
shared use
promotional

Open WebSearch.eu

OWI Index

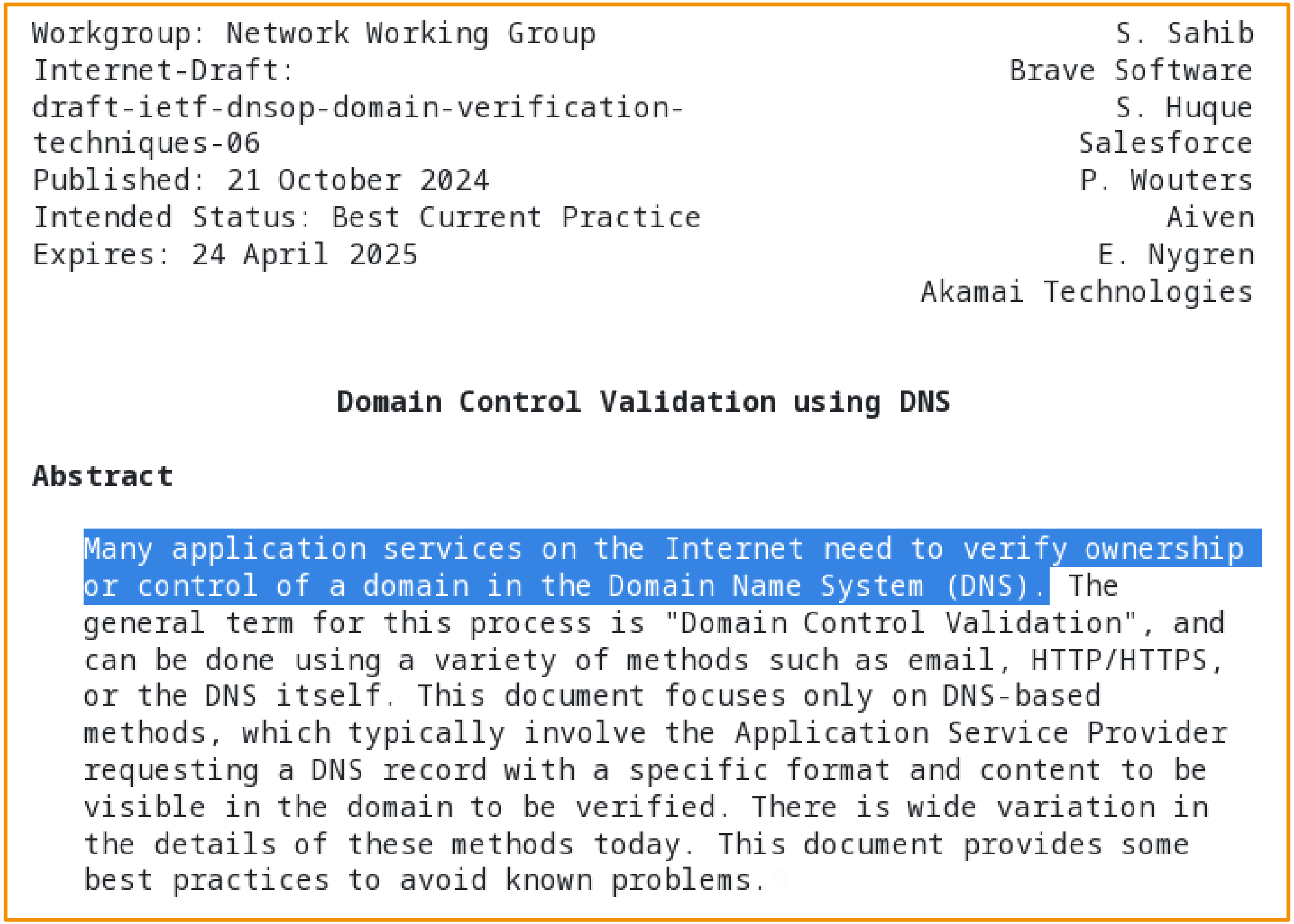
content classif's

DLR Impressum

Domain ownership proof

RFC lists implementations by

- Let's Encrypt
- Google Workspace
- The AT Protocol
- GitHub orga's
- Public Suffix List
- DocuSign
- CDNs
- AWS Certificate Manager
- Atlassian



```
Workgroup: Network Working Group                              S. Sahib
Internet-Draft:                                         Brave Software
draft-ietf-dnsop-domain-verification-                         S. Huque
techniques-06                                               Salesforce
Published: 21 October 2024                                  P. Wouters
Intended Status: Best Current Practice                           Aiven
Expires: 24 April 2025                                       E. Nygren
                                                  Akamai Technologies
```

Domain Control Validation using DNS

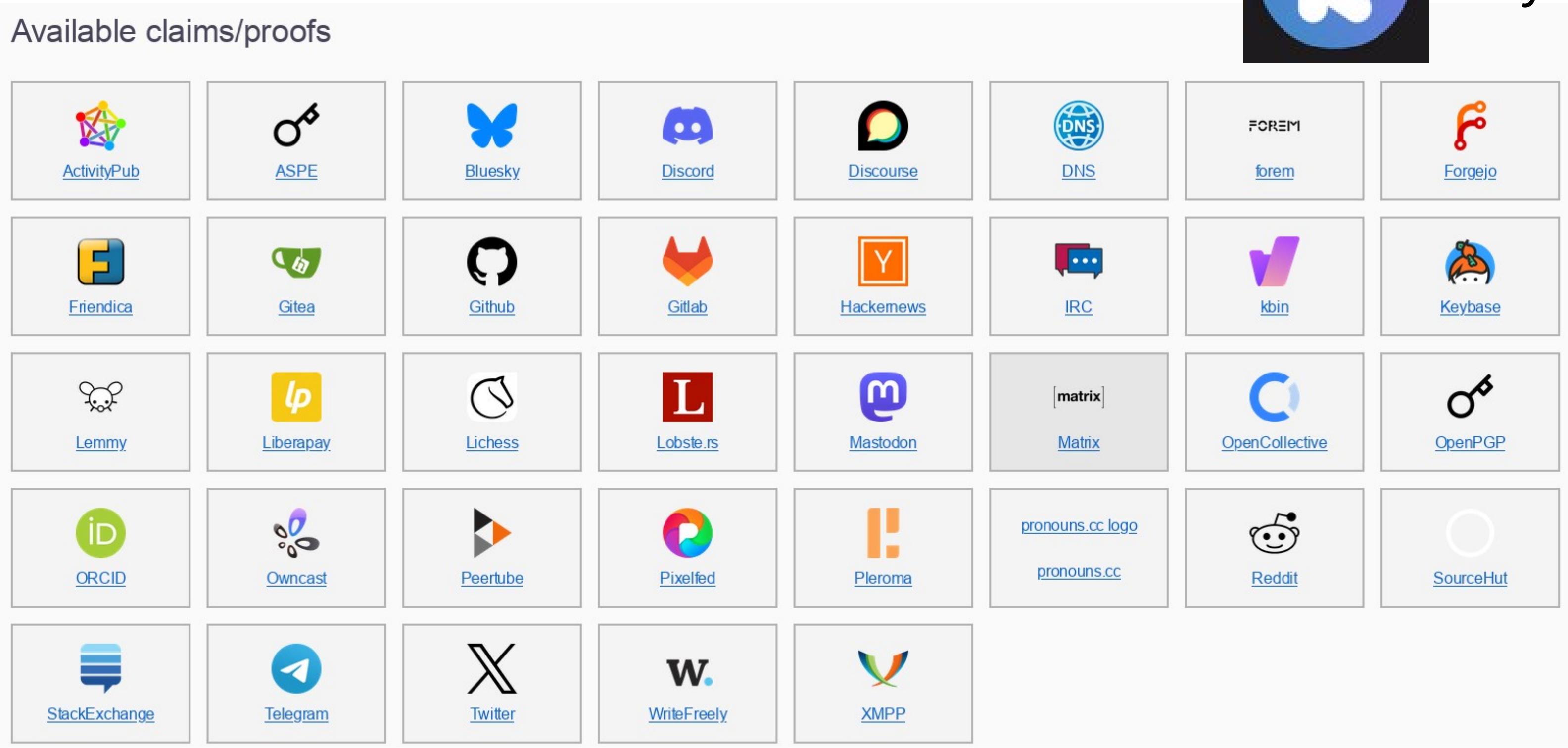
Abstract

Many application services on the Internet need to verify ownership or control of a domain in the Domain Name System (DNS). The general term for this process is "Domain Control Validation", and can be done using a variety of methods such as email, HTTP/HTTPS, or the DNS itself. This document focuses only on DNS-based methods, which typically involve the Application Service Provider requesting a DNS record with a specific format and content to be visible in the domain to be verified. There is wide variation in the details of these methods today. This document provides some best practices to avoid known problems.

Managing

It is not about creating access!

keyoxide.org

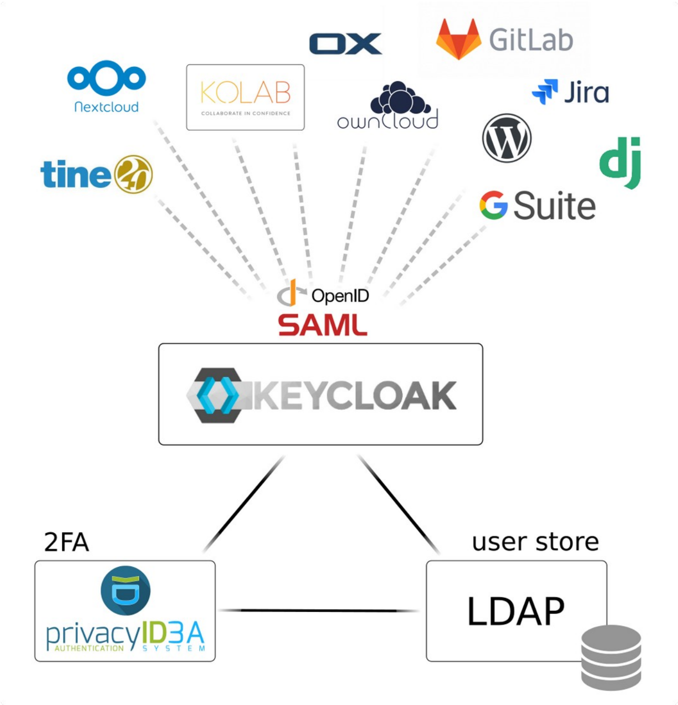


Available claims/proofs

ActivityPub	ASPE	Bluesky	Discord	Discourse	DNS	forem	Forgejo
Friendica	Gitea	Github	Gitlab	Hackernews	IRC	kbin	Keybase
Lemmy	Liberapay	Lichess	Lobste.rs	Mastodon	Matrix	OpenCollective	OpenPGP
ORCID	Owncast	Peertube	Pixelfed	Pleroma	pronouns.cc logo pronouns.cc	Reddit	SourceHut
StackExchange	Telegram	Twitter	WriteFreely	XMPP			

Managing

It is not about your organization



Managing

It is *not* about creating access

It is *not* about your organization

It's a fight against fragmentation

from *your* personal perspective

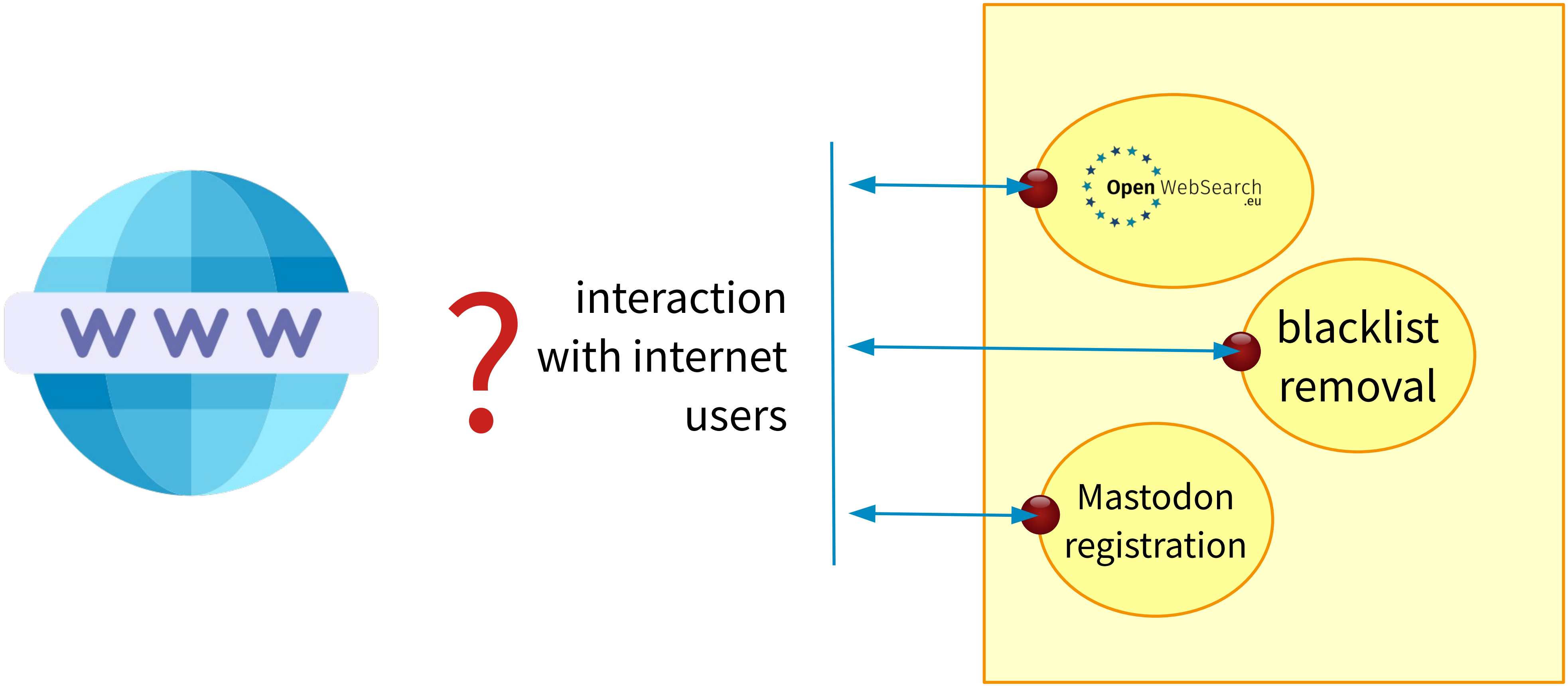
Help!

I have 500+ independent registrations already!

Composition

- Organization of many "back-ends"
- Privacy
- Legal diversity
- Parties need the same kind of registration
  - some personal facts
  - email ownership proof
  - website ownership proof
- Disconnected implementations

Positioning, generic use



?

interaction with internet users

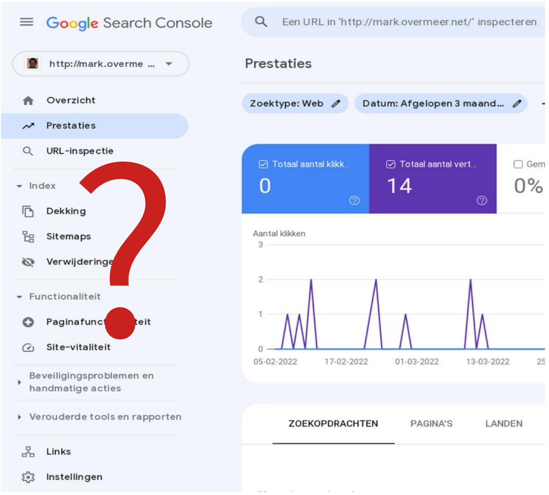
Open WebSearch .eu

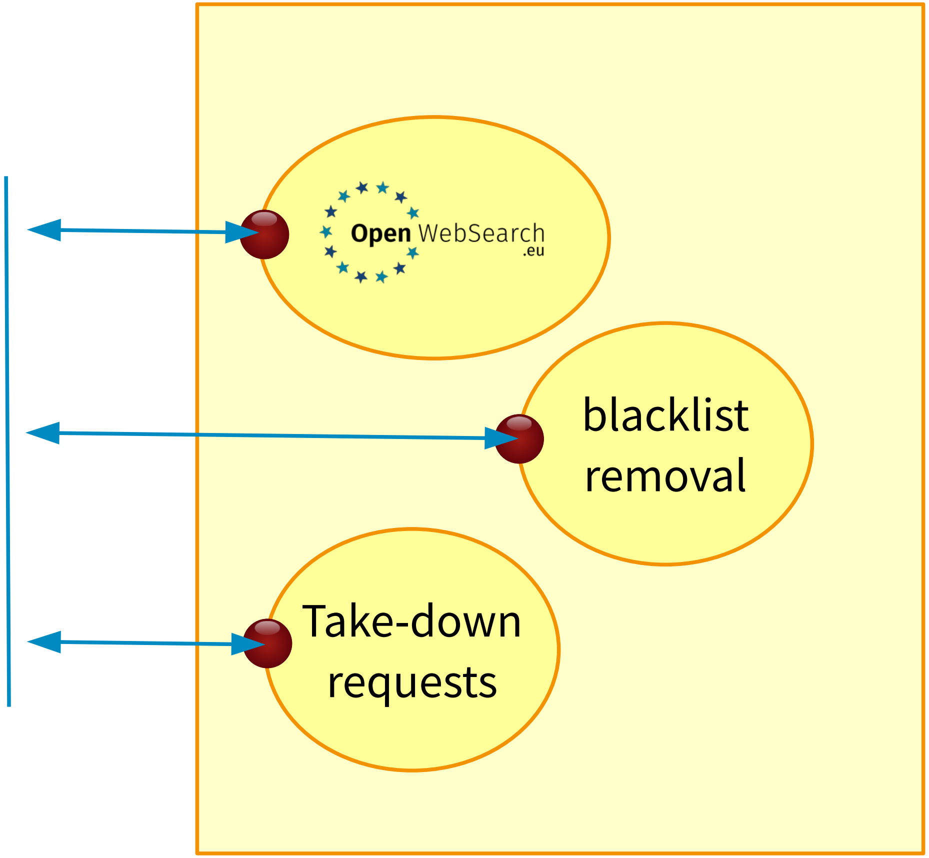
blacklist removal

Mastodon registration

Generic Console

Google Search Console





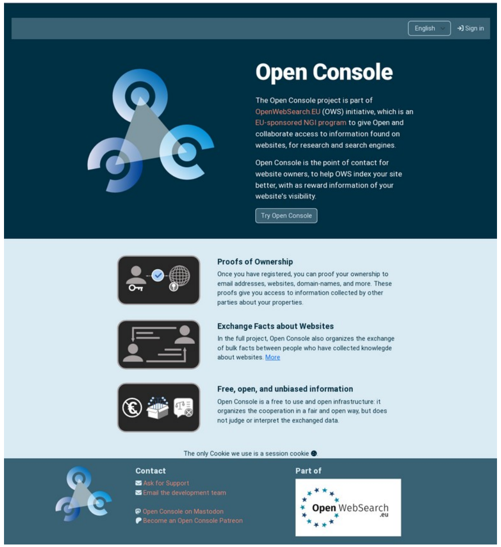
Open WebSearch .eu

blacklist removal

Take-down requests

Generic Console

Open Console



Open Console

The Open Console project is part of OpenWebSearch.EU (OWS) initiative, which is an EU-sponsored NGI program to give Open and collaborate access to information found on websites, for research and search engines.

Open Console is the point of contact for website owners, to help OWS index your site better, with as reward information of your website's visibility.

Proofs of Ownership

Once you have registered, you can proof your ownership to email addresses, websites, domain-names, and more. These proofs give you access to information collected by other parties about your properties.

Exchange Facts about Websites

In the full project, Open Console also organizes the exchange of bulk facts between people who have collected knowlegde about websites. More

Free, open, and unbiased information

Open Console is a free to use and open infrastructure: it organizes the cooperation in a fair and open way, but does not judge or interpret the exchanged data.

The only Cookie we use is a session cookie 🍪.

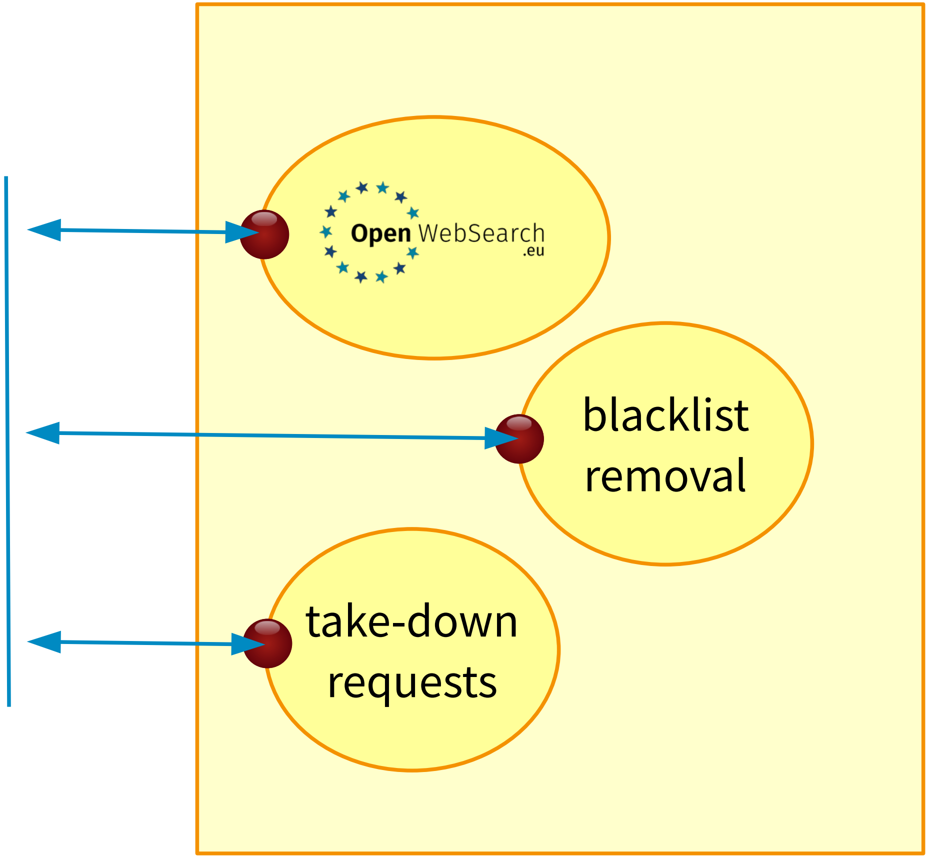
Contact

✉ Ask for Support
✉ Email the development team

Open Console on Mastodon
Become an Open Console Patreon

Part of

Open WebSearch .eu



Target

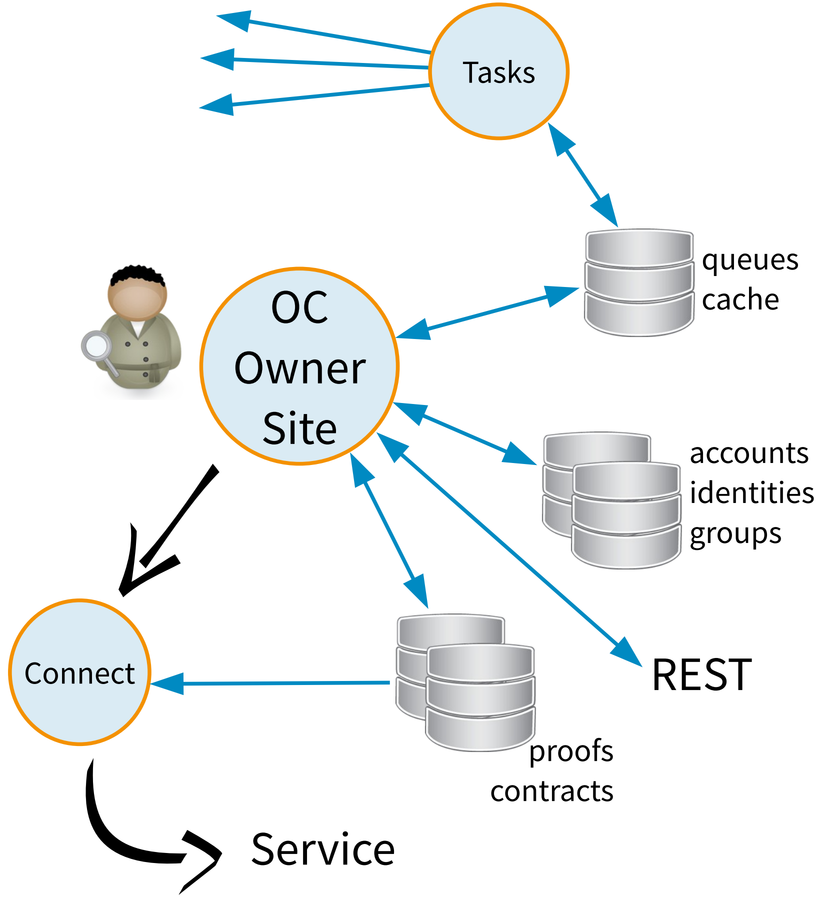
Google's power, created for Open Communities

- Service discovery: who has info for me?
- "OpenID" provider, single sign on

- Huge scale:
  - 300M+ websites → 100M+ website owners
  - any internet user
  - any open source application

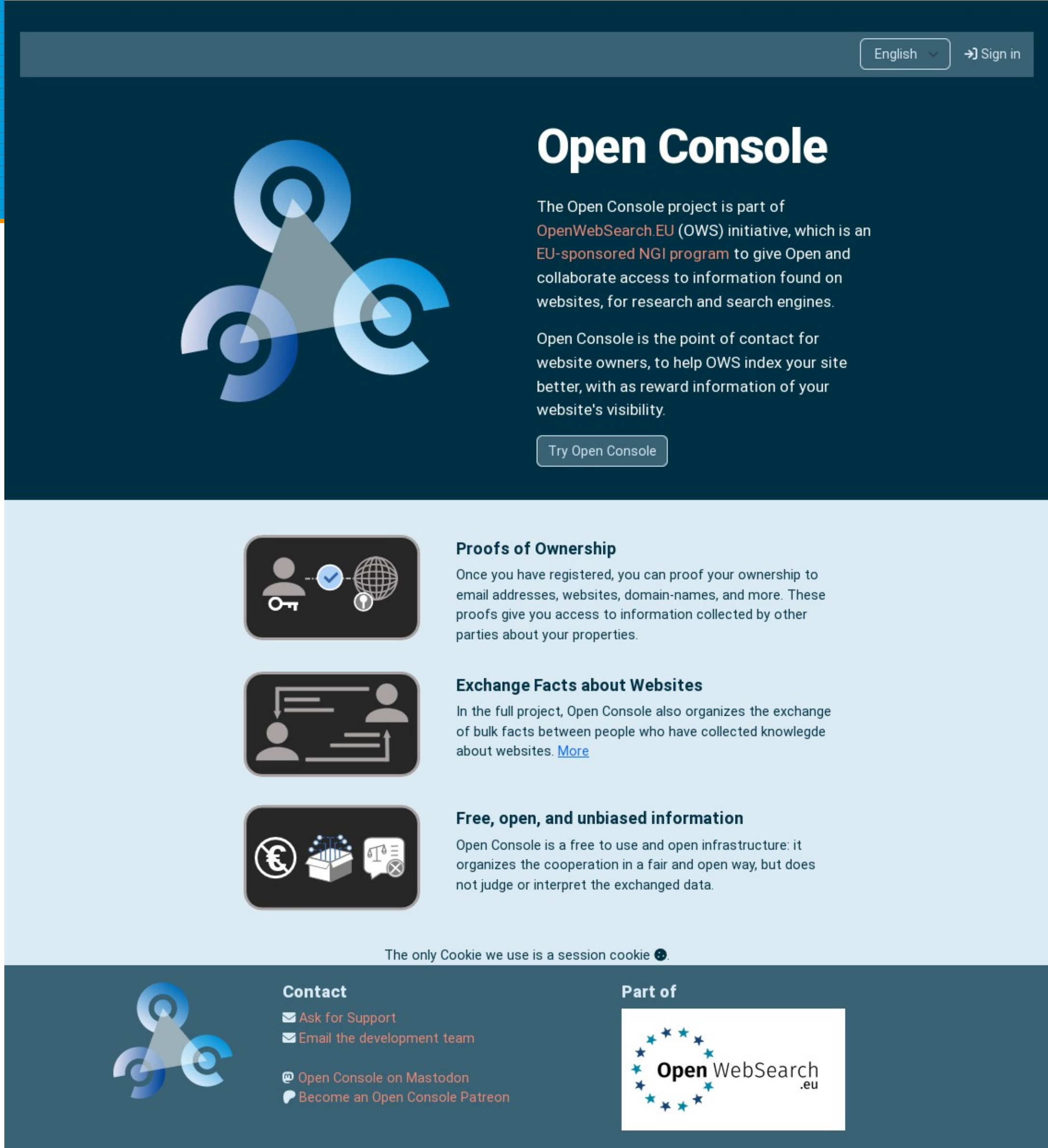
Prepared for HUGE scale

- Different DBs clusters per data character, different DB types.
- Cluster of worker servers for slow tasks.
- Cluster of servers for connect (login) processes
- Security/Privacy/Fairness



"Console"

- Use is **not limited** to OpenWebSearch.EU!



Open Console

The Open Console project is part of OpenWebSearch.EU (OWS) initiative, which is an EU-sponsored NGI program to give Open and collaborate access to information found on websites, for research and search engines.

Open Console is the point of contact for website owners, to help OWS index your site better, with as reward information of your website's visibility.

Proofs of Ownership

Once you have registered, you can proof your ownership to email addresses, websites, domain-names, and more. These proofs give you access to information collected by other parties about your properties.

Exchange Facts about Websites

In the full project, Open Console also organizes the exchange of bulk facts between people who have collected knowlegde about websites. More

Free, open, and unbiased information

Open Console is a free to use and open infrastructure: it organizes the cooperation in a fair and open way, but does not judge or interpret the exchanged data.

The only Cookie we use is a session cookie 🍪.

Contact

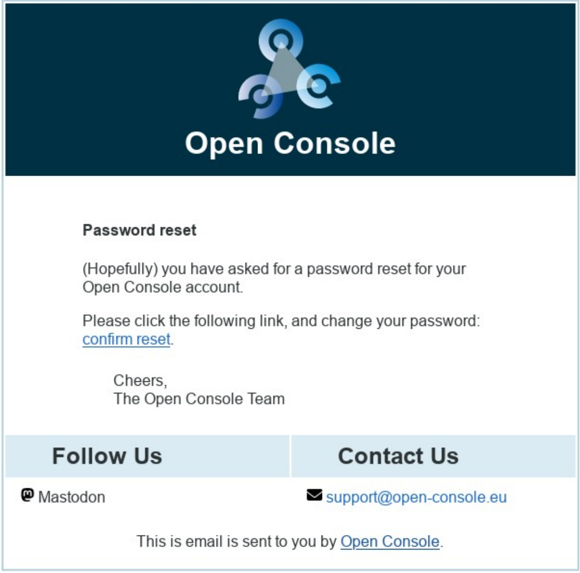
- Ask for Support
- Email the development team
- Open Console on Mastodon
- Become an Open Console Patreon

Part of

Login

- Register
- **Reset password**
- Sign in

reset email



Open Console

Password reset

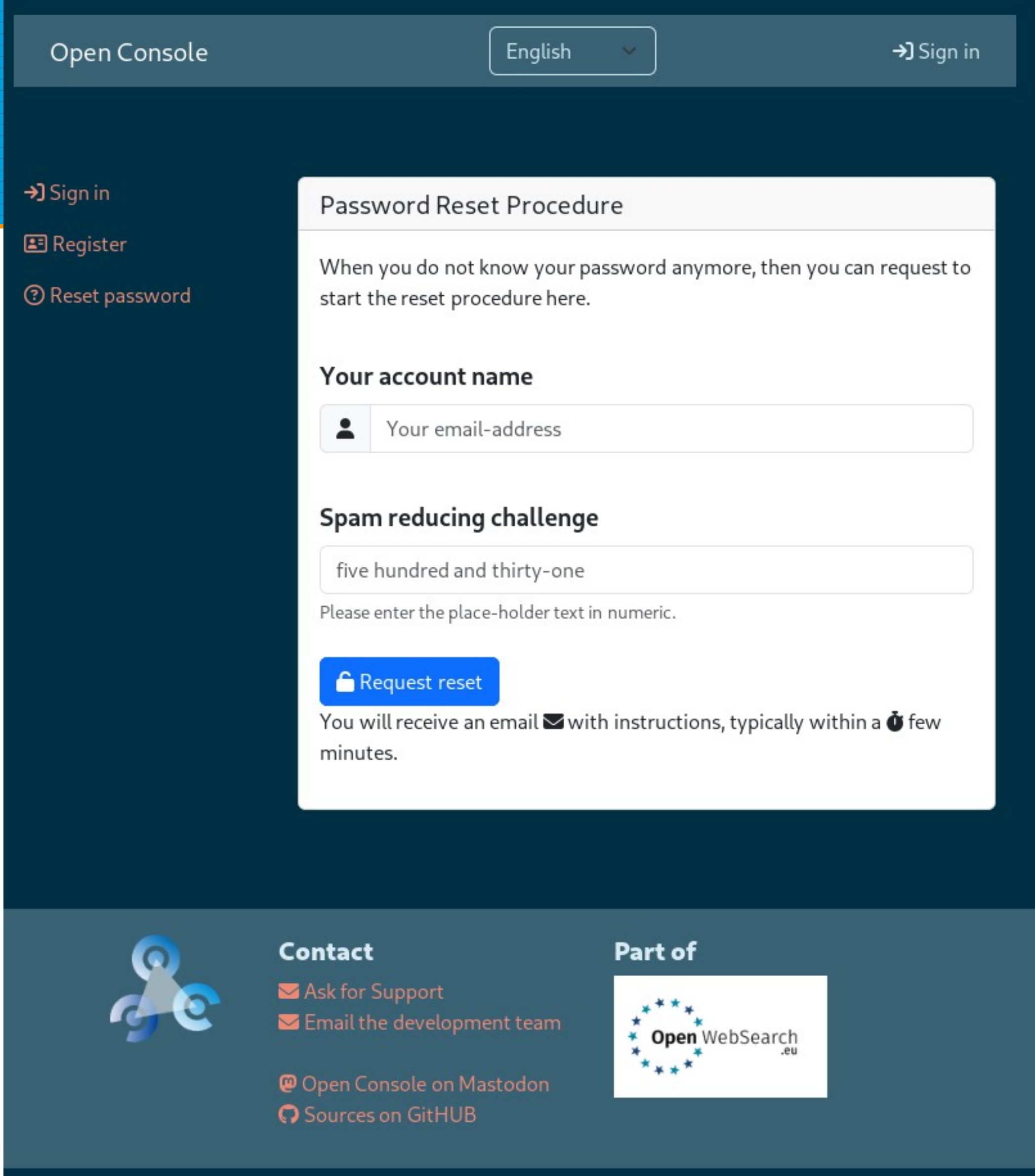
(Hopefully) you have asked for a password reset for your Open Console account.

Please click the following link, and change your password: confirm reset.

Cheers,
The Open Console Team

Follow Us	Contact Us
Mastodon	✉ support@open-console.eu

This is email is sent to you by Open Console.



Password Reset Procedure

When you do not know your password anymore, then you can request to start the reset procedure here.

Your account name

Your email-address

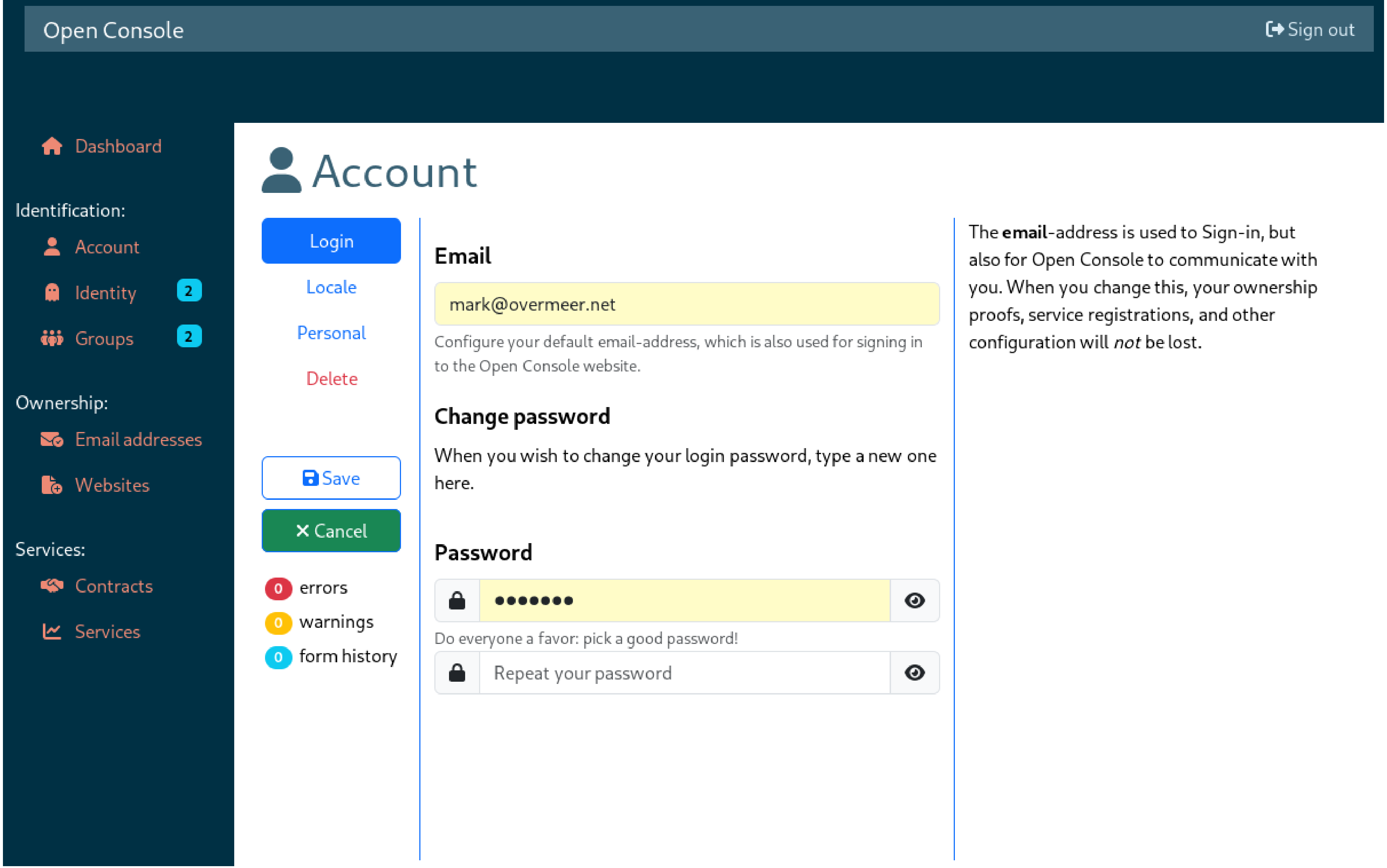
Spam reducing challenge

five hundred and thirty-one

Please enter the place-holder text in numeric.

Request reset

You will receive an email ✉ with instructions, typically within a ⏱ few minutes.



Account

Email

mark@overmeer.net

Configure your default email-address, which is also used for signing in to the Open Console website.

Change password

When you wish to change your login password, type a new one here.

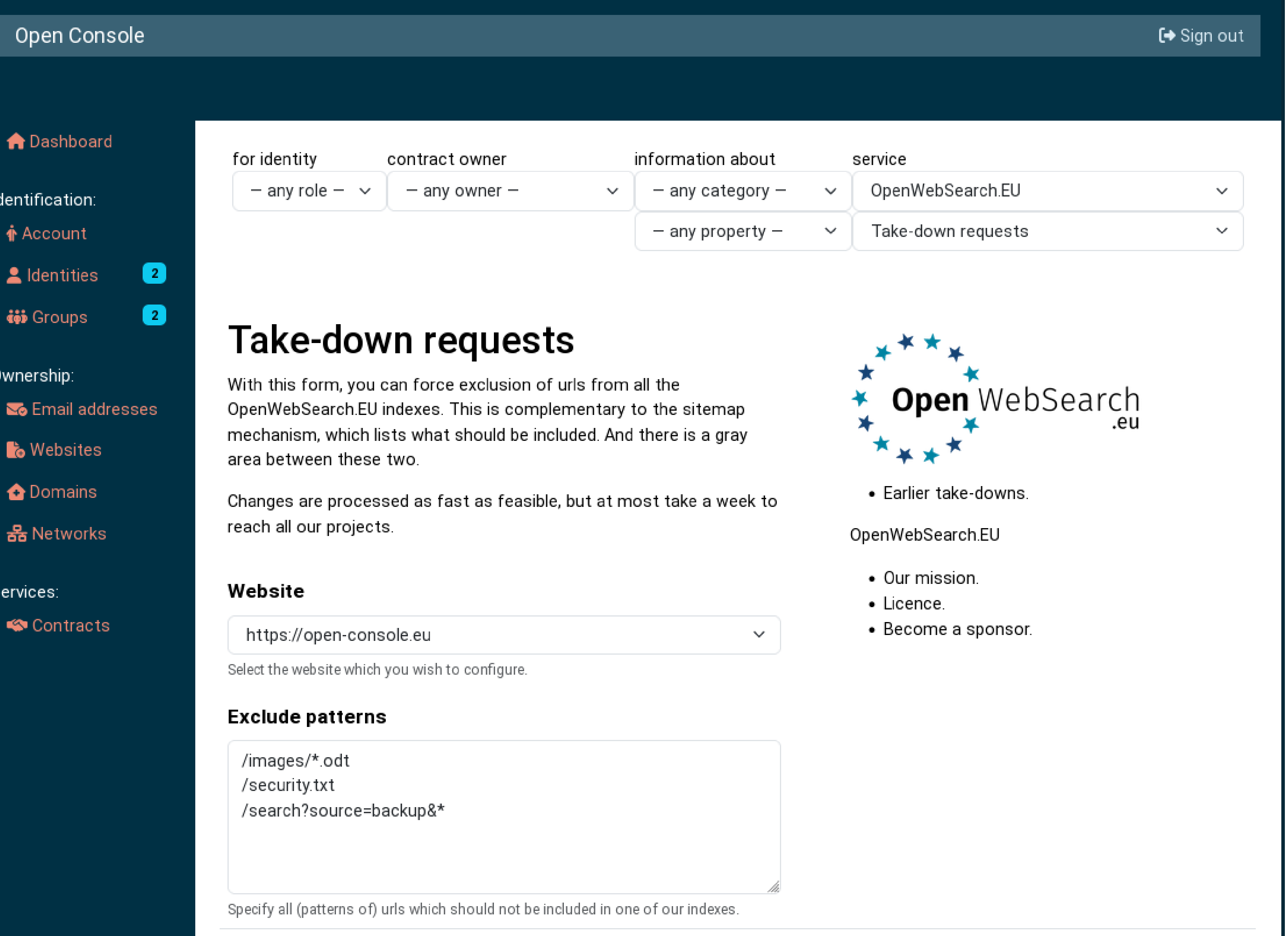
Password

●●●●●●●

Do everyone a favor: pick a good password!

Repeat your password

The **email**-address is used to Sign-in, but also for Open Console to communicate with you. When you change this, your ownership proofs, service registrations, and other configuration will *not* be lost.



Open Console

Sign out

Dashboard

dentification:

Account

Identities 2

Groups 2

wnership:

Email addresses

Websites

Domains

Networks

ervices:

Contracts

for identity	contract owner	information about	service
– any role –	– any owner –	– any category –	OpenWebSearch.EU
		– any property –	Take-down requests

Take-down requests

With this form, you can force exclusion of urls from all the OpenWebSearch.EU indexes. This is complementary to the sitemap mechanism, which lists what should be included. And there is a gray area between these two.

Changes are processed as fast as feasible, but at most take a week to reach all our projects.

Website

https://open-console.eu

Select the website which you wish to configure.

Exclude patterns

```
/images/*.odt
/security.txt
/search?source=backup&*
```

Specify all (patterns of) urls which should not be included in one of our indexes.

Open WebSearch .eu

- Earlier take-downs.

OpenWebSearch.EU

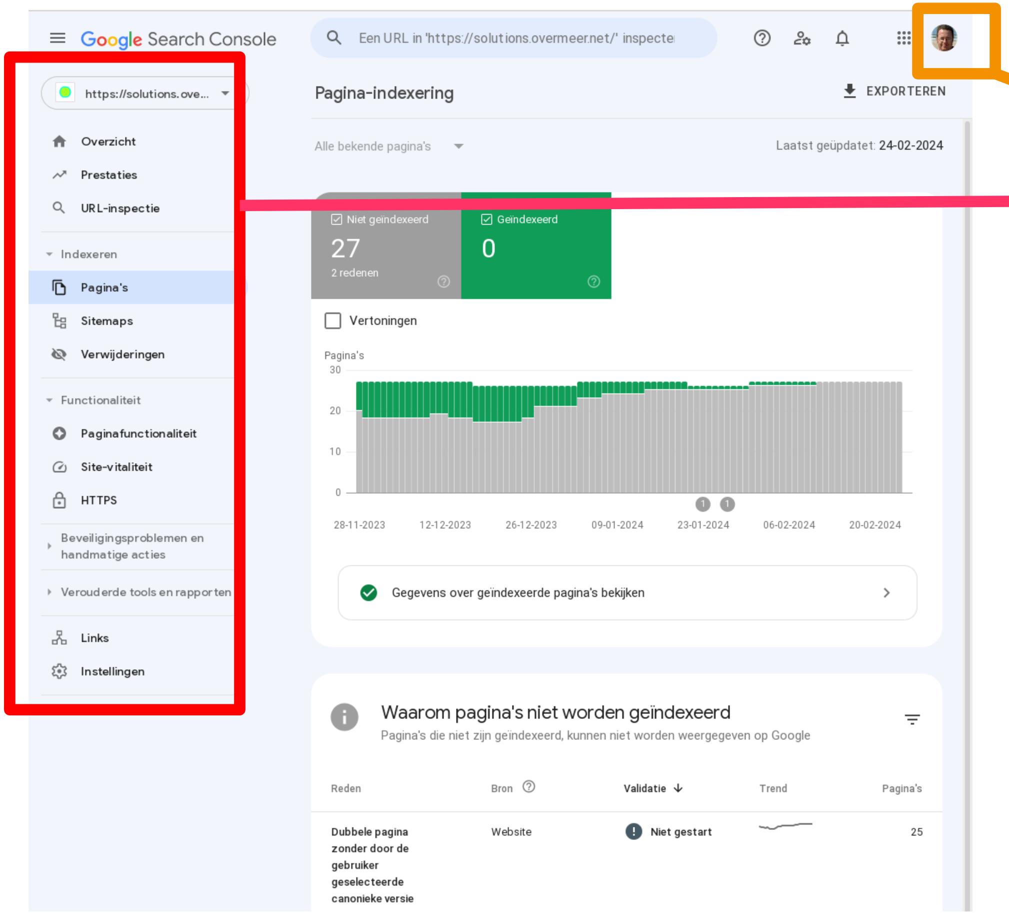
- Our mission.
- Licence.
- Become a sponsor.

Two modes:

1) Integrated display

2) Login button

Consoles Side-by-side



Pagina-indexering

Laatst geüpdatet: 24-02-2024

☑ Niet geïndexeerd 27 2 redenen

☑ Geïndexeerd 0

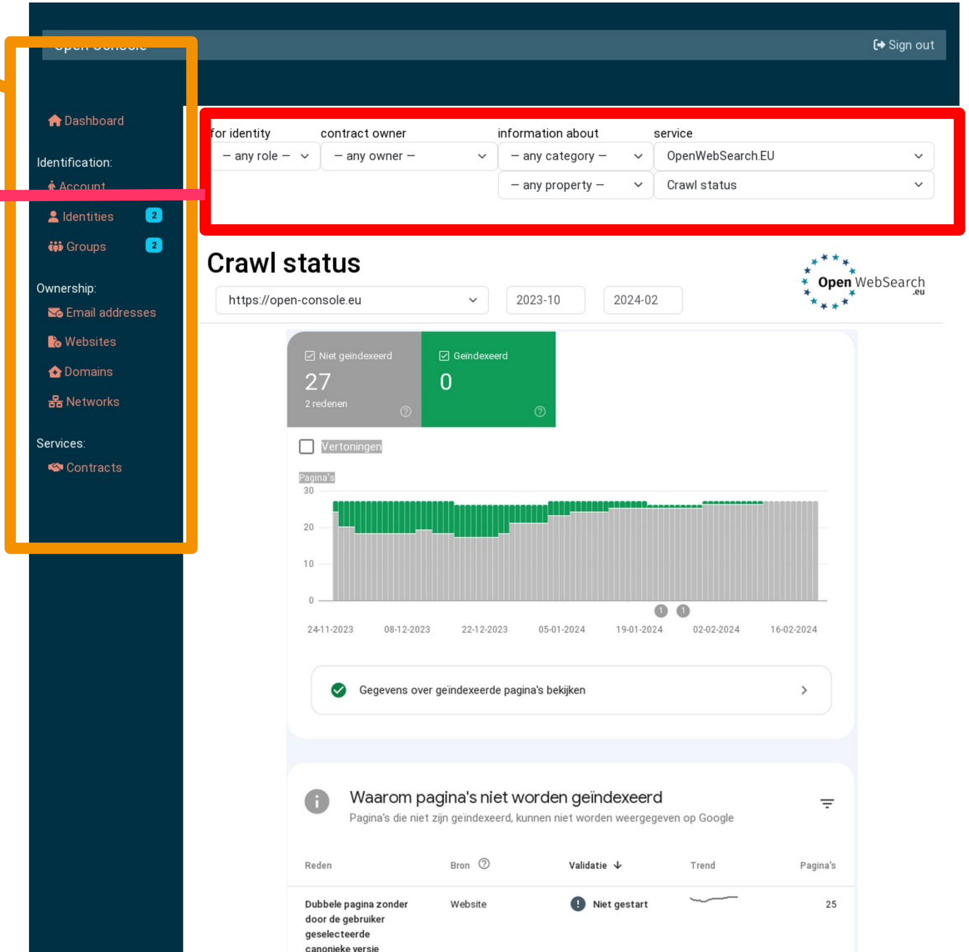
□ Vertoningen

Gegevens over geïndexeerde pagina's bekijken

Waarom pagina's niet worden geïndexeerd

Pagina's die niet zijn geïndexeerd, kunnen niet worden weergegeven op Google

Reden	Bron	Validatie	Trend	Pagina's
Dubbele pagina zonder door de gebruiker geselecteerde canonieke versie	Website	Niet gestart		25



for identity: – any role –

contract owner: – any owner –

information about: – any category – / – any property –

service: OpenWebSearch.EU / Crawl status

Crawl status

https://open-console.eu 2023-10 2024-02

☑ Niet geïndexeerd 27 2 redenen

☑ Geïndexeerd 0

□ Vertoningen

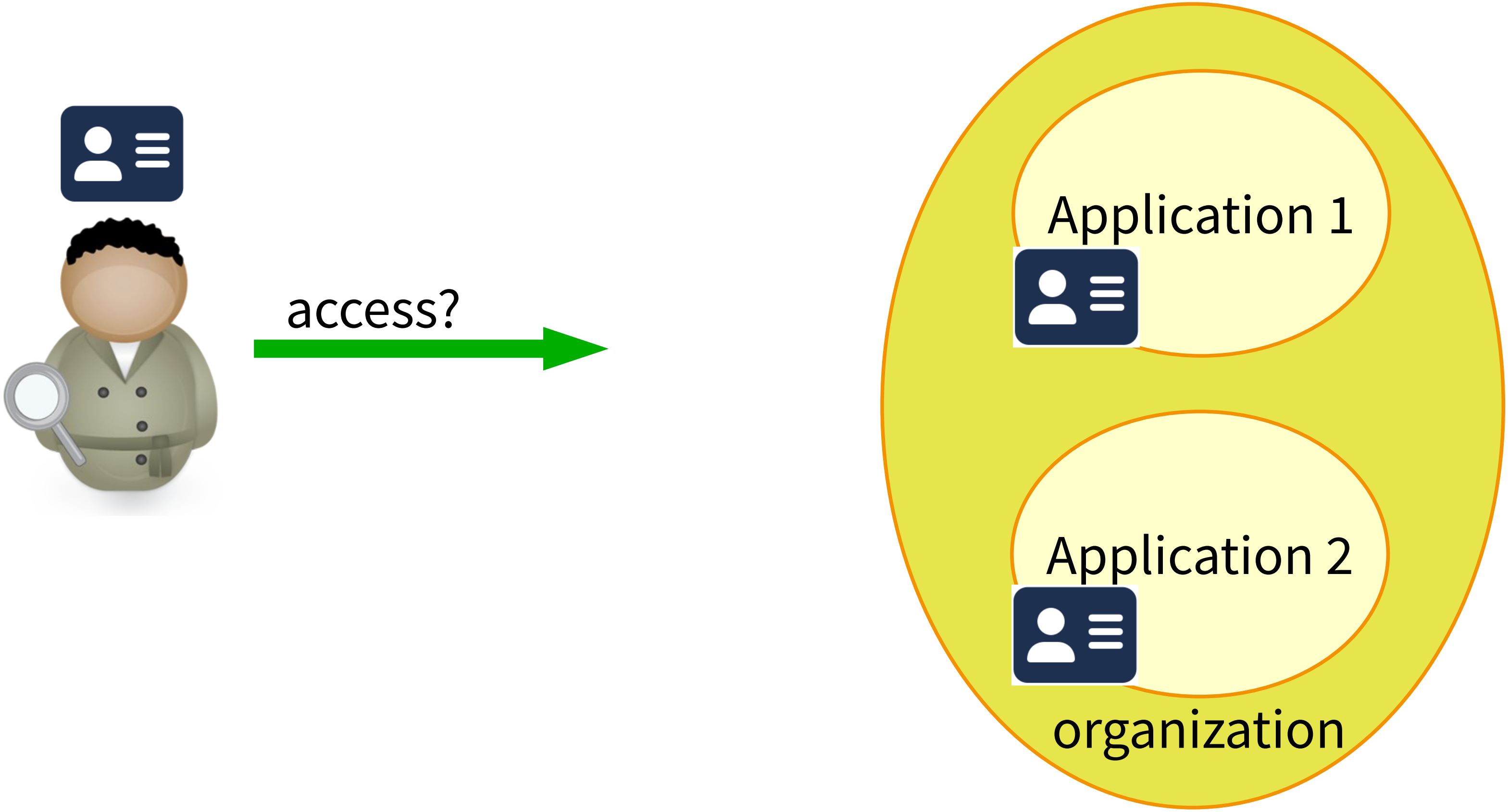
Gegevens over geïndexeerde pagina's bekijken

Waarom pagina's niet worden geïndexeerd

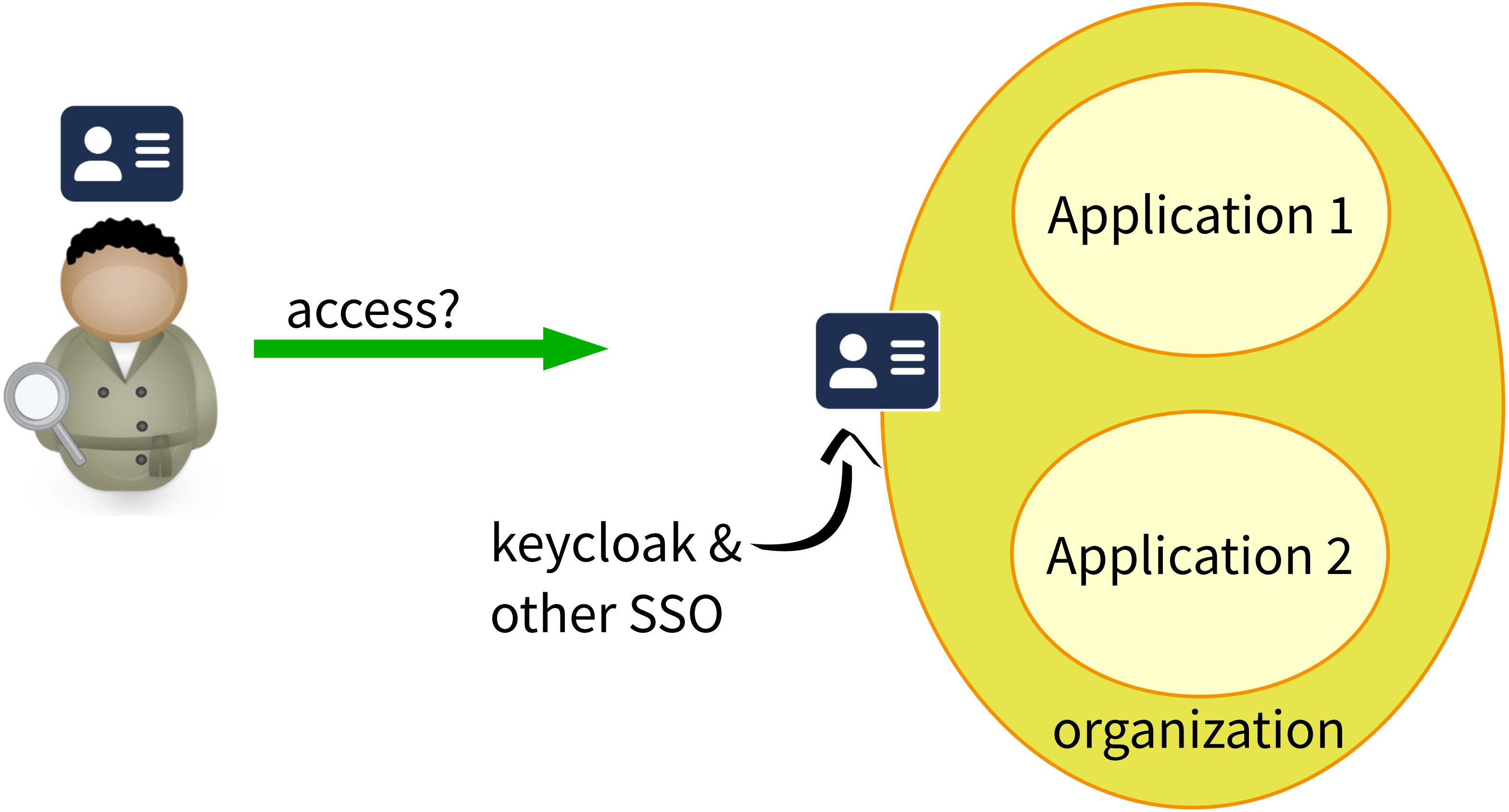
Pagina's die niet zijn geïndexeerd, kunnen niet worden weergegeven op Google

Reden	Bron	Validatie	Trend	Pagina's
Dubbele pagina zonder door de gebruiker geselecteerde canonieke versie	Website	Niet gestart		25

Level of integration



Level of integration



access?

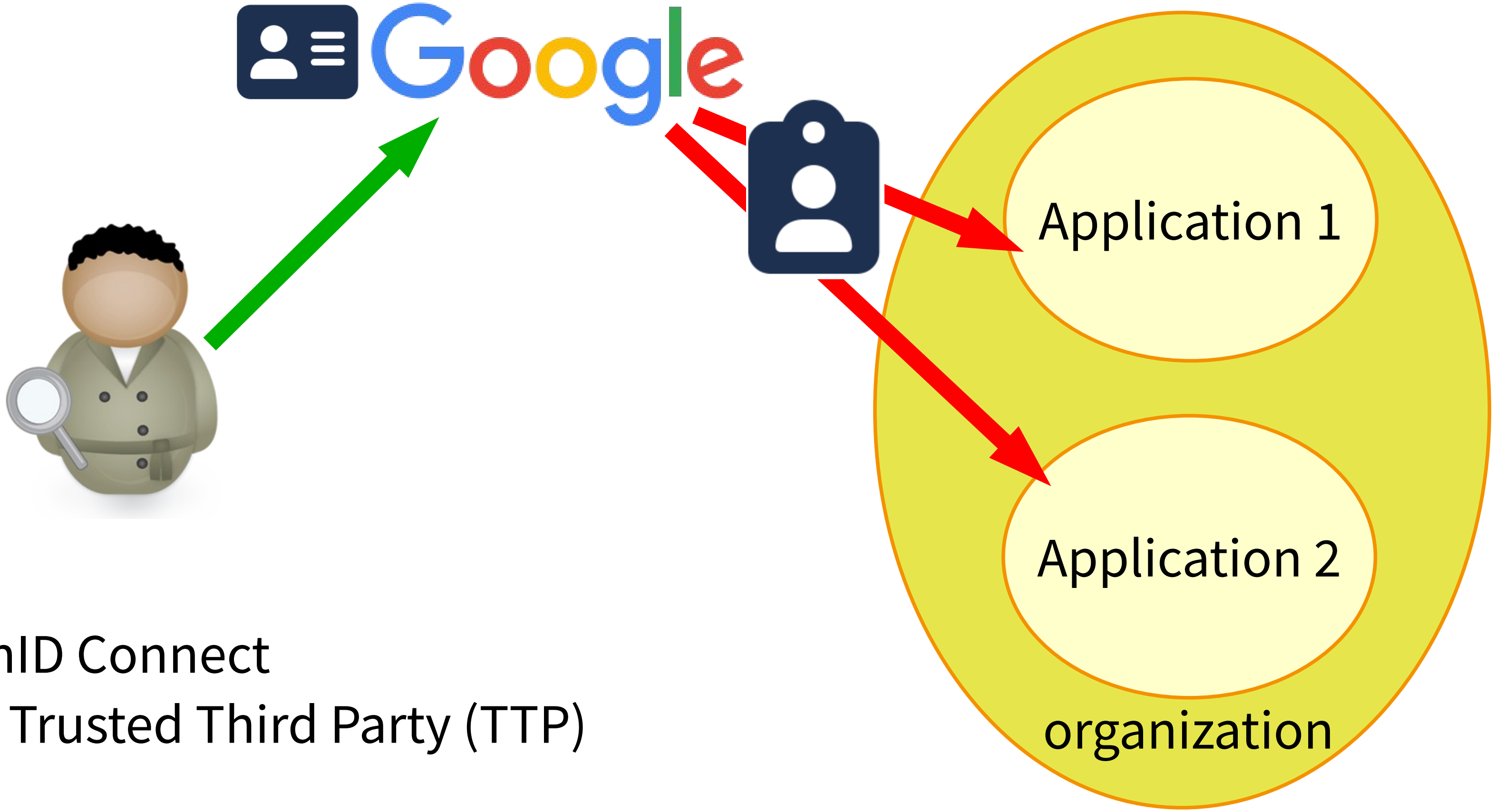
keycloak &
other SSO

Application 1

Application 2

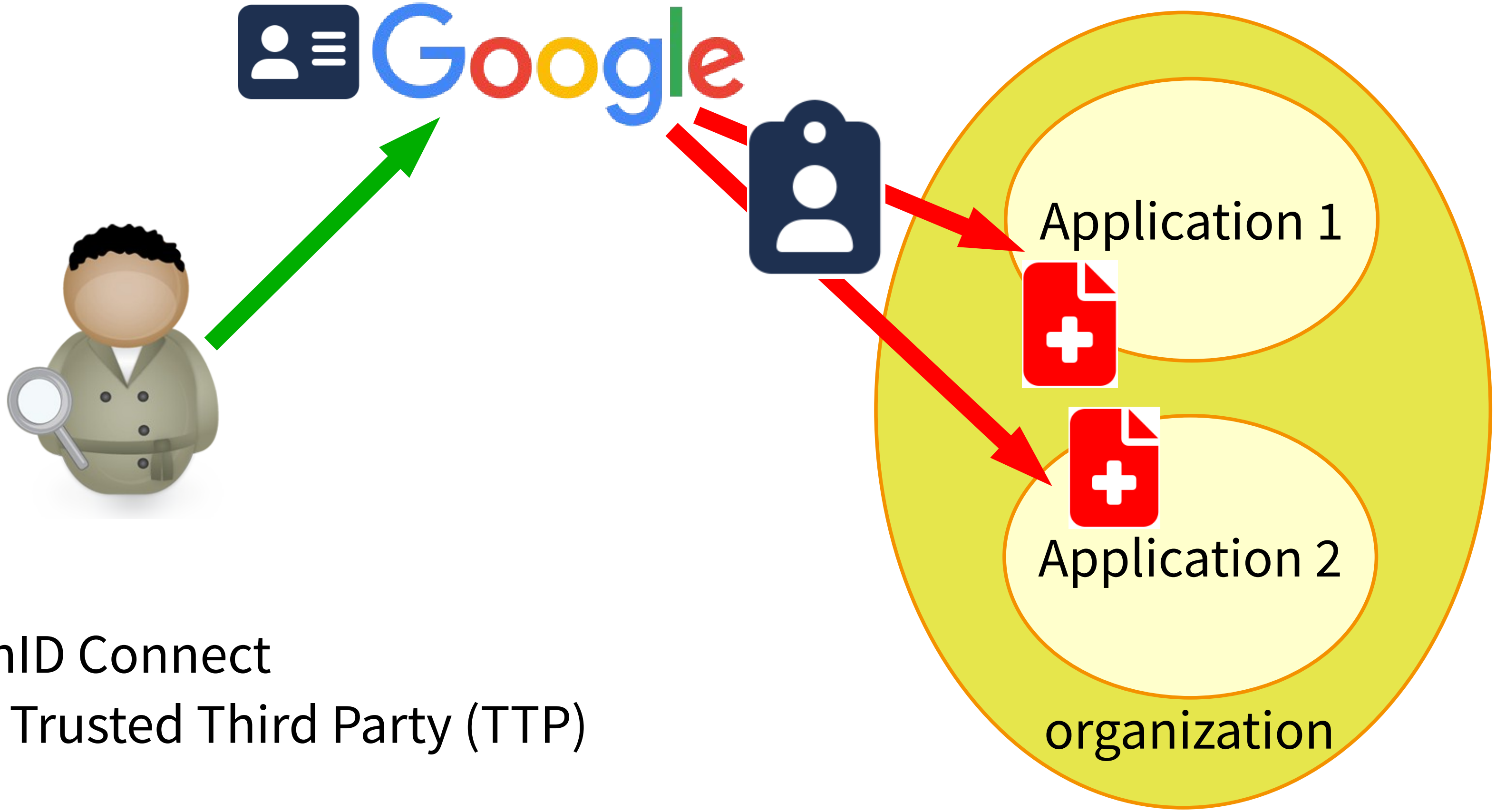
organization

Level of integration



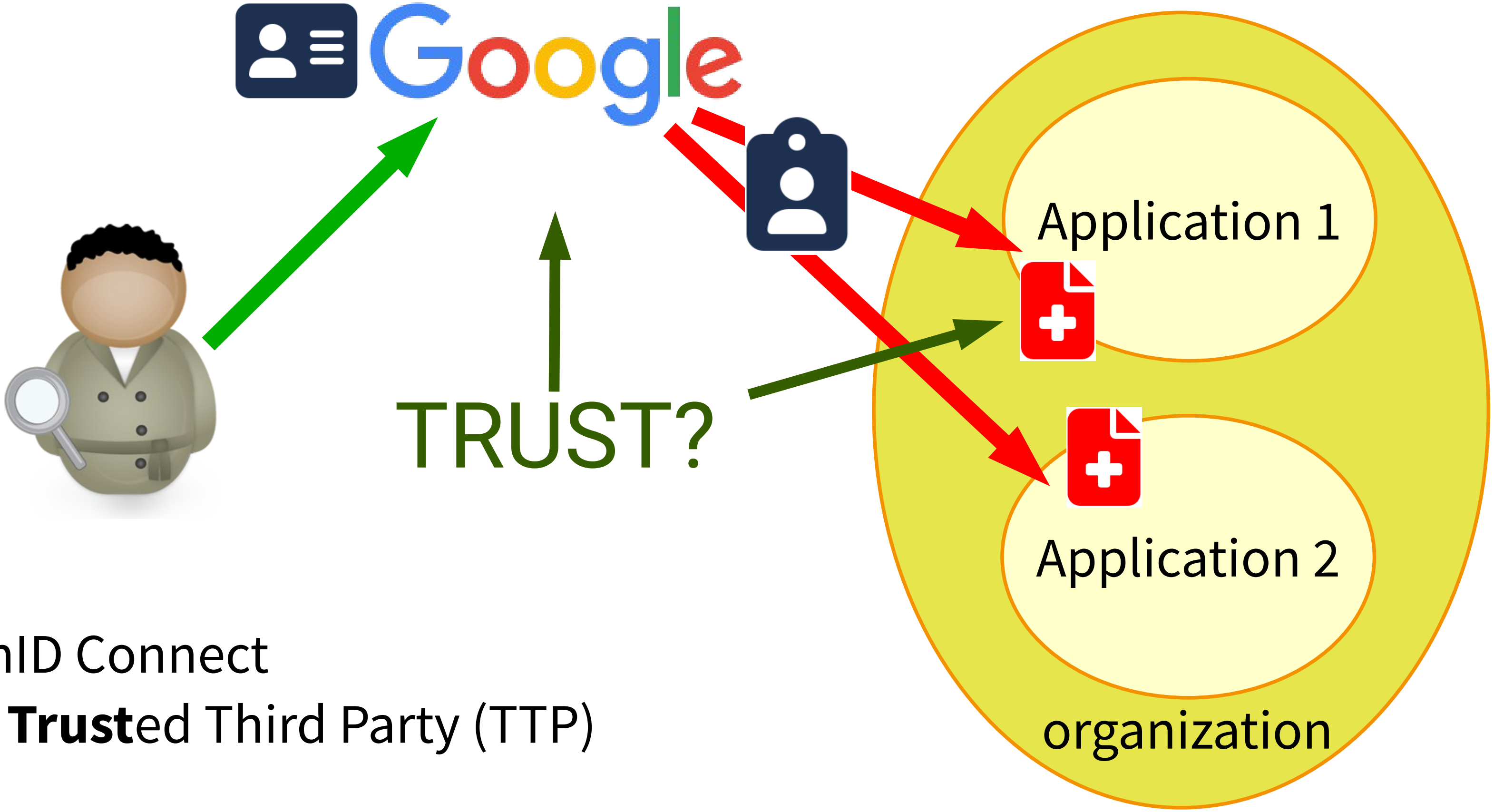
OpenID Connect
via a Trusted Third Party (TTP)

Level of integration



OpenID Connect
via a Trusted Third Party (TTP)

Level of integration

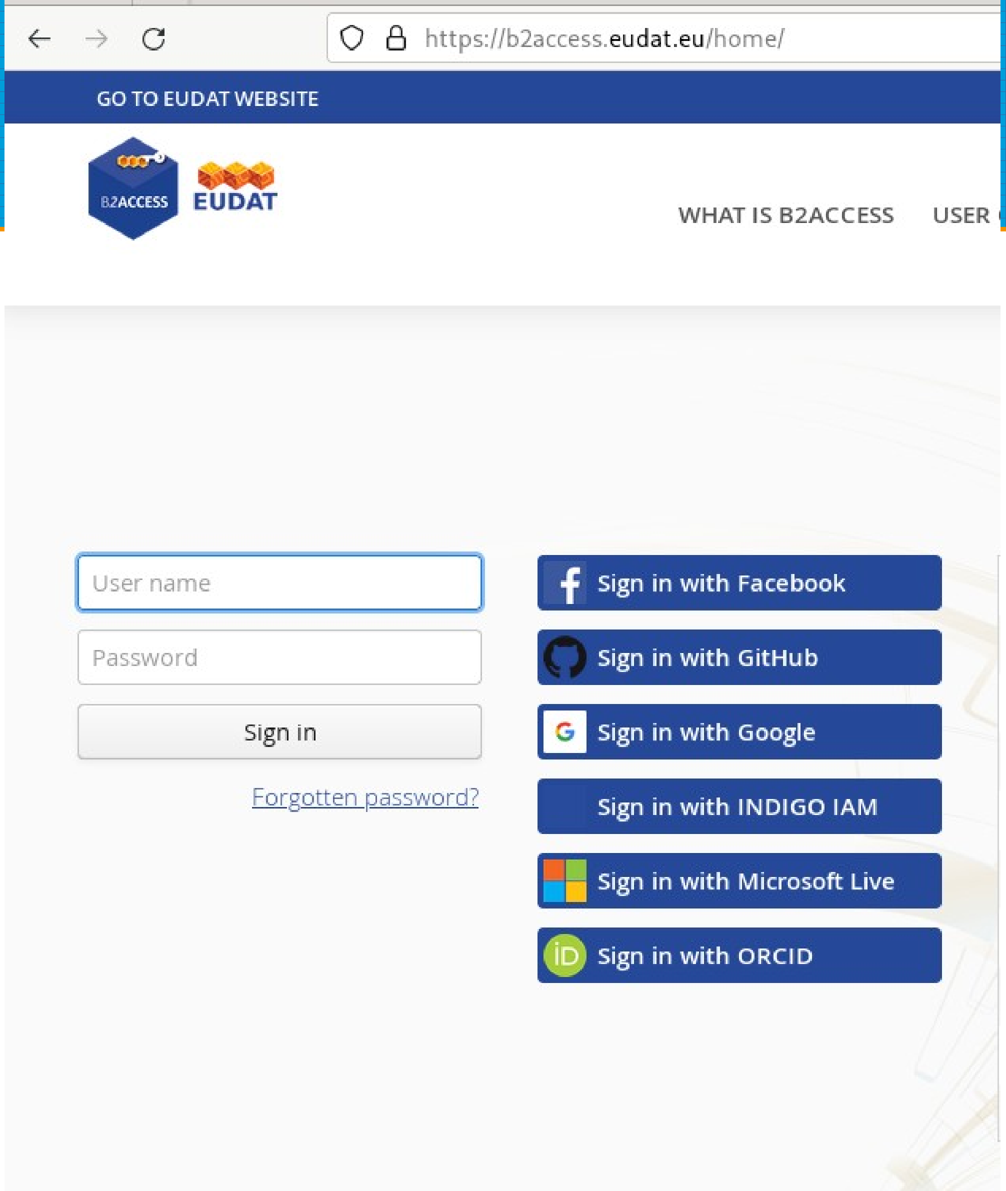


OpenID Connect
via a **Trust**ed Third Party (TTP)

TTP

Who do you TRUST

?



https://b2access.eudat.eu/home/

GO TO EUDAT WEBSITE

WHAT IS B2ACCESS USER

Current possibilities are PRIMITIVE!

- organize me
- limited and transparent
- cooperation
- insufficient facts

Current possibilities are PRIMITIVE!

- My activities are **diverse**
- My services come from **many sources**

- I want to **manage** which facts are shared
- I do not (want to) **trust** the TTF (BigTech)

- Some logins are **shared** with colleagues
- My boss is **responsible** for my use!

- Still need for **additional registration**, like "agree terms"
- **Additional facts** needed

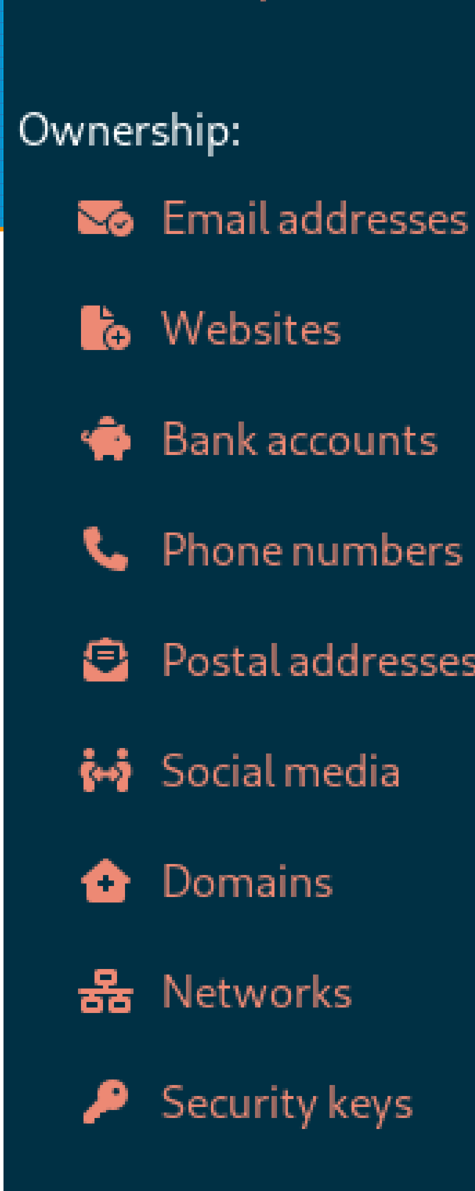
Facts to share

"Login via Google"

- OpenID Connect:
  sub name given_name family_name middle_name nickname preferred_username profile picture website email email_verified gender birthdate zoneinfo locale phone_number phone_number_verified address updated_at
- Website use statistics

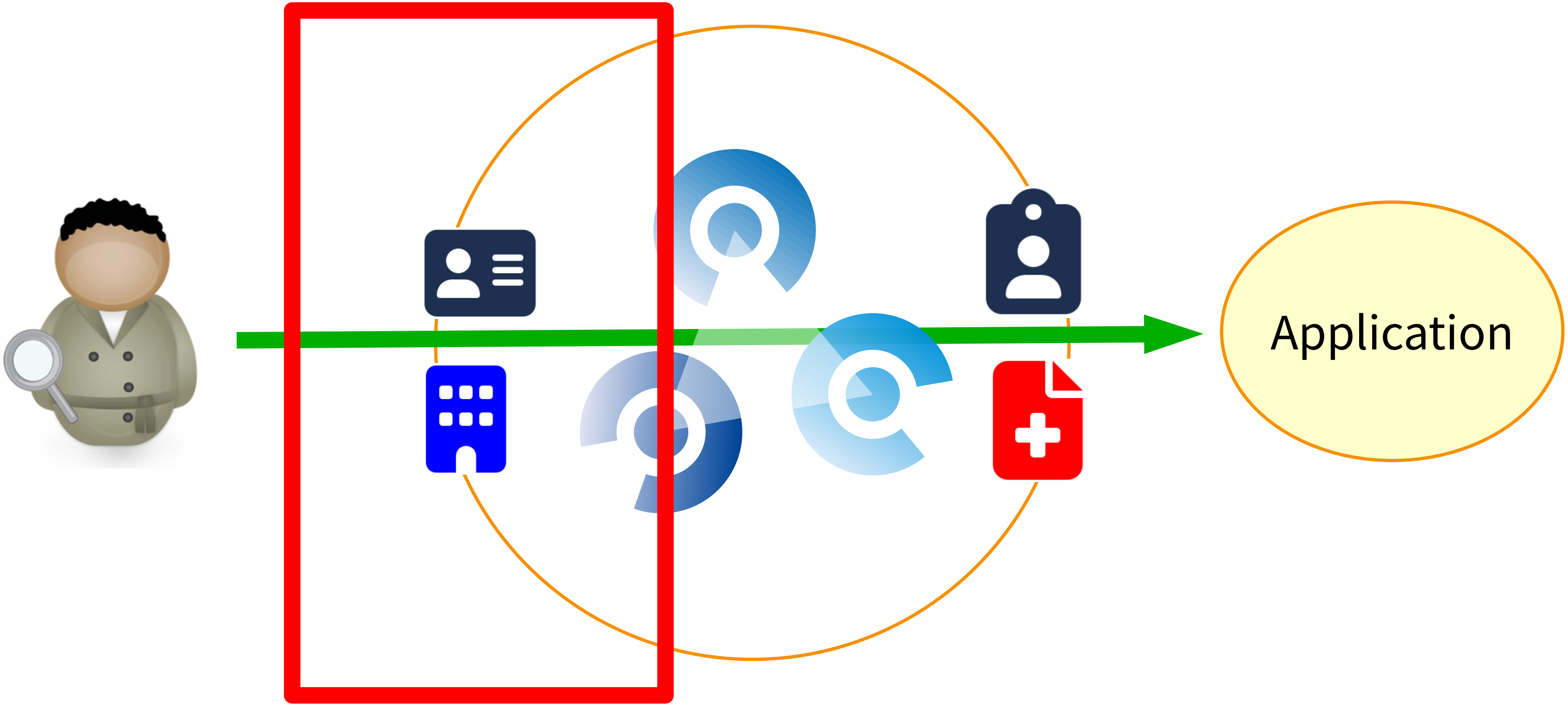
"Login via Open Console"

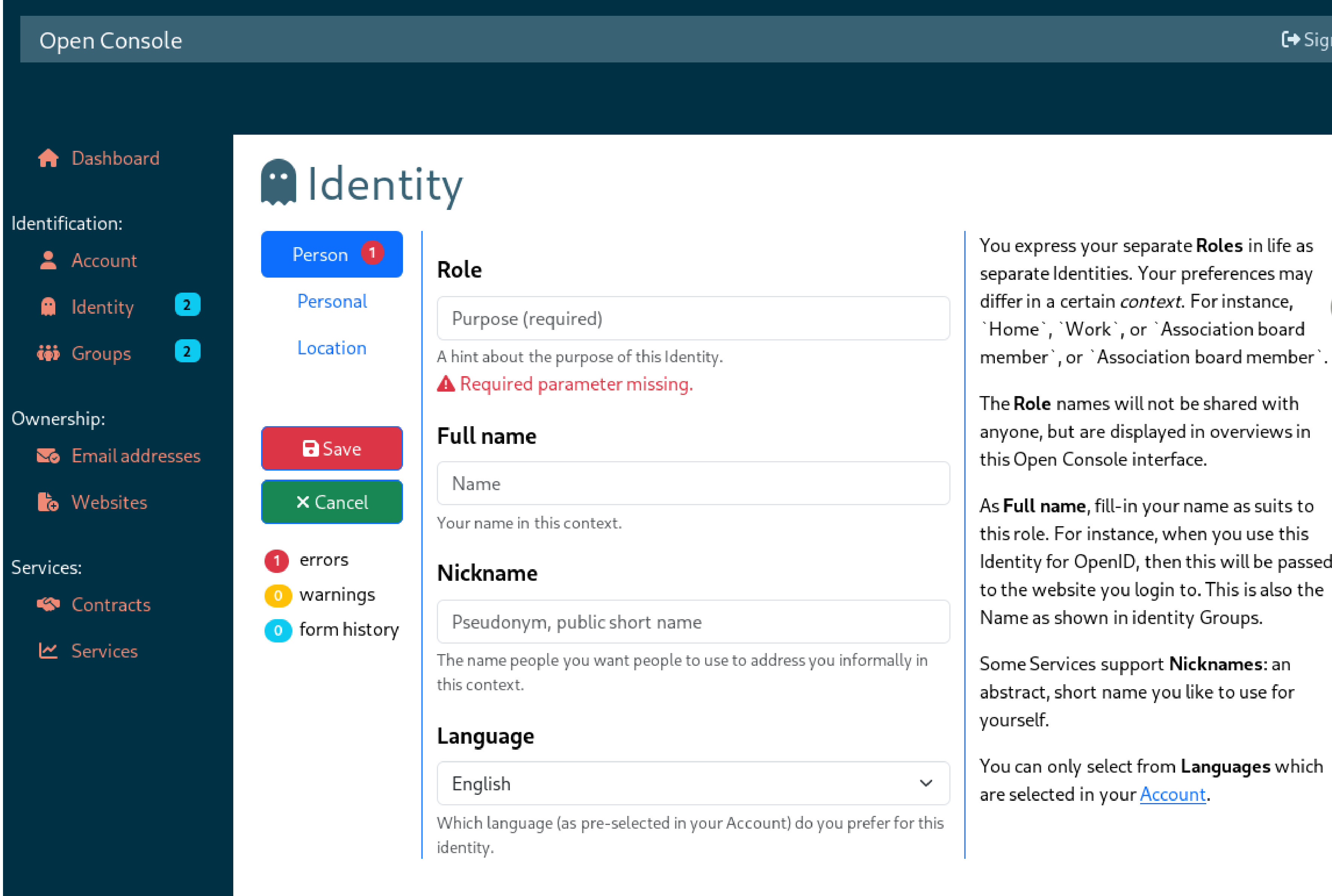
- Selected OpenID claims
- Identities and Groups
- Proofs →
- No tracing in any way


Ownership:

- Email addresses
- Websites
- Bank accounts
- Phone numbers
- Postal addresses
- Social media
- Domains
- Networks
- Security keys

Level of integration





Open Console

Sign out

Dashboard

Identification:

Account

Identity 2

Groups 2

Ownership:

Email addresses

Websites

Services:

Contracts

Services

Identity

Person 1

Personal

Location

Save

✕ Cancel

1 errors

0 warnings

0 form history

Role

Purpose (required)

A hint about the purpose of this Identity.

⚠ Required parameter missing.

Full name

Name

Your name in this context.

Nickname

Pseudonym, public short name

The name people you want people to use to address you informally in this context.

Language

English

Which language (as pre-selected in your Account) do you prefer for this identity.

You express your separate **Roles** in life as separate Identities. Your preferences may differ in a certain *context*. For instance, `Home`, `Work`, or `Association board member`, or `Association board member`.

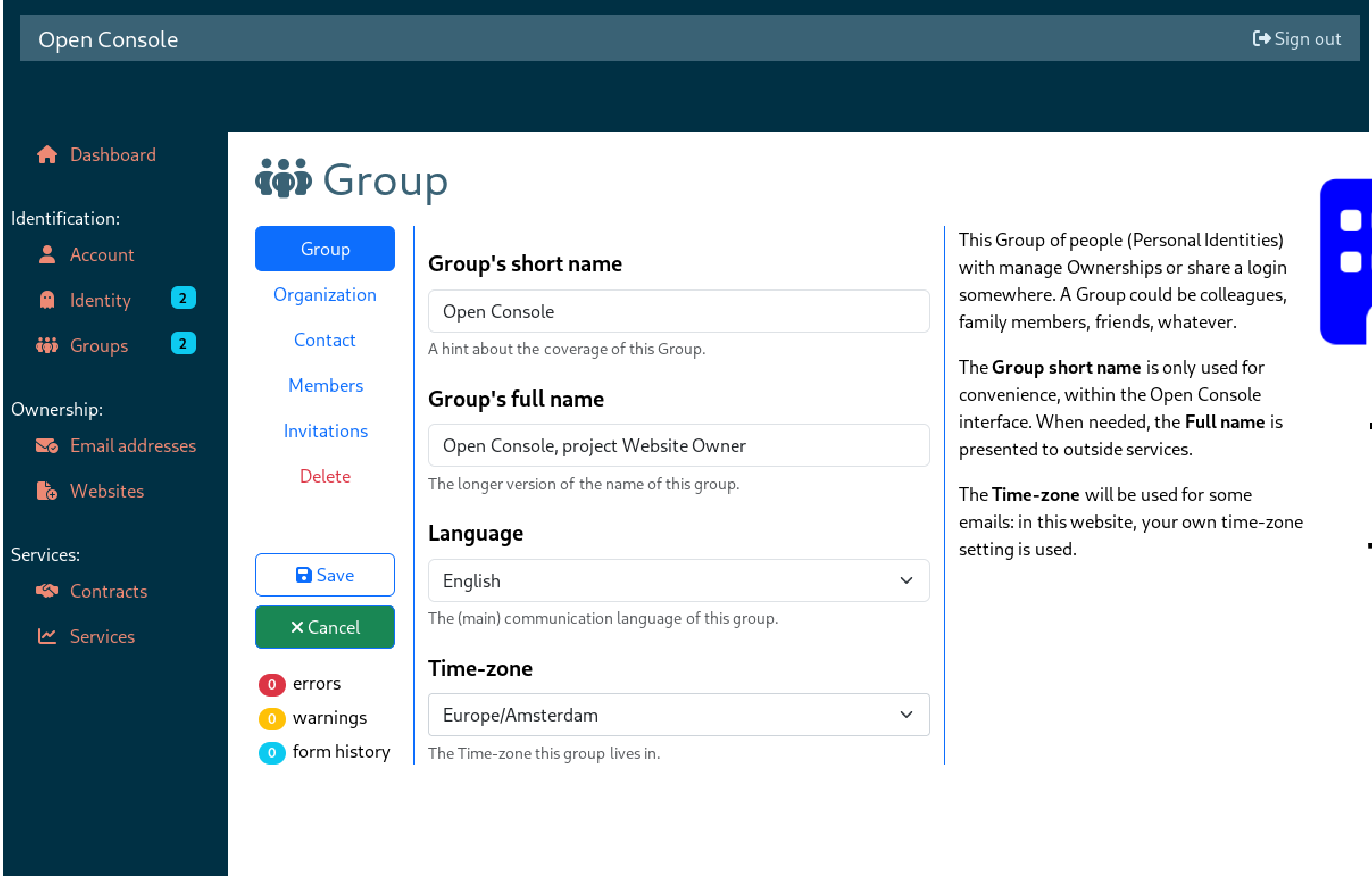
The **Role** names will not be shared with anyone, but are displayed in overviews in this Open Console interface.

As **Full name**, fill-in your name as suits to this role. For instance, when you use this Identity for OpenID, then this will be passed to the website you login to. This is also the Name as shown in identity Groups.

Some Services support **Nicknames**: an abstract, short name you like to use for yourself.

You can only select from **Languages** which are selected in your Account.

I am not flat!



Group

Group's short name

Open Console

A hint about the coverage of this Group.

Group's full name

Open Console, project Website Owner

The longer version of the name of this group.

Language

English

The (main) communication language of this group.

Time-zone

Europe/Amsterdam

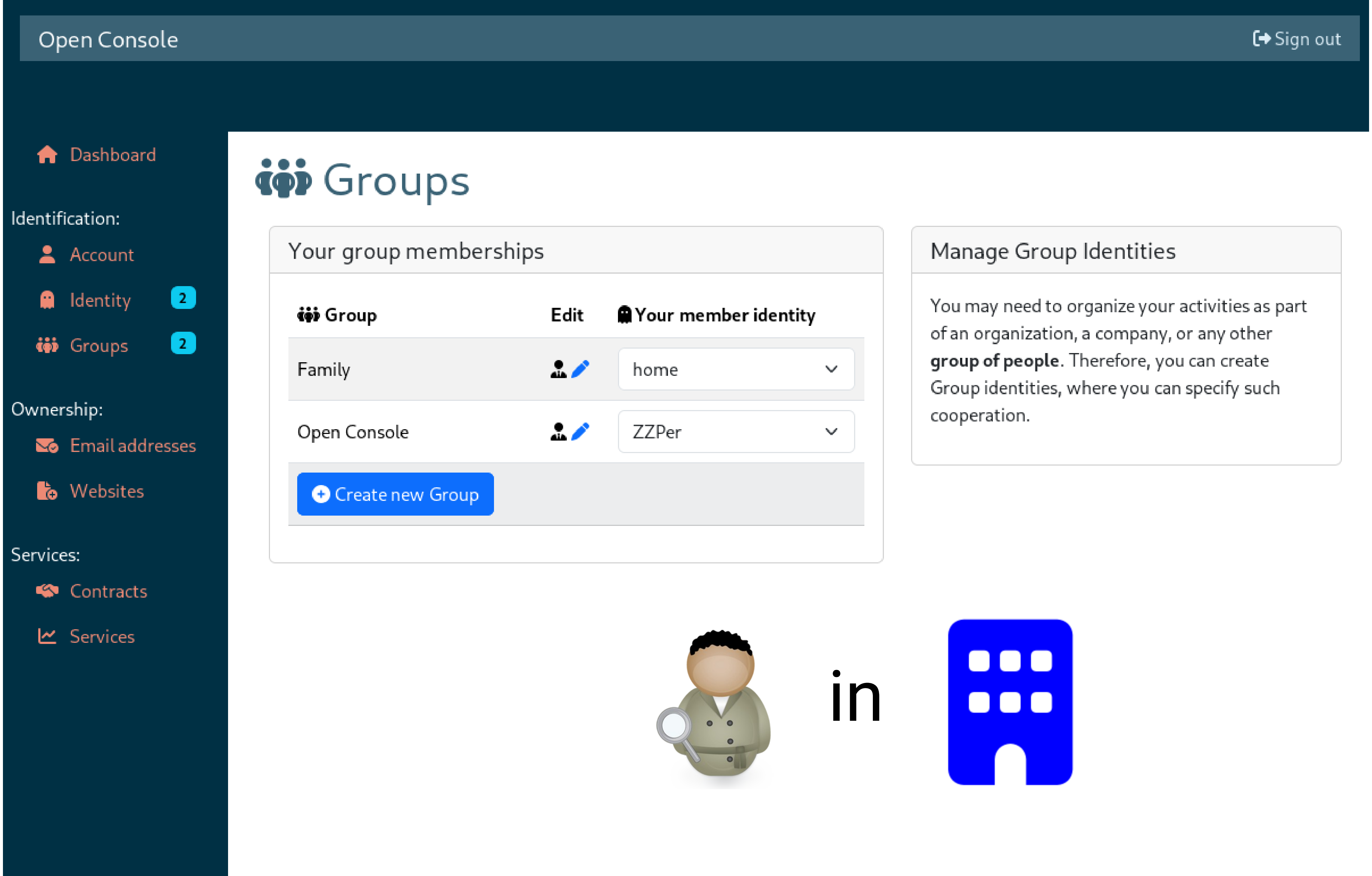
The Time-zone this group lives in.

This Group of people (Personal Identities) with manage Ownerships or share a login somewhere. A Group could be colleagues, family members, friends, whatever.

The **Group short name** is only used for convenience, within the Open Console interface. When needed, the **Full name** is presented to outside services.

The **Time-zone** will be used for some emails: in this website, your own time-zone setting is used.

I am not alone!



Groups

Your group memberships

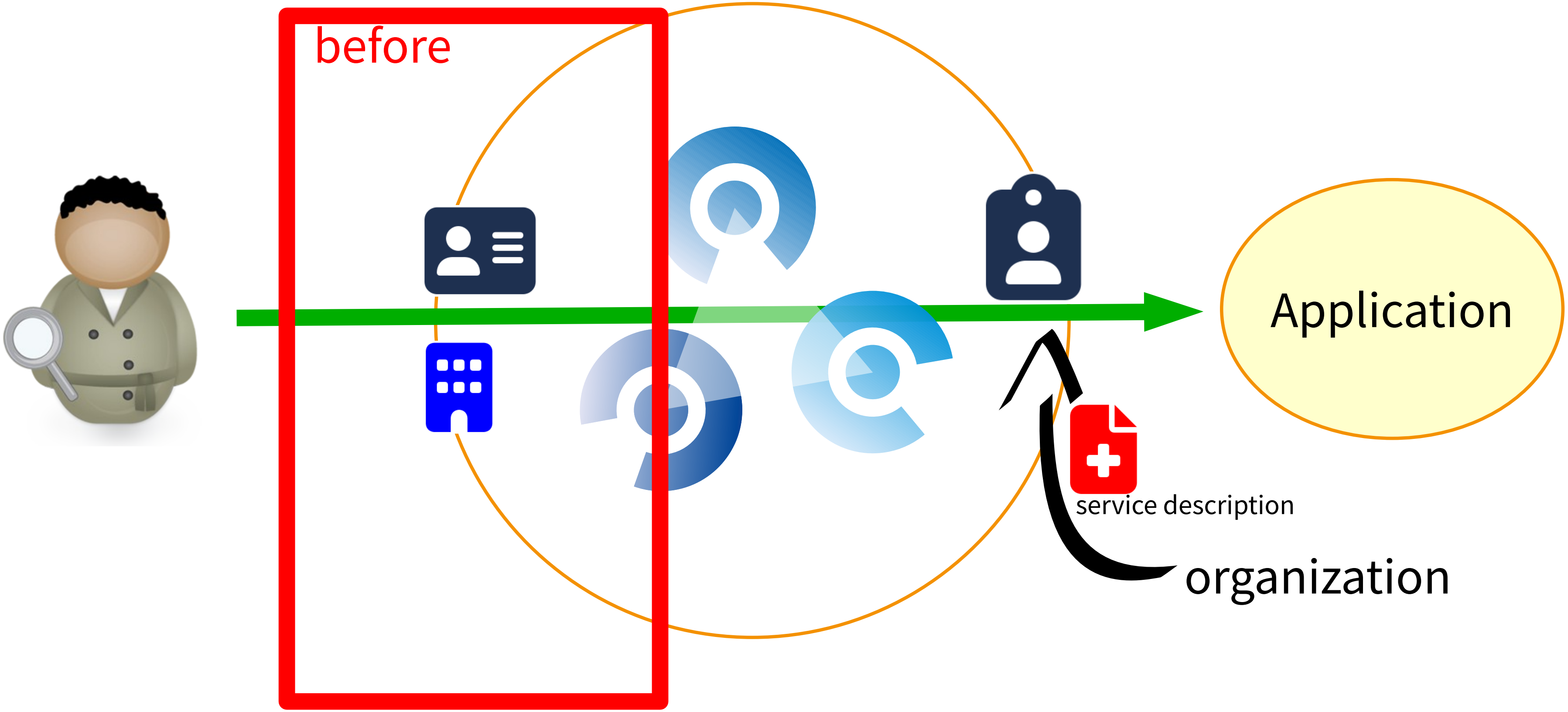
Group	Edit	Your member identity
Family		home
Open Console		ZZPer

Manage Group Identities

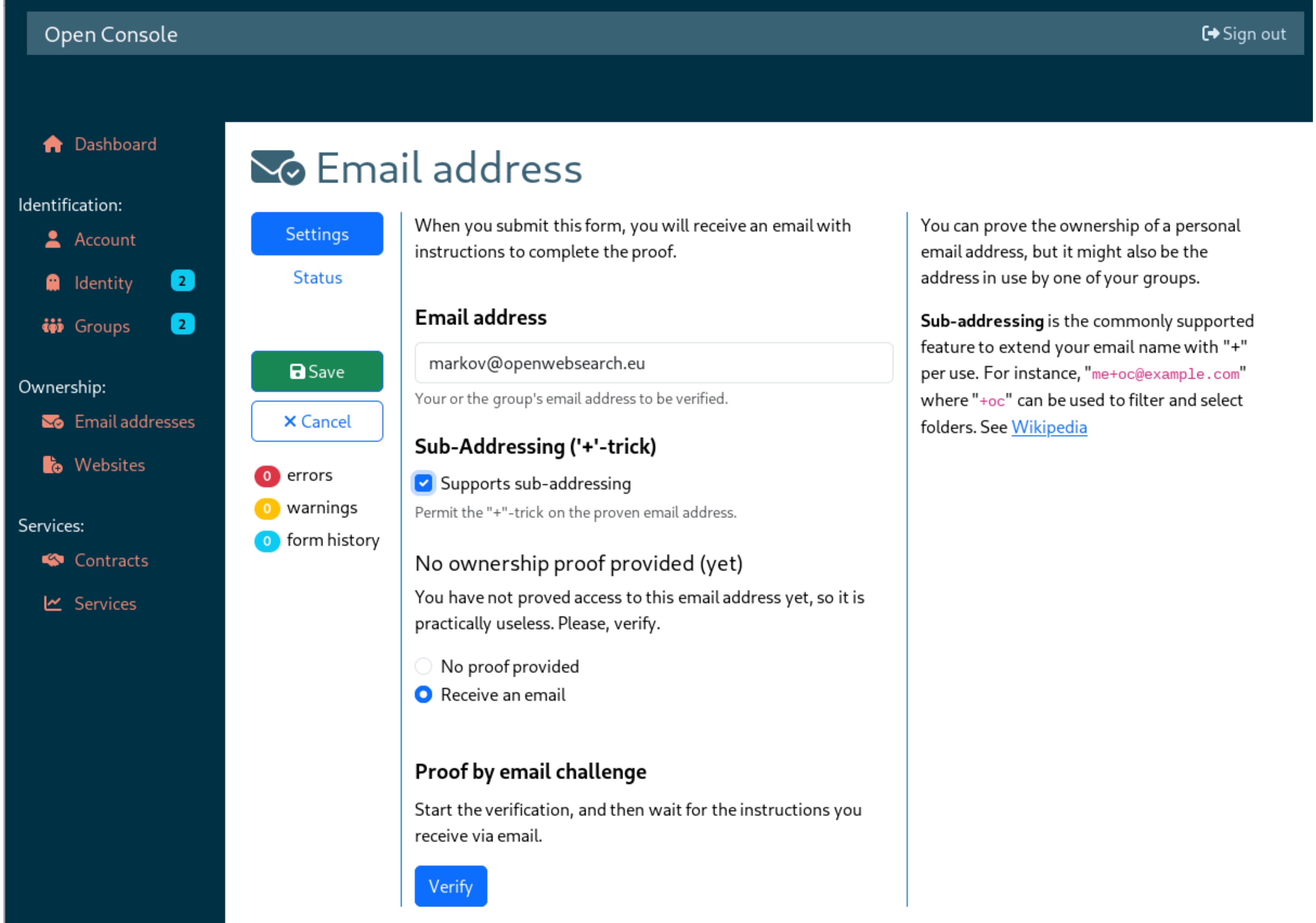
You may need to organize your activities as part of an organization, a company, or any other **group of people**. Therefore, you can create Group identities, where you can specify such cooperation.

in

Level of integration



Collecting proofs



Email address

When you submit this form, you will receive an email with instructions to complete the proof.

Email address

markov@openwebsearch.eu

Your or the group's email address to be verified.

Sub-Addressing ('+'-trick)

☑ Supports sub-addressing

Permit the "+"-trick on the proven email address.

No ownership proof provided (yet)

You have not proved access to this email address yet, so it is practically useless. Please, verify.

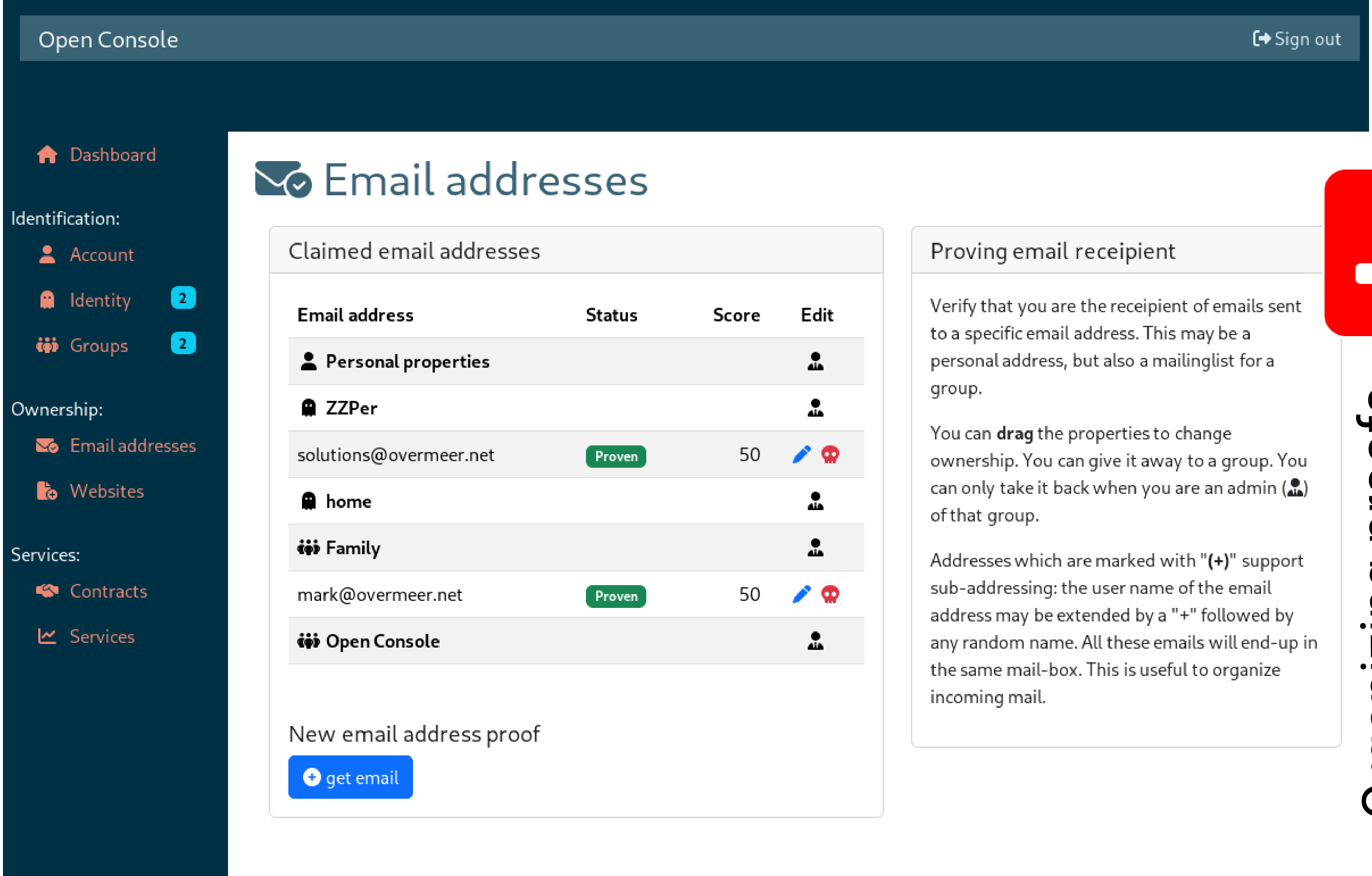
○ No proof provided
● Receive an email

Proof by email challenge

Start the verification, and then wait for the instructions you receive via email.

You can prove the ownership of a personal email address, but it might also be the address in use by one of your groups.

Sub-addressing is the commonly supported feature to extend your email name with "+" per use. For instance, "`me+oc@example.com`" where "`+oc`" can be used to filter and select folders. See Wikipedia



Open Console

Email addresses

Claimed email addresses

Email address	Status	Score	Edit
Personal properties			👤
ZZPer			👤
solutions@overmeer.net	Proven	50	✎ ☠
home			👤
Family			👤
mark@overmeer.net	Proven	50	✎ ☠
Open Console			👤

New email address proof

Proving email receipient

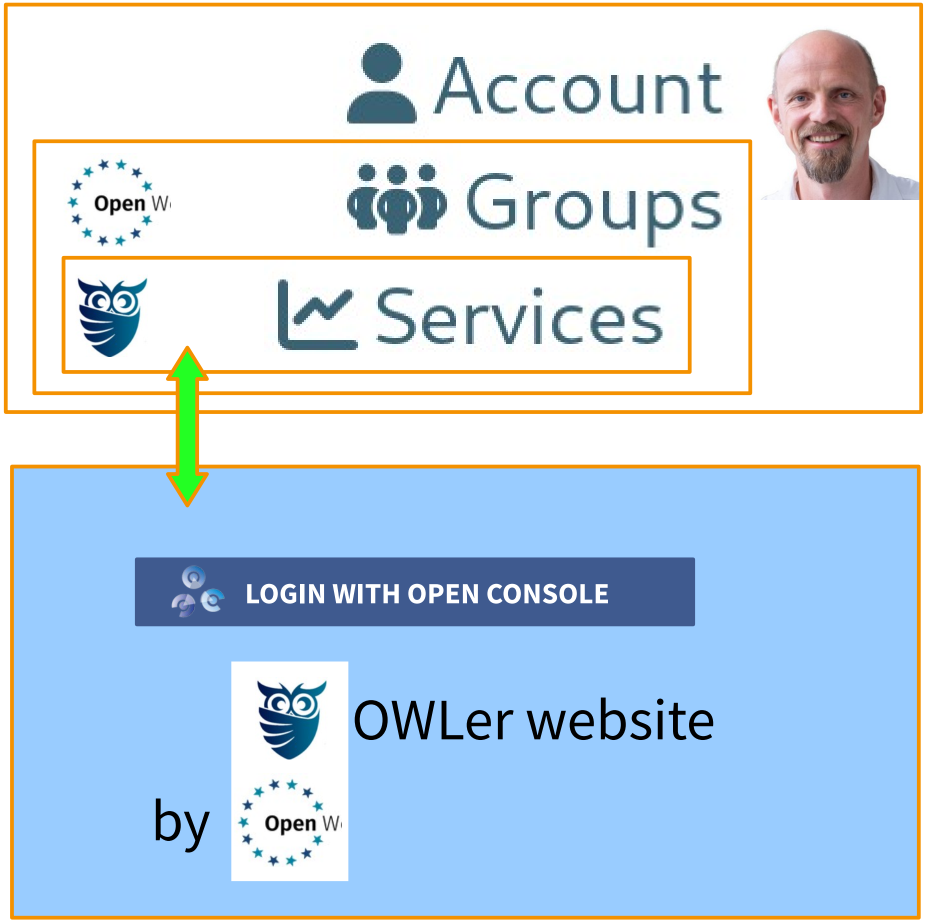
Verify that you are the receipient of emails sent to a specific email address. This may be a personal address, but also a mailinglist for a group.

You can **drag** the properties to change ownership. You can give it away to a group. You can only take it back when you are an admin (👤) of that group.

Addresses which are marked with "**(+)**" support sub-addressing: the user name of the email address may be extended by a "+" followed by any random name. All these emails will end-up in the same mail-box. This is useful to organize incoming mail.

Organizing proofs

Example



Account

Groups

Services

LOGIN WITH OPEN CONSOLE

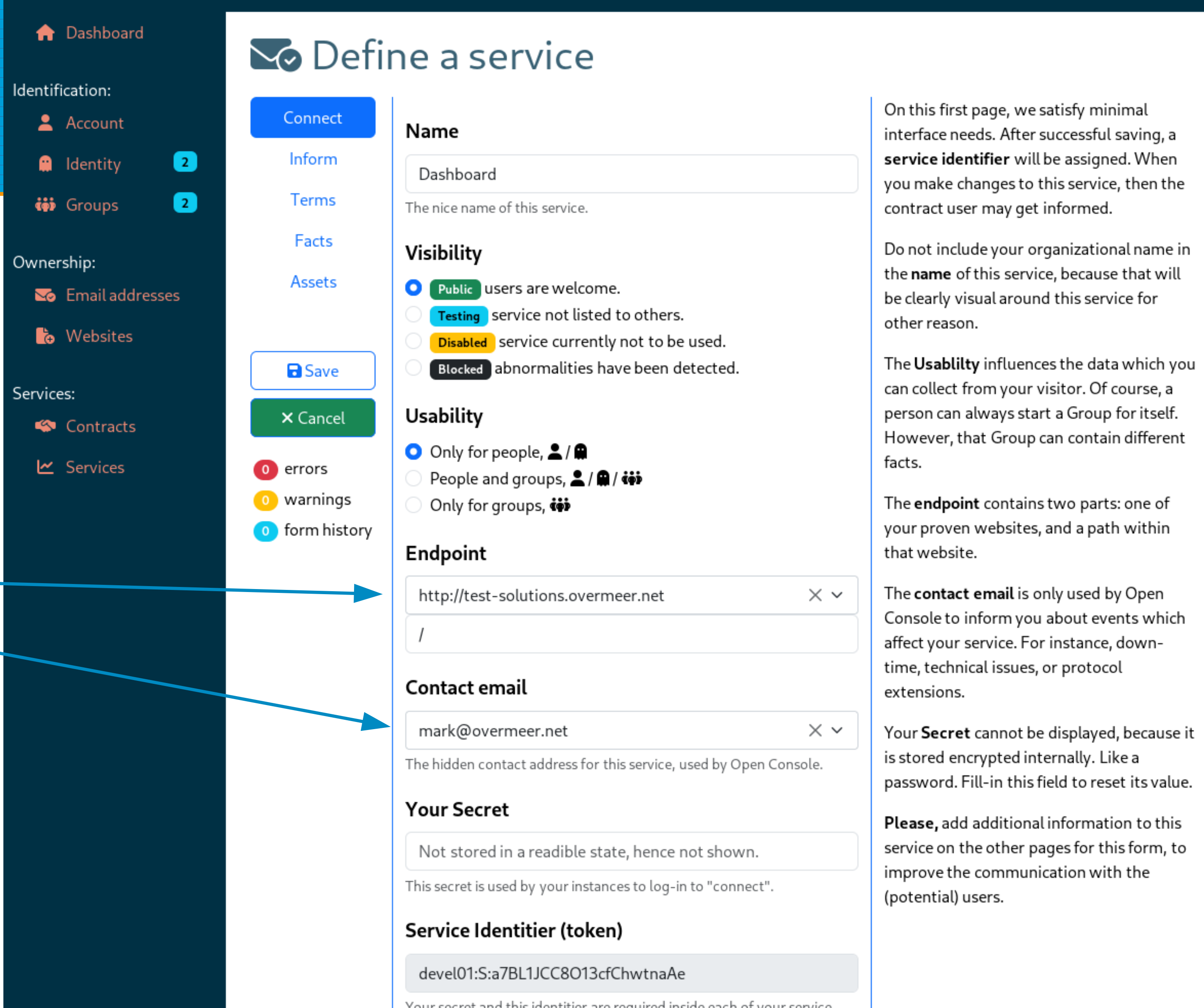
OWLer website

by

step 1

Define your service.

proven
elements
only!



Define a service

Name

Dashboard

The nice name of this service.

Visibility

● Public users are welcome.
○ Testing service not listed to others.
○ Disabled service currently not to be used.
○ Blocked abnormalities have been detected.

Usability

● Only for people, 👤 / 👻
○ People and groups, 👤 / 👻 / 👪
○ Only for groups, 👪

Endpoint

http://test-solutions.overmeer.net

/

Contact email

mark@overmeer.net

The hidden contact address for this service, used by Open Console.

Your Secret

Not stored in a readible state, hence not shown.

This secret is used by your instances to log-in to "connect".

Service Identitier (token)

devel01:S:a7BL1JCC8O13cfChwtnaAe

Your secret and this identitier are required inside each of your service

On this first page, we satisfy minimal interface needs. After successful saving, a **service identifier** will be assigned. When you make changes to this service, then the contract user may get informed.

Do not include your organizational name in the **name** of this service, because that will be clearly visual around this service for other reason.

The **Usablilty** influences the data which you can collect from your visitor. Of course, a person can always start a Group for itself. However, that Group can contain different facts.

The **endpoint** contains two parts: one of your proven websites, and a path within that website.

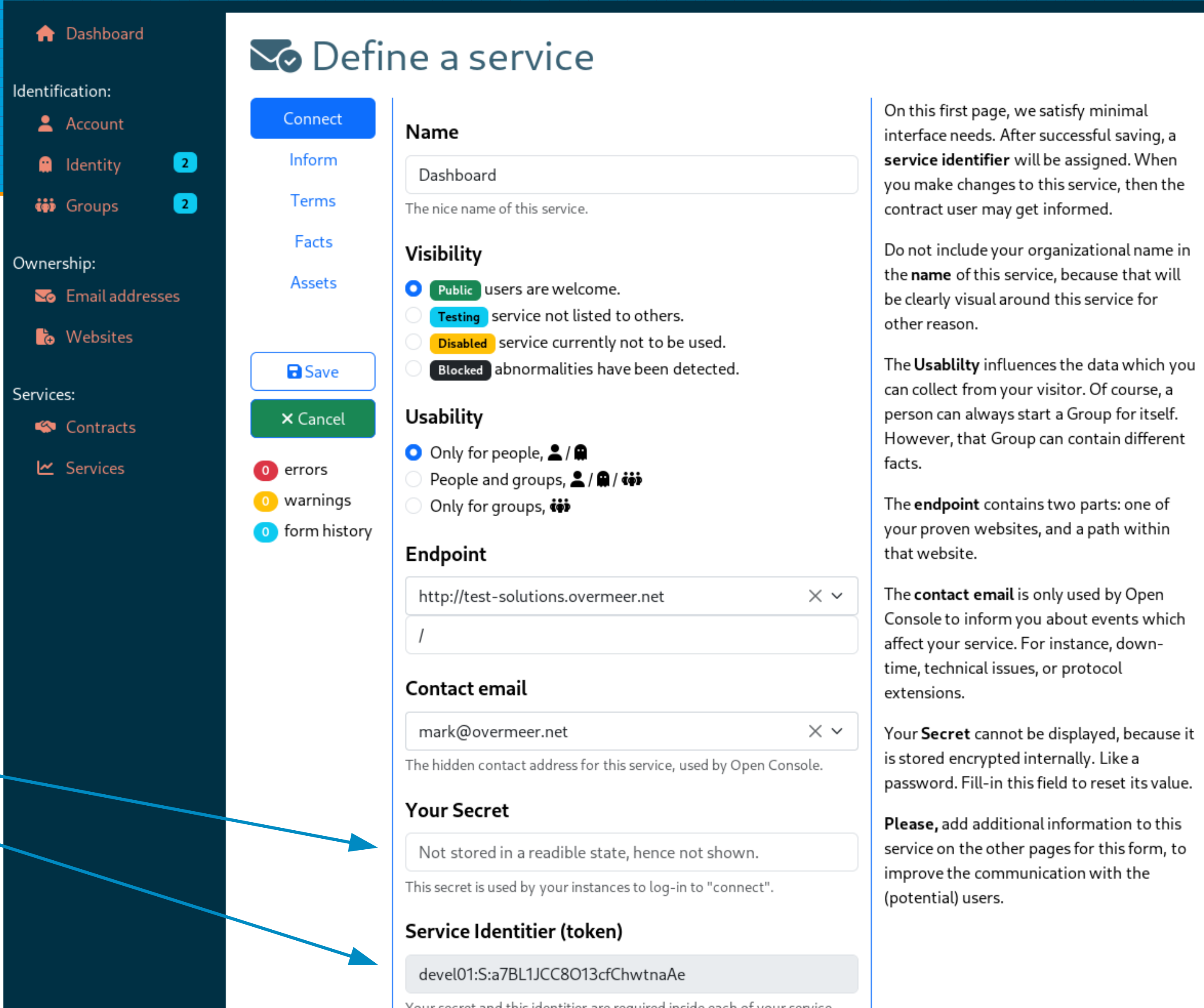
The **contact email** is only used by Open Console to inform you about events which affect your service. For instance, down-time, technical issues, or protocol extensions.

Your **Secret** cannot be displayed, because it is stored encrypted internally. Like a password. Fill-in this field to reset its value.

Please, add additional information to this service on the other pages for this form, to improve the communication with the (potential) users.

Step 1: Define your service.

OAuth secrets



Dashboard

Identification:

- Account
- Identity 2
- Groups 2

Ownership:

- Email addresses
- Websites

Services:

- Contracts
- Services

Define a service

Connect

Inform

Terms

Facts

Assets

Save

✕ Cancel

0 errors

0 warnings

0 form history

Name

Dashboard

The nice name of this service.

Visibility

● Public users are welcome.

○ Testing service not listed to others.

○ Disabled service currently not to be used.

○ Blocked abnormalities have been detected.

Usability

● Only for people, 👤/👻

○ People and groups, 👤/👻/👥

○ Only for groups, 👥

Endpoint

http://test-solutions.overmeer.net

/

Contact email

mark@overmeer.net

The hidden contact address for this service, used by Open Console.

Your Secret

Not stored in a readible state, hence not shown.

This secret is used by your instances to log-in to "connect".

Service Identitier (token)

devel01:S:a7BL1JCC8O13cfChwtnaAe

Your secret and this identifier are required inside each of your service

On this first page, we satisfy minimal interface needs. After successful saving, a **service identifier** will be assigned. When you make changes to this service, then the contract user may get informed.

Do not include your organizational name in the **name** of this service, because that will be clearly visual around this service for other reason.

The **Usablilty** influences the data which you can collect from your visitor. Of course, a person can always start a Group for itself. However, that Group can contain different facts.

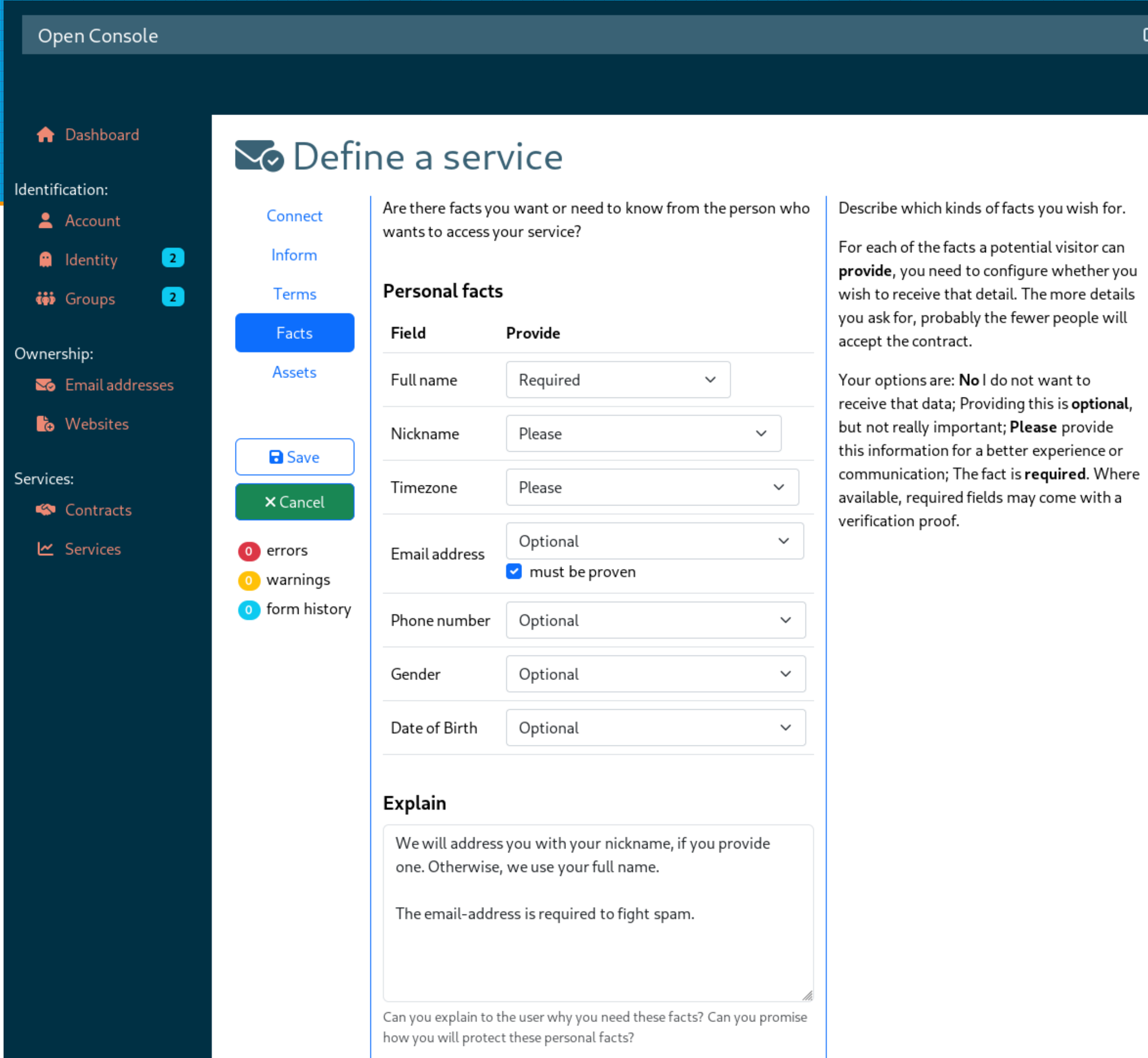
The **endpoint** contains two parts: one of your proven websites, and a path within that website.

The **contact email** is only used by Open Console to inform you about events which affect your service. For instance, down-time, technical issues, or protocol extensions.

Your **Secret** cannot be displayed, because it is stored encrypted internally. Like a password. Fill-in this field to reset its value.

Please, add additional information to this service on the other pages for this form, to improve the communication with the (potential) users.

Step 1



Define a service

Are there facts you want or need to know from the person who wants to access your service?

Personal facts

Field	Provide
Full name	Required
Nickname	Please
Timezone	Please
Email address	Optional ☑ must be proven
Phone number	Optional
Gender	Optional
Date of Birth	Optional

Explain

We will address you with your nickname, if you provide one. Otherwise, we use your full name.

The email-address is required to fight spam.

Can you explain to the user why you need these facts? Can you promise how you will protect these personal facts?

Describe which kinds of facts you wish for.

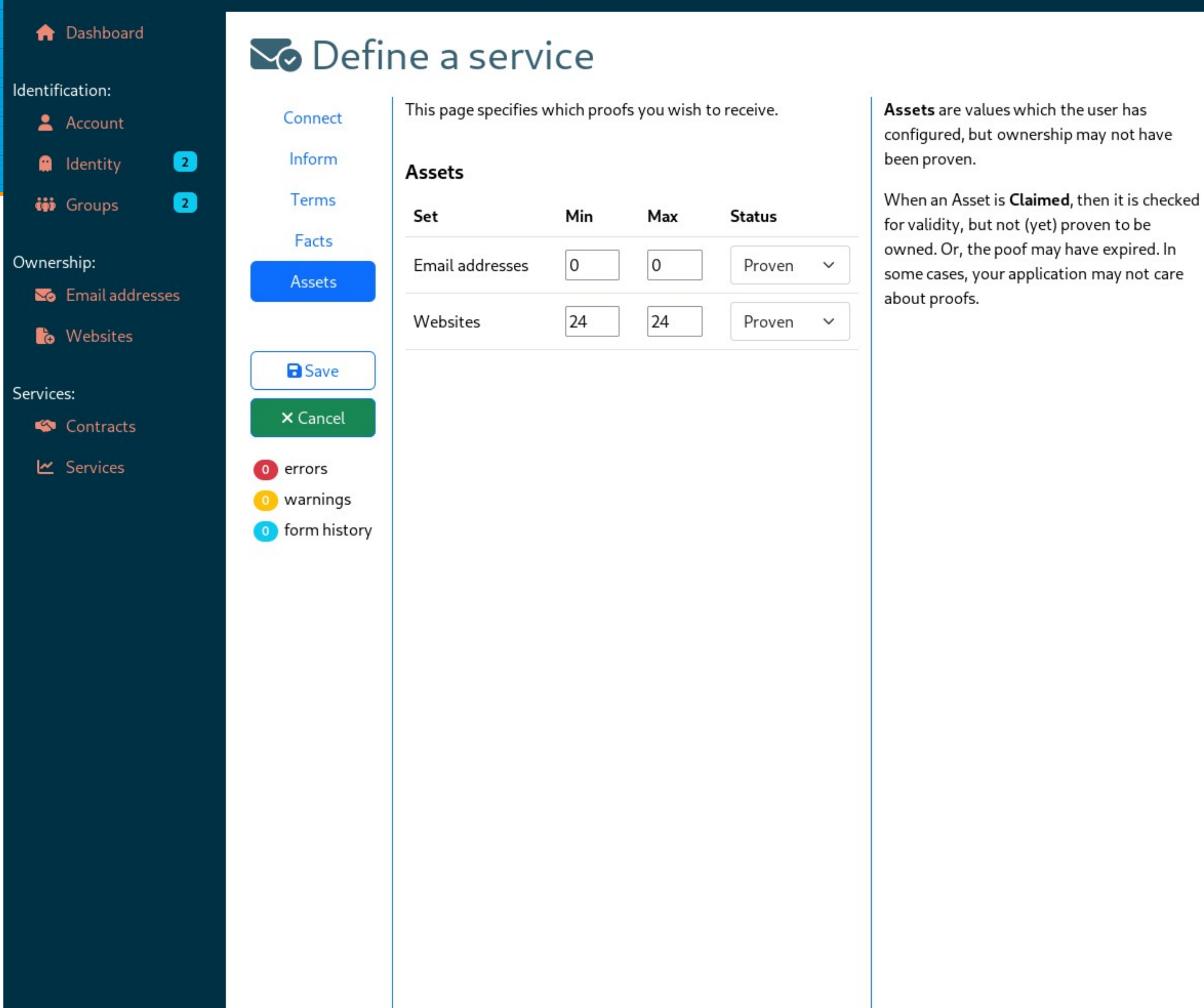
For each of the facts a potential visitor can **provide**, you need to configure whether you wish to receive that detail. The more details you ask for, probably the fewer people will accept the contract.

Your options are: **No** I do not want to receive that data; Providing this is **optional**, but not really important; **Please** provide this information for a better experience or communication; The fact is **required**. Where available, required fields may come with a verification proof.

Step 1

additional proofs

and other assets.



Define a service

This page specifies which proofs you wish to receive.

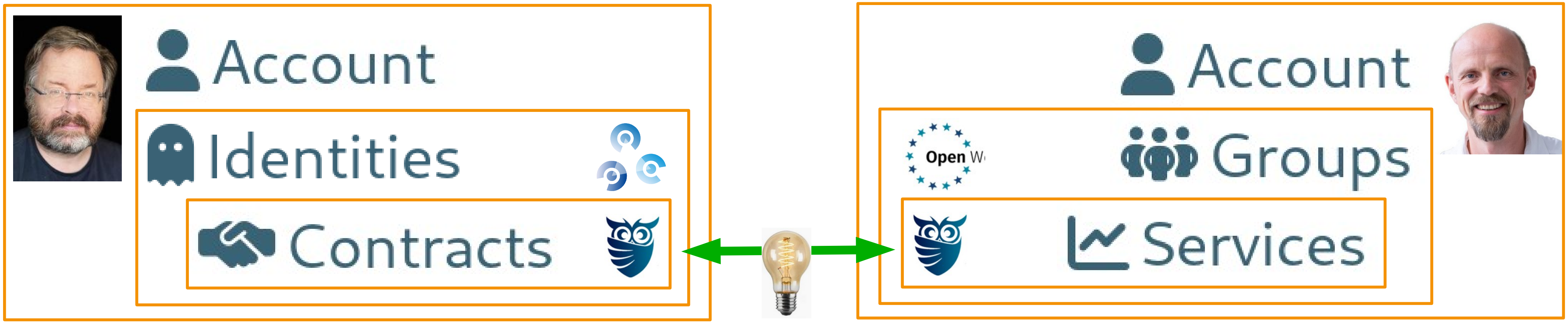
Assets

Set	Min	Max	Status
Email addresses	0	0	Proven
Websites	24	24	Proven

Assets are values which the user has configured, but ownership may not have been proven.

When an Asset is **Claimed**, then it is checked for validity, but not (yet) proven to be owned. Or, the poof may have expired. In some cases, your application may not care about proofs.

Example



Account

Identities

Contracts

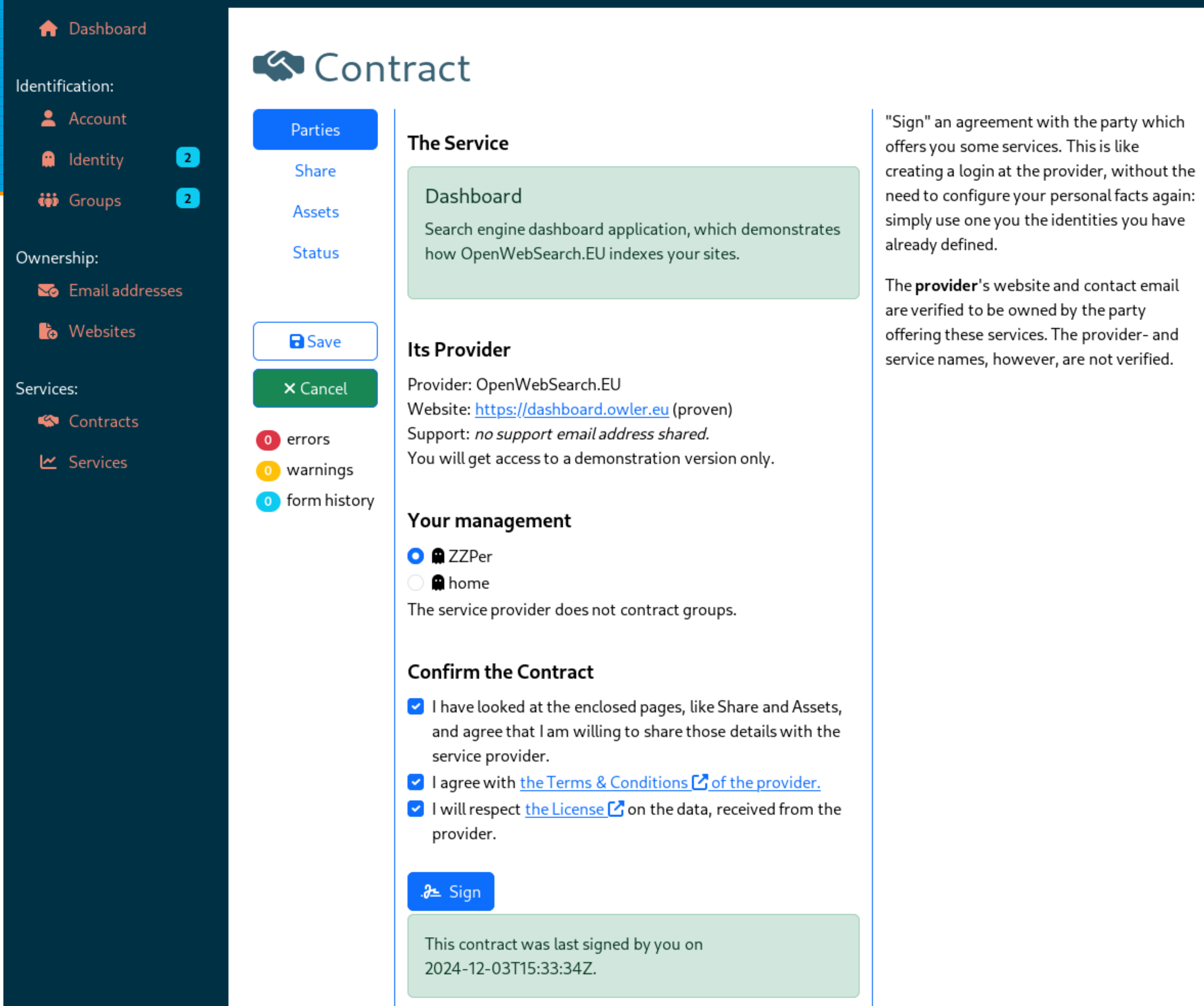
Account

Groups

Services

Step 2

User signs contract.



Contract

The Service

Dashboard

Search engine dashboard application, which demonstrates how OpenWebSearch.EU indexes your sites.

Its Provider

Provider: OpenWebSearch.EU
Website: https://dashboard.owler.eu (proven)
Support: *no support email address shared.*
You will get access to a demonstration version only.

Your management

● ZZPer
○ home

The service provider does not contract groups.

Confirm the Contract

☑ I have looked at the enclosed pages, like Share and Assets, and agree that I am willing to share those details with the service provider.

☑ I agree with the Terms & Conditions of the provider.

☑ I will respect the License on the data, received from the provider.

Sign

This contract was last signed by you on 2024-12-03T15:33:34Z.

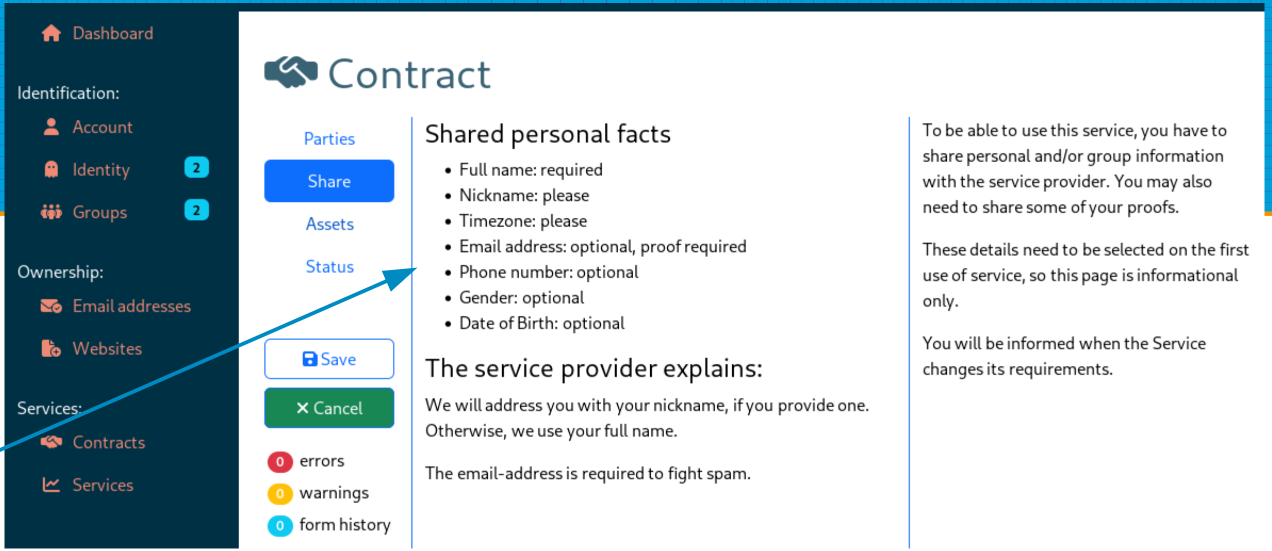
"Sign" an agreement with the party which offers you some services. This is like creating a login at the provider, without the need to configure your personal facts again: simply use one you the identities you have already defined.

The **provider**'s website and contact email are verified to be owned by the party offering these services. The provider- and service names, however, are not verified.

Step 2

User signs contract.

shows what data is requested



Contract

Shared personal facts

- Full name: required
- Nickname: please
- Timezone: please
- Email address: optional, proof required
- Phone number: optional
- Gender: optional
- Date of Birth: optional

The service provider explains:

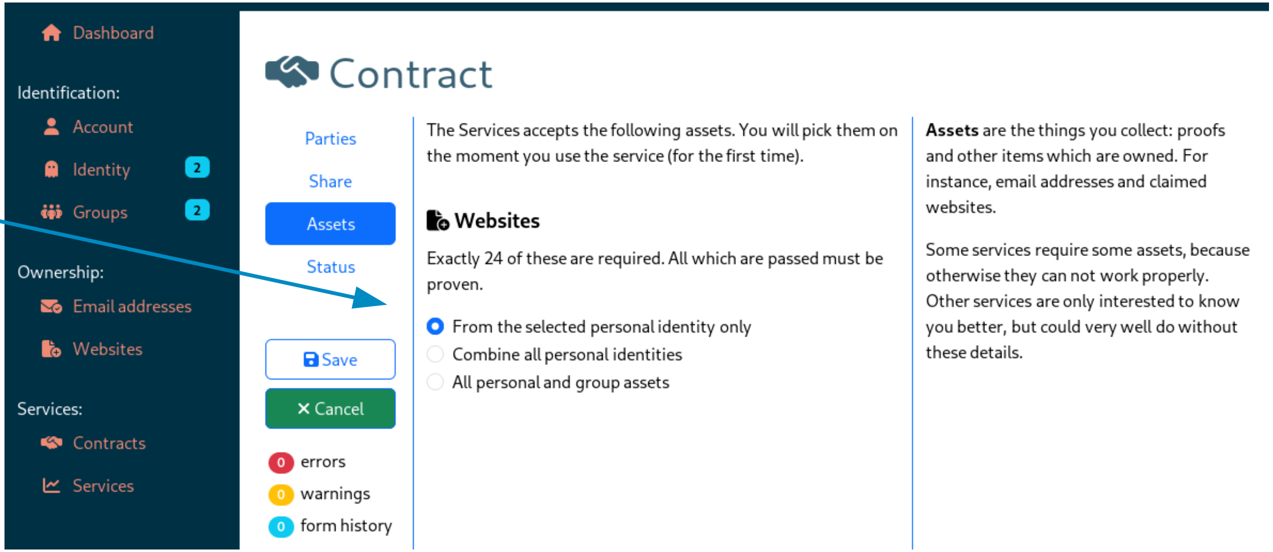
We will address you with your nickname, if you provide one. Otherwise, we use your full name.

The email-address is required to fight spam.

To be able to use this service, you have to share personal and/or group information with the service provider. You may also need to share some of your proofs.

These details need to be selected on the first use of service, so this page is informational only.

You will be informed when the Service changes its requirements.



Contract

The Services accepts the following assets. You will pick them on the moment you use the service (for the first time).

Websites

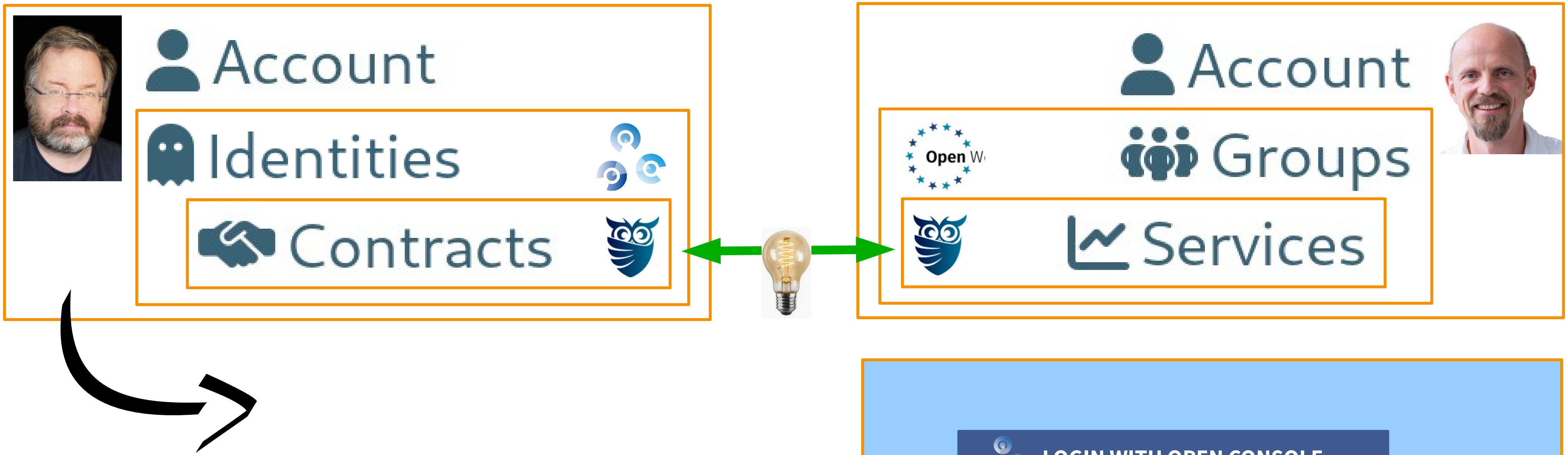
Exactly 24 of these are required. All which are passed must be proven.

● From the selected personal identity only
○ Combine all personal identities
○ All personal and group assets

Assets are the things you collect: proofs and other items which are owned. For instance, email addresses and claimed websites.

Some services require some assets, because otherwise they can not work properly. Other services are only interested to know you better, but could very well do without these details.

Example



Account

Identities

Contracts

Account

Groups

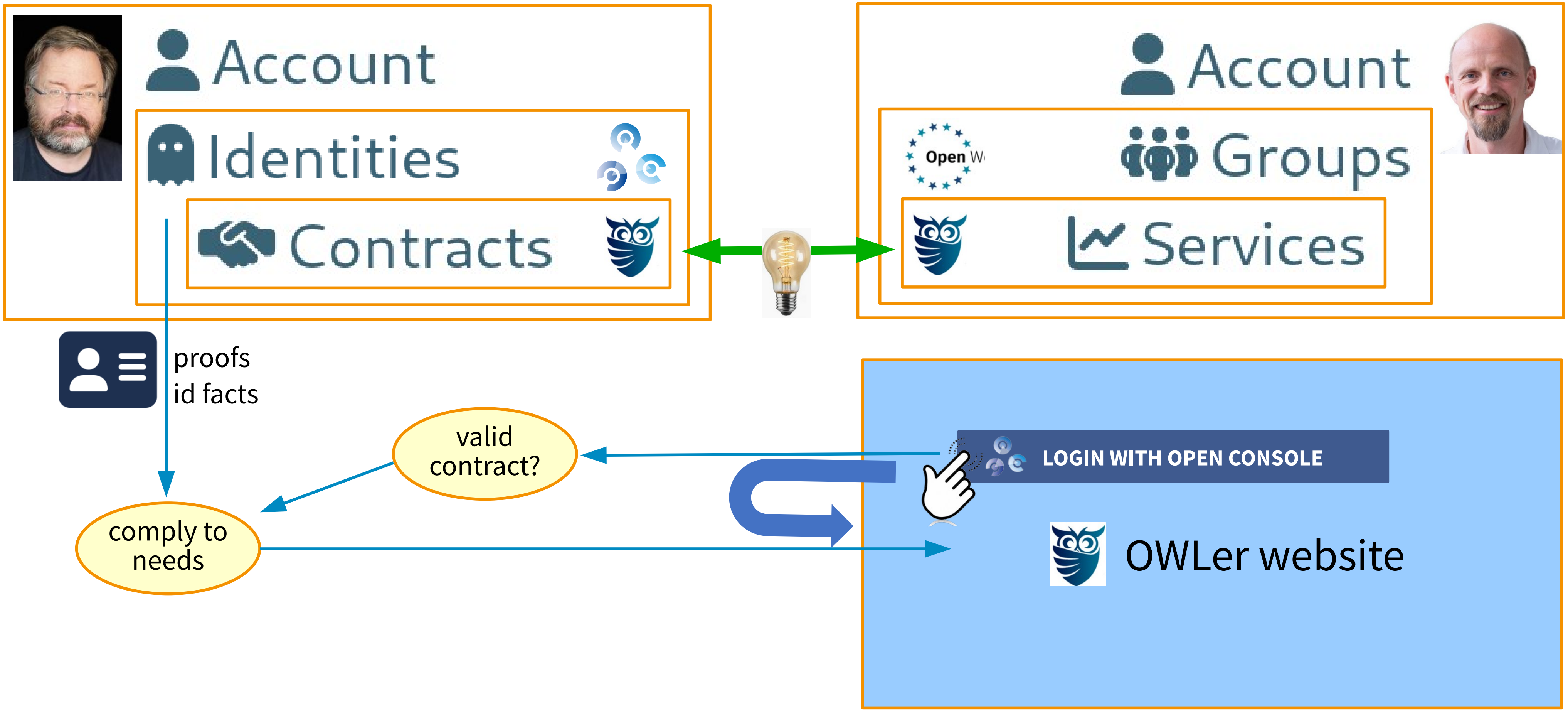
Services

LOGIN WITH OPEN CONSOLE

OWLer website

by

Example



Account

Identities

Contracts

Account

Open W

Groups

Services

proofs
id facts

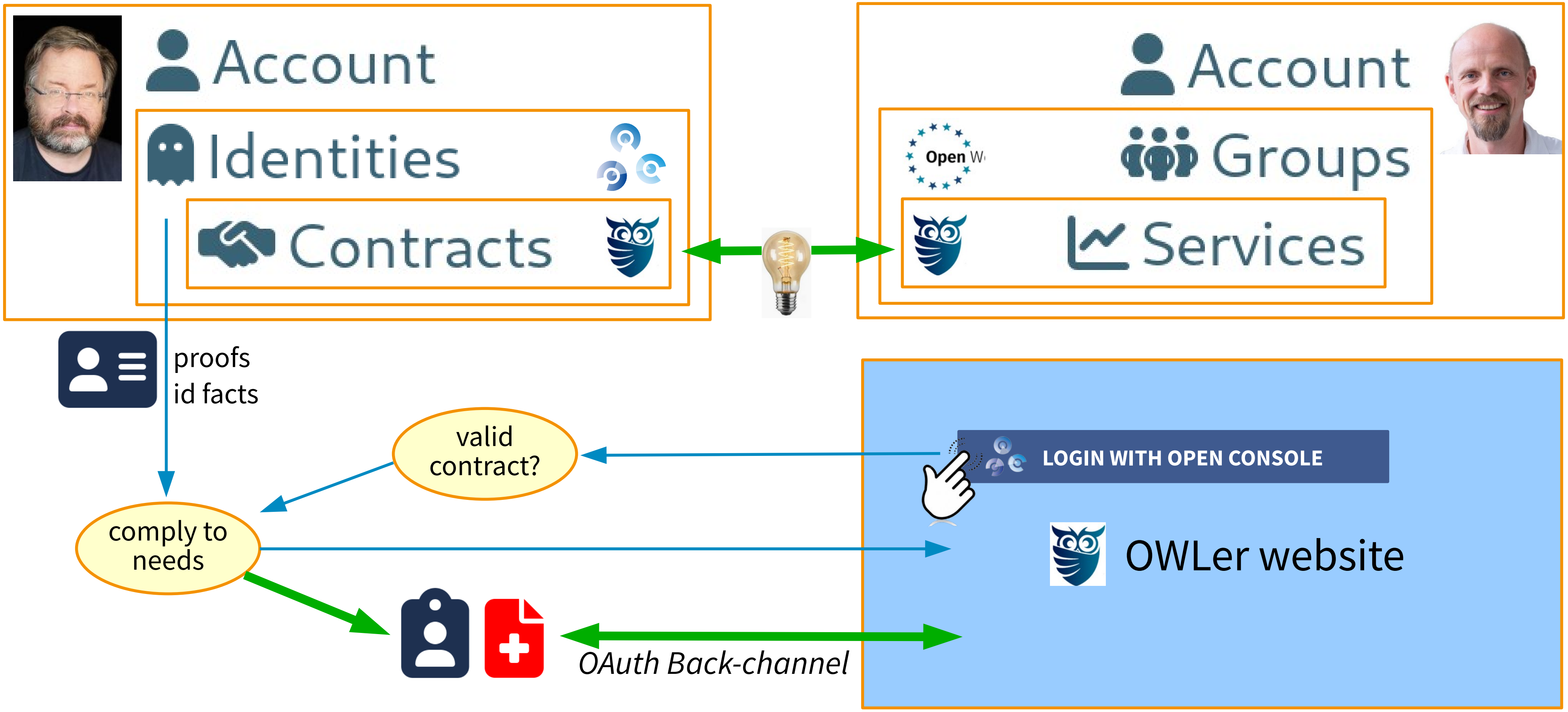
valid contract?

comply to needs

LOGIN WITH OPEN CONSOLE

OWLer website

Example



Account

Identities

Contracts

proofs
id facts

valid
contract?

comply to
needs

OAuth Back-channel

Account

Open W

Groups

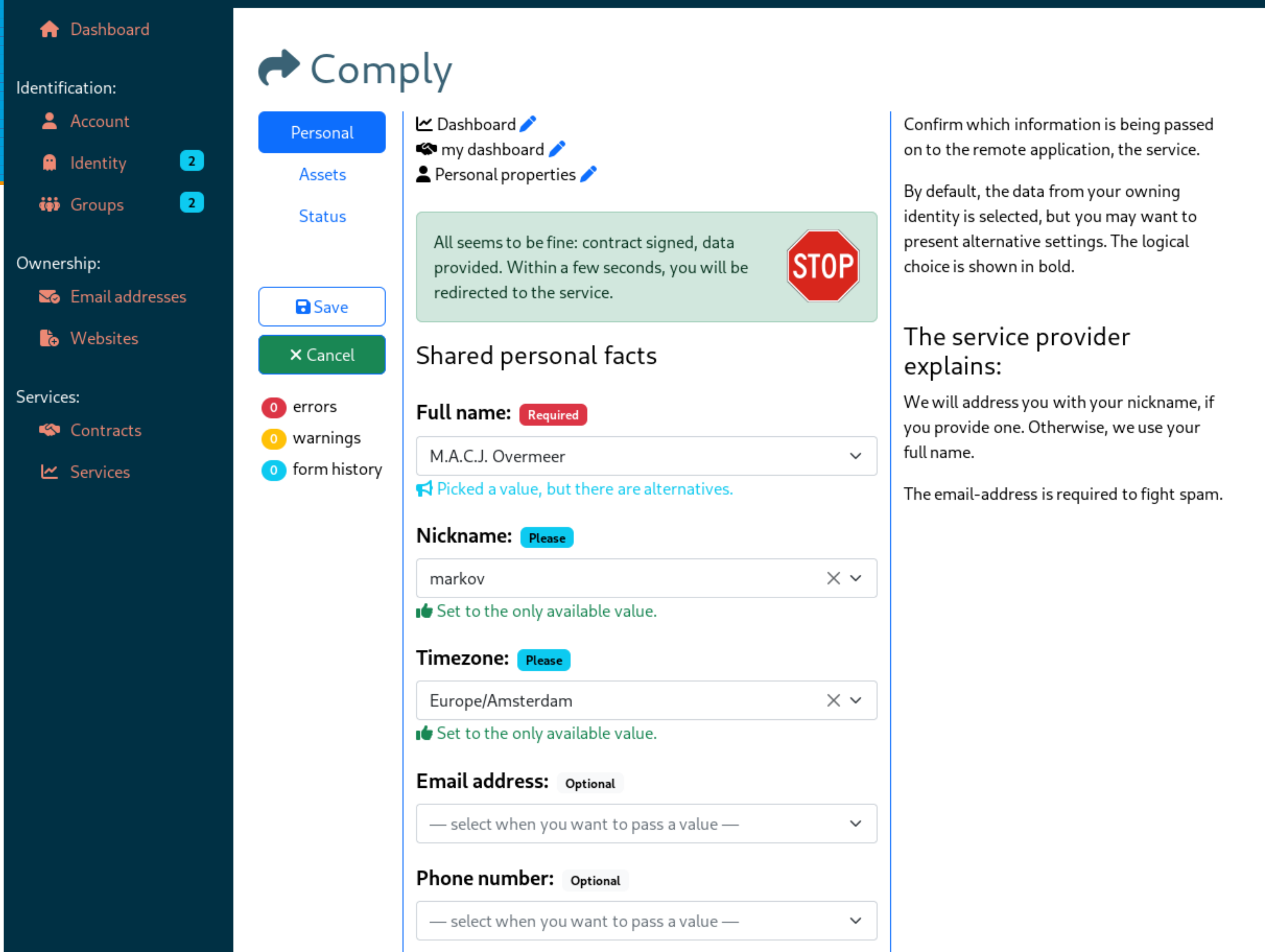
Services

LOGIN WITH OPEN CONSOLE

OWLer website

Step 3

Provide the info



Comply

Dashboard
my dashboard
Personal properties

All seems to be fine: contract signed, data provided. Within a few seconds, you will be redirected to the service. STOP

Shared personal facts

Full name: Required

M.A.C.J. Overmeer

Picked a value, but there are alternatives.

Nickname: Please

markov

Set to the only available value.

Timezone: Please

Europe/Amsterdam

Set to the only available value.

Email address: Optional

— select when you want to pass a value —

Phone number: Optional

— select when you want to pass a value —

Confirm which information is being passed on to the remote application, the service.

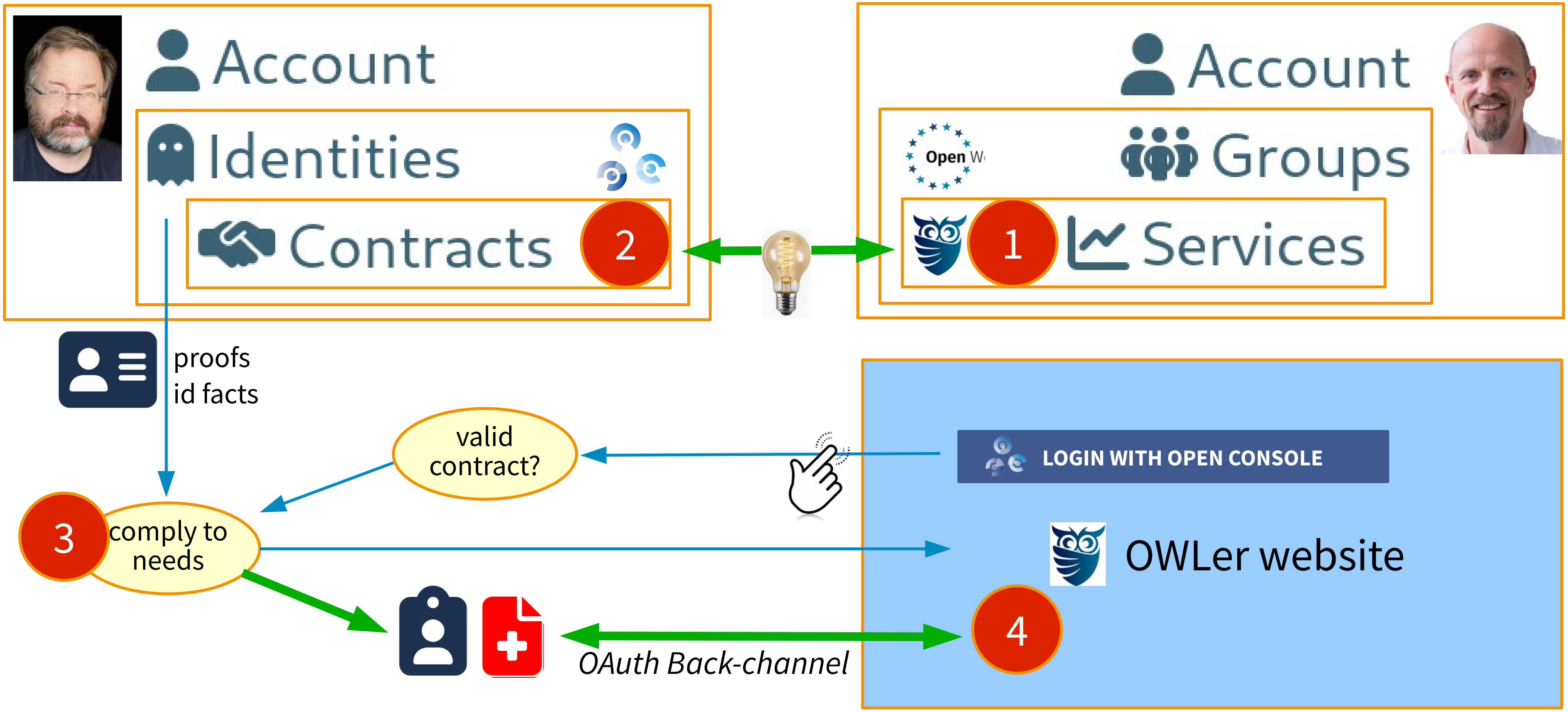
By default, the data from your owning identity is selected, but you may want to present alternative settings. The logical choice is shown in bold.

The service provider explains:

We will address you with your nickname, if you provide one. Otherwise, we use your full name.

The email-address is required to fight spam.

Example



Account

Identities

Contracts

2

Account

Open W

Groups

1

Services

proofs
id facts

valid contract?

LOGIN WITH OPEN CONSOLE

3

comply to needs

OWLer website

4

OAuth Back-channel

Step 4: OAuth Back-channel

- OpenID Connect

```
{
 "sub": "248289761001",
 "name": "Jane Doe",
 "given_name": "Jane",
 "family_name": "Doe",
 "preferred_username": "j.doe",
 "email": "janedoe@example.com",
 "picture": "http://example.com/me.jpg"
}
```

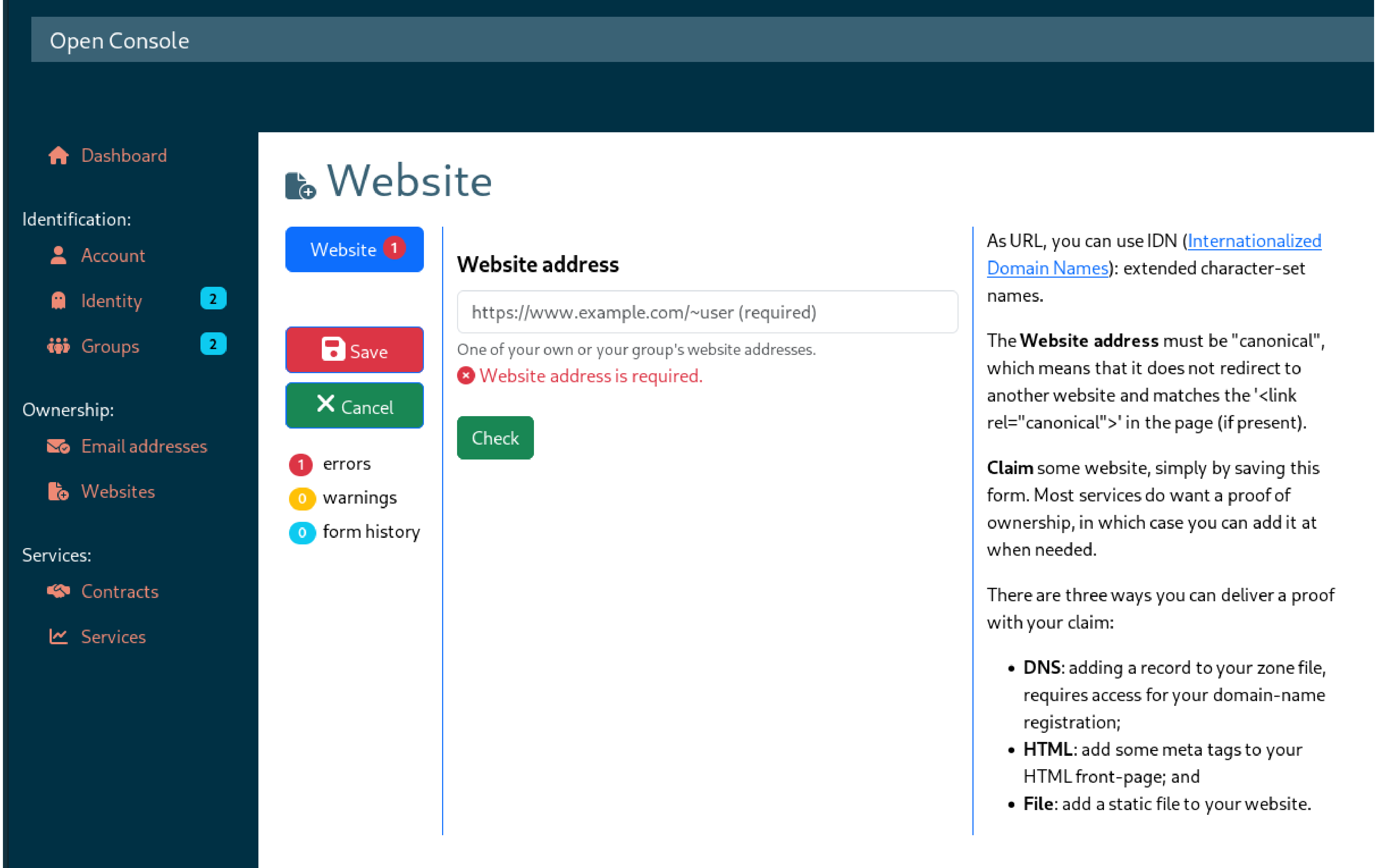
- "Open Console Connect"

```
{
    'id': 'WDJ@OI@JOJiqjodihohOhoh',
    'service':  {
       'websites': [ 'https://www.doe.com' ],
       'version': '2021v1'
    },
    'account': {            # selected facts of the Account
       'created': '2022-12-21T15:34:12Z',
       'oc_instance': '001'
    },
    'person': {             # selected facts of an Identity
       'name': 'John Doe',
       'email': [ 'joe@doe.com', 'joe@example.com' ]
    },
    'group': {              # selected facts of a group
    },
    'contract': {
        'id': 'xyz:C:WDJ@OI@JOJWqjqljdoiqjodihohOhoh',
        'created': '2022-12-21T15:34:12Z',
        'signed': '2024-07-21T15:36:12Z'
    },
    'proofs': [ ... ]
  }
```

Additional proofs

- Website ownership
- Domain ownership
- Network ownership
- …

Website proofs



Website

Website address

https://www.example.com/~user (required)

One of your own or your group's website addresses.

Website address is required.

As URL, you can use IDN (Internationalized Domain Names): extended character-set names.

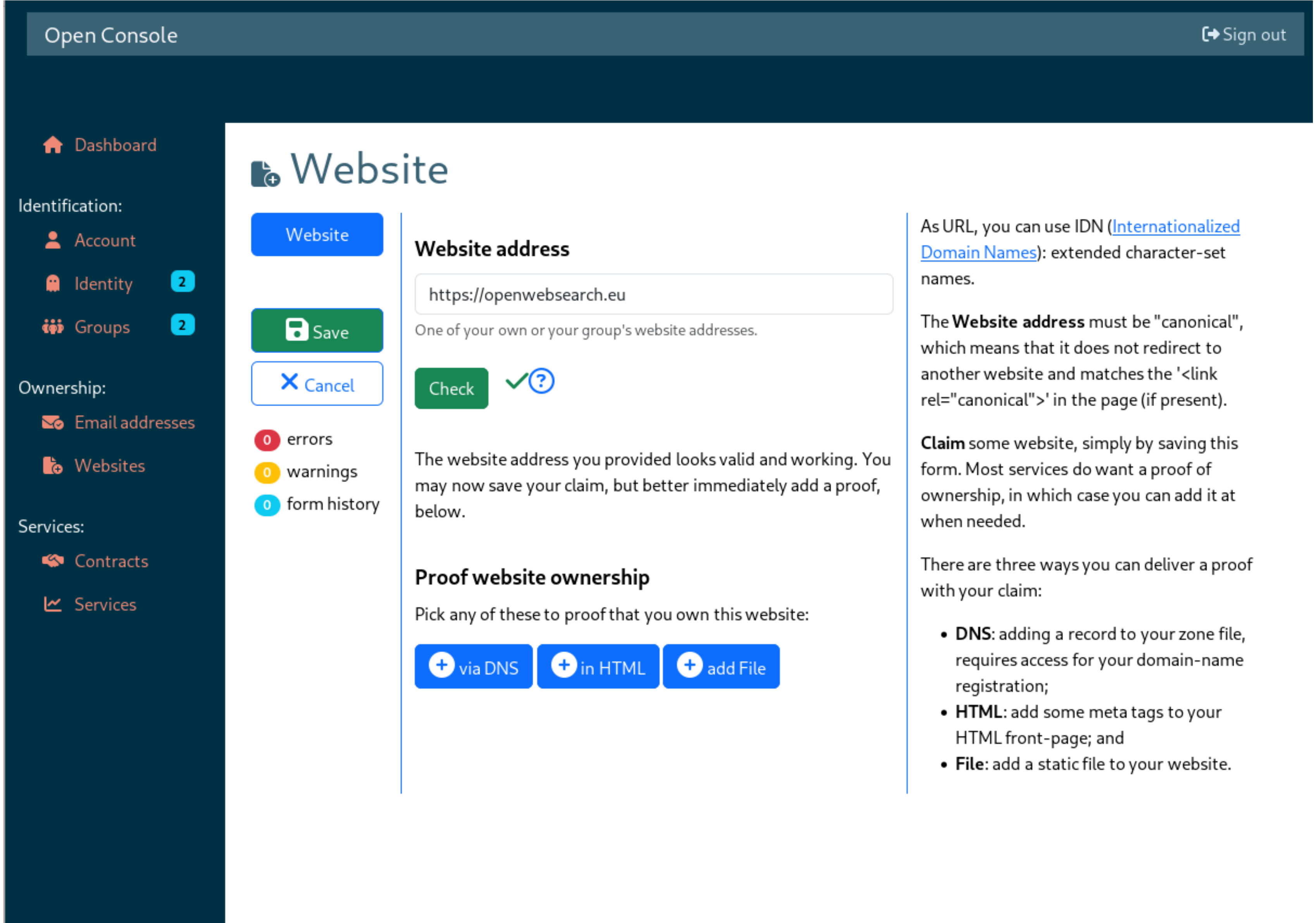
The **Website address** must be "canonical", which means that it does not redirect to another website and matches the '<link rel="canonical">' in the page (if present).

Claim some website, simply by saving this form. Most services do want a proof of ownership, in which case you can add it at when needed.

There are three ways you can deliver a proof with your claim:

- **DNS**: adding a record to your zone file, requires access for your domain-name registration;
- **HTML**: add some meta tags to your HTML front-page; and
- **File**: add a static file to your website.

Website proofs



Website

Website address

https://openwebsearch.eu

One of your own or your group's website addresses.

The website address you provided looks valid and working. You may now save your claim, but better immediately add a proof, below.

Proof website ownership

Pick any of these to proof that you own this website:

As URL, you can use IDN (Internationalized Domain Names): extended character-set names.

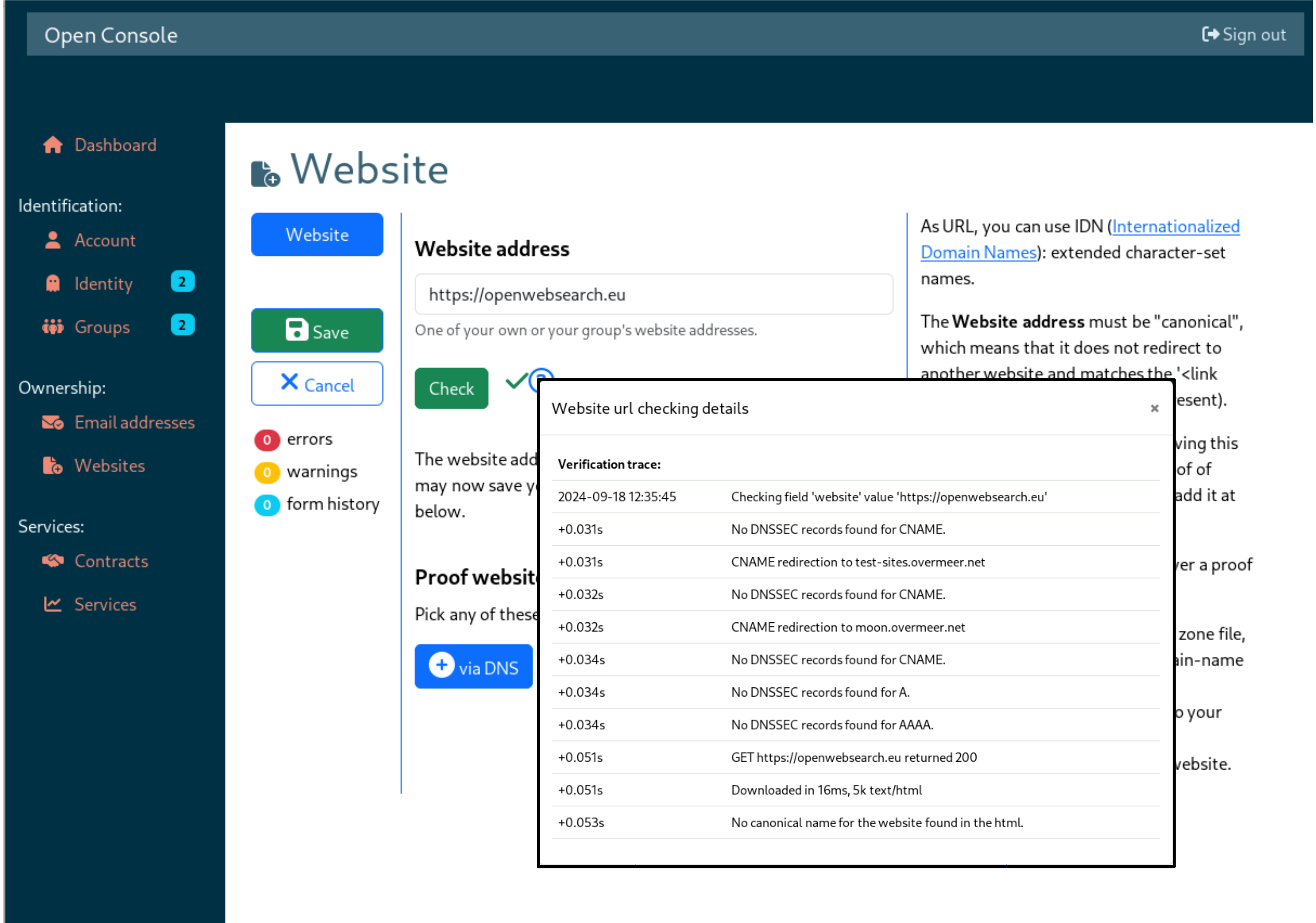
The **Website address** must be "canonical", which means that it does not redirect to another website and matches the '<link rel="canonical">' in the page (if present).

Claim some website, simply by saving this form. Most services do want a proof of ownership, in which case you can add it at when needed.

There are three ways you can deliver a proof with your claim:

- **DNS**: adding a record to your zone file, requires access for your domain-name registration;
- **HTML**: add some meta tags to your HTML front-page; and
- **File**: add a static file to your website.

Website proofs



Open Console

Website

0 errors
0 warnings
0 form history

Website address

https://openwebsearch.eu

One of your own or your group's website addresses.

The website add
may now save y
below.

Proof websit

Pick any of these

As URL, you can use IDN (Internationalized Domain Names): extended character-set names.

The **Website address** must be "canonical", which means that it does not redirect to another website and matches the '<link
esent).

ving this
of of
add it at

ver a proof

zone file,
ain-name

o your

vebsite.

Website url checking details ×

Verification trace:

2024-09-18 12:35:45	Checking field 'website' value 'https://openwebsearch.eu'
+0.031s	No DNSSEC records found for CNAME.
+0.031s	CNAME redirection to test-sites.overmeer.net
+0.032s	No DNSSEC records found for CNAME.
+0.032s	CNAME redirection to moon.overmeer.net
+0.034s	No DNSSEC records found for CNAME.
+0.034s	No DNSSEC records found for A.
+0.034s	No DNSSEC records found for AAAA.
+0.051s	GET https://openwebsearch.eu returned 200
+0.051s	Downloaded in 16ms, 5k text/html
+0.053s	No canonical name for the website found in the html.

Website URL complications

Is this a top?

- http://www.abc.nl/~user/xyz.html
- Redirects: http → https, .nl → .com
- Redirects: www.xyz.nl → xyz.nl
- <link rel="canonical">
- Public Suffix List

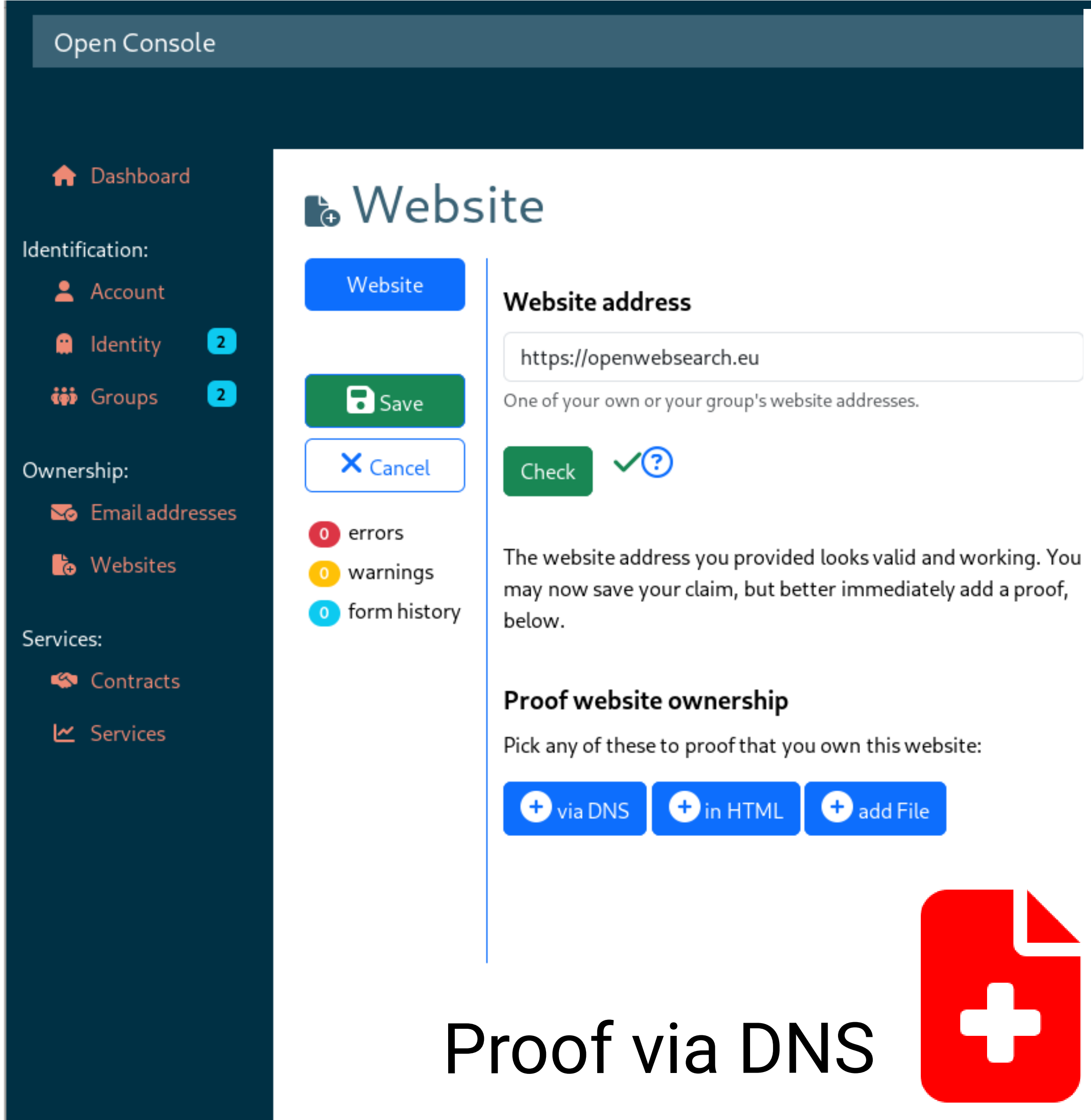
- Redirects: ibm.com → ibm.com/nl-NL **NO**

Website URL complications

Normalization:

- Remove fragments (#) and queries (?)
- IDNA2008 (Punycode)
- www.räksmörgås.se → www.xn—rksmrgs-5wao1o.se
- Character normalization: `%43 → C`
- UTF8 HEX encoding normalization: `ä → %72%E4`
- Defaults: `http://abc.nl:80 == http://abc.nl`
- Casing: `HTTP://ABC.NL == http://abc.nl`

Proof via DNS



Website

Website address

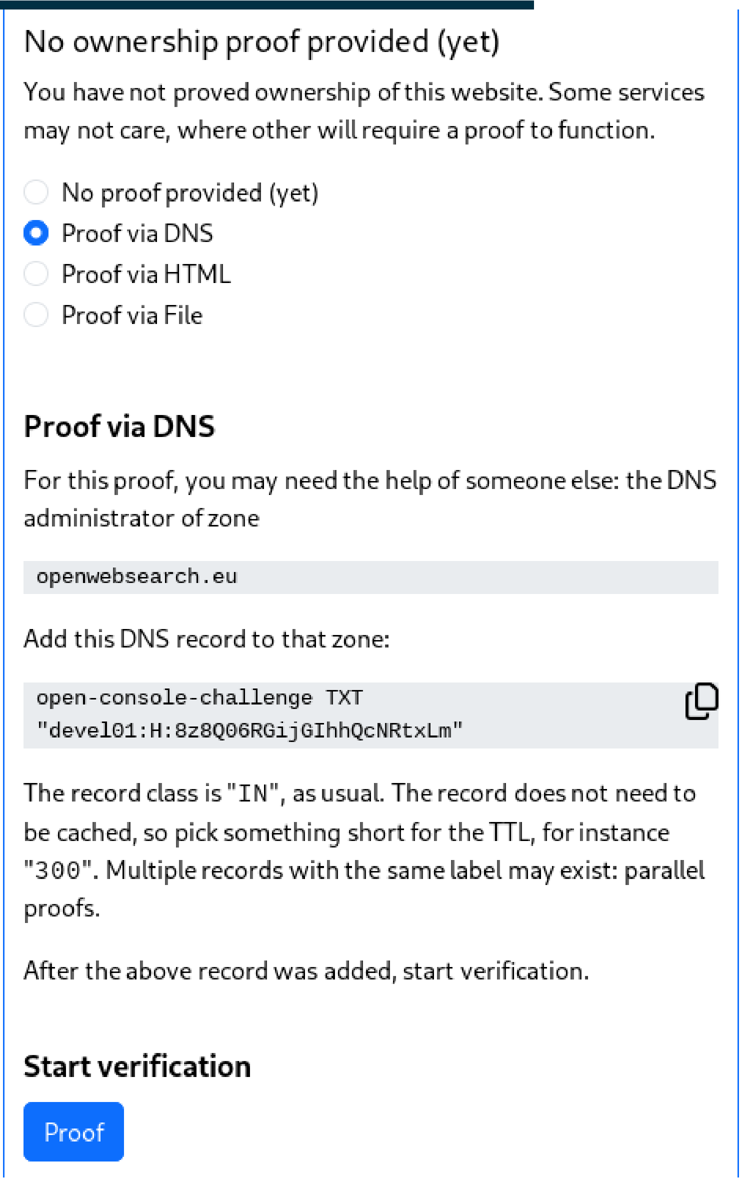
https://openwebsearch.eu

One of your own or your group's website addresses.

The website address you provided looks valid and working. You may now save your claim, but better immediately add a proof, below.

Proof website ownership

Pick any of these to proof that you own this website:



No ownership proof provided (yet)

You have not proved ownership of this website. Some services may not care, where other will require a proof to function.

- ○ No proof provided (yet)
- ● Proof via DNS
- ○ Proof via HTML
- ○ Proof via File

Proof via DNS

For this proof, you may need the help of someone else: the DNS administrator of zone

```
openwebsearch.eu
```

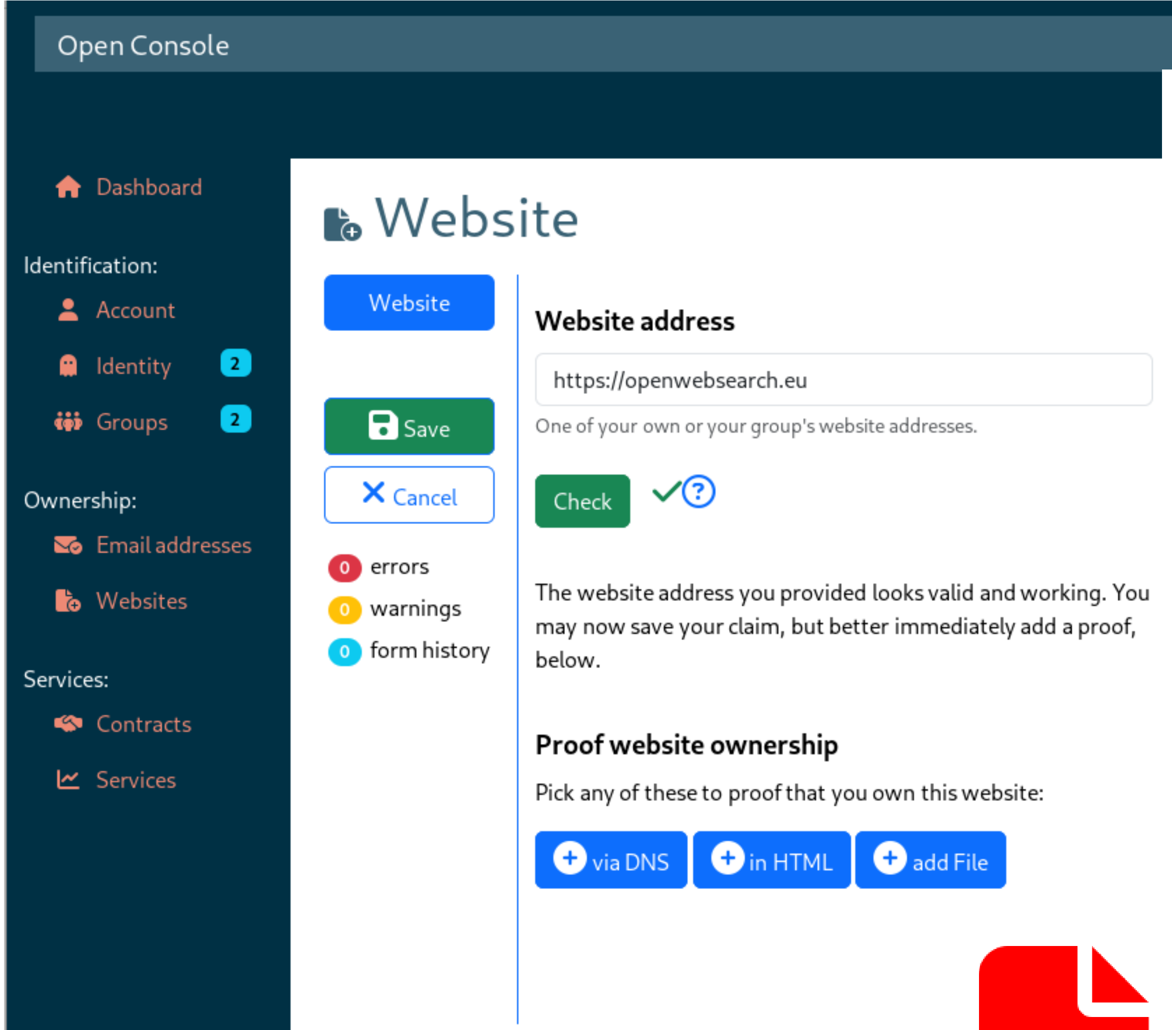
Add this DNS record to that zone:

```
open-console-challenge TXT
"devel01:H:8z8Q06RGijGIhhQcNRtxLm"
```

The record class is "IN", as usual. The record does not need to be cached, so pick something short for the TTL, for instance "300". Multiple records with the same label may exist: parallel proofs.

After the above record was added, start verification.

Start verification



Website

0 errors
0 warnings
0 form history

Website address

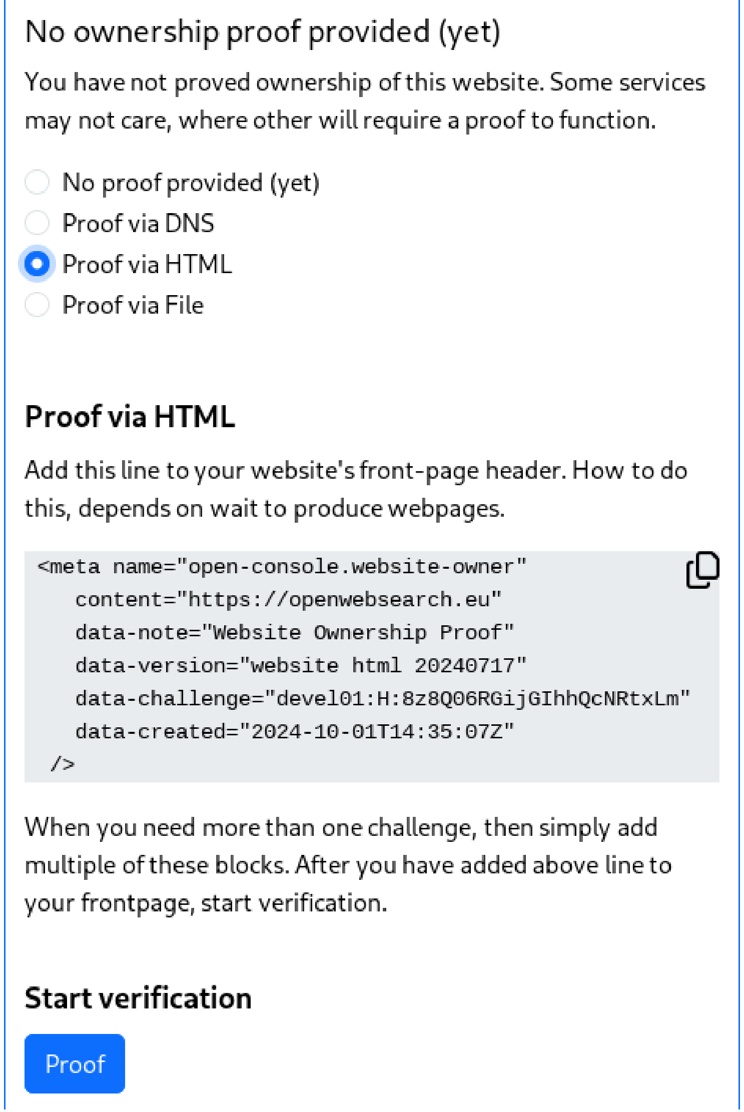
https://openwebsearch.eu

One of your own or your group's website addresses.

The website address you provided looks valid and working. You may now save your claim, but better immediately add a proof, below.

Proof website ownership

Pick any of these to proof that you own this website:



No ownership proof provided (yet)

You have not proved ownership of this website. Some services may not care, where other will require a proof to function.

○ No proof provided (yet)
○ Proof via DNS
● Proof via HTML
○ Proof via File

Proof via HTML

Add this line to your website's front-page header. How to do this, depends on wait to produce webpages.

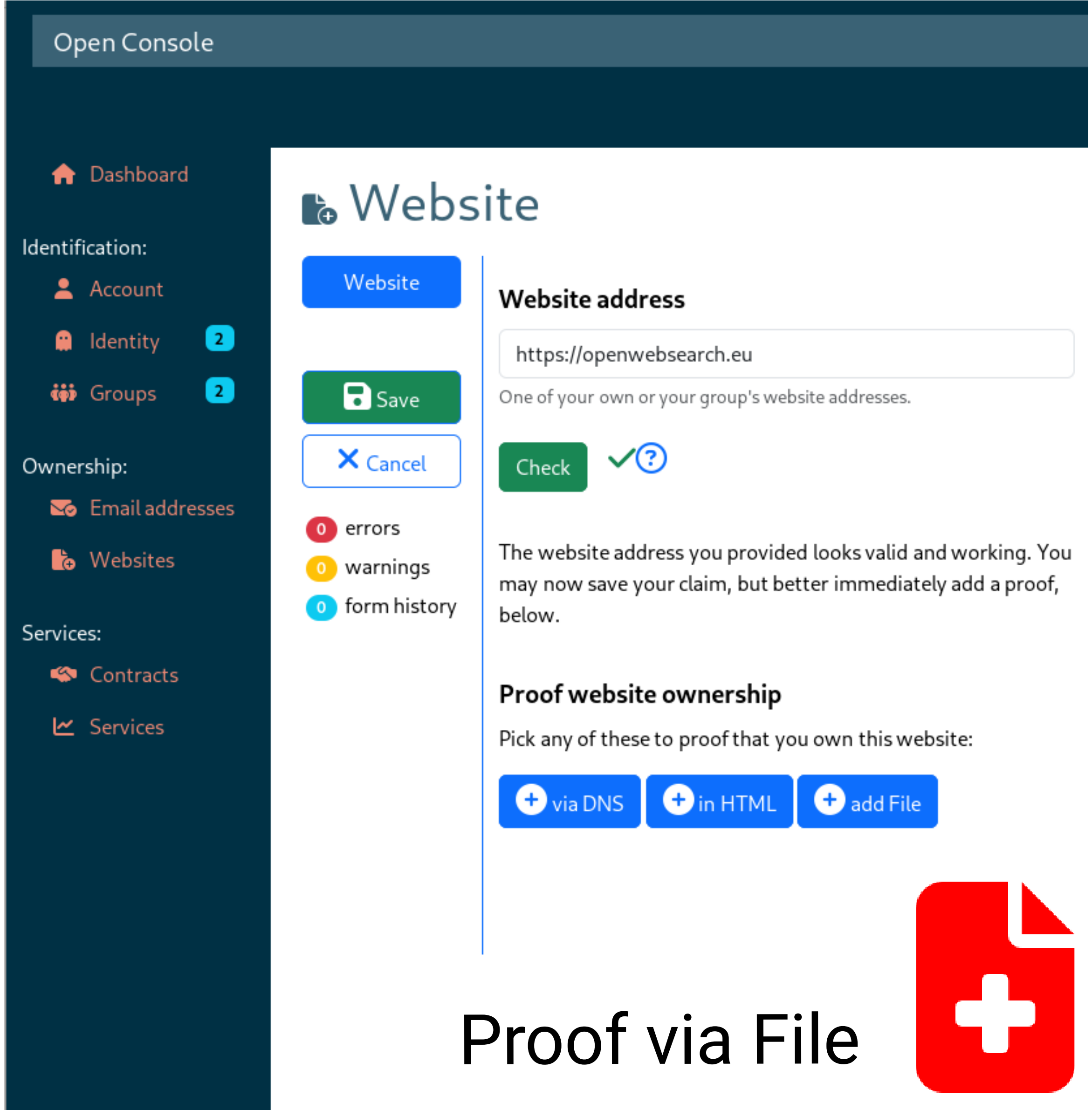
```
<meta name="open-console.website-owner"
   content="https://openwebsearch.eu"
   data-note="Website Ownership Proof"
   data-version="website html 20240717"
   data-challenge="devel01:H:8z8Q06RGijGIhhQcNRtxLm"
   data-created="2024-10-01T14:35:07Z"
 />
```

When you need more than one challenge, then simply add multiple of these blocks. After you have added above line to your frontpage, start verification.

Start verification

Proof via HTML

Proof via File



Open Console

Dashboard

Identification:

Account

Identity 2

Groups 2

Ownership:

Email addresses

Websites

Services:

Contracts

Services

Website

Website

Save

✕ Cancel

0 errors

0 warnings

0 form history

Website address

https://openwebsearch.eu

One of your own or your group's website addresses.

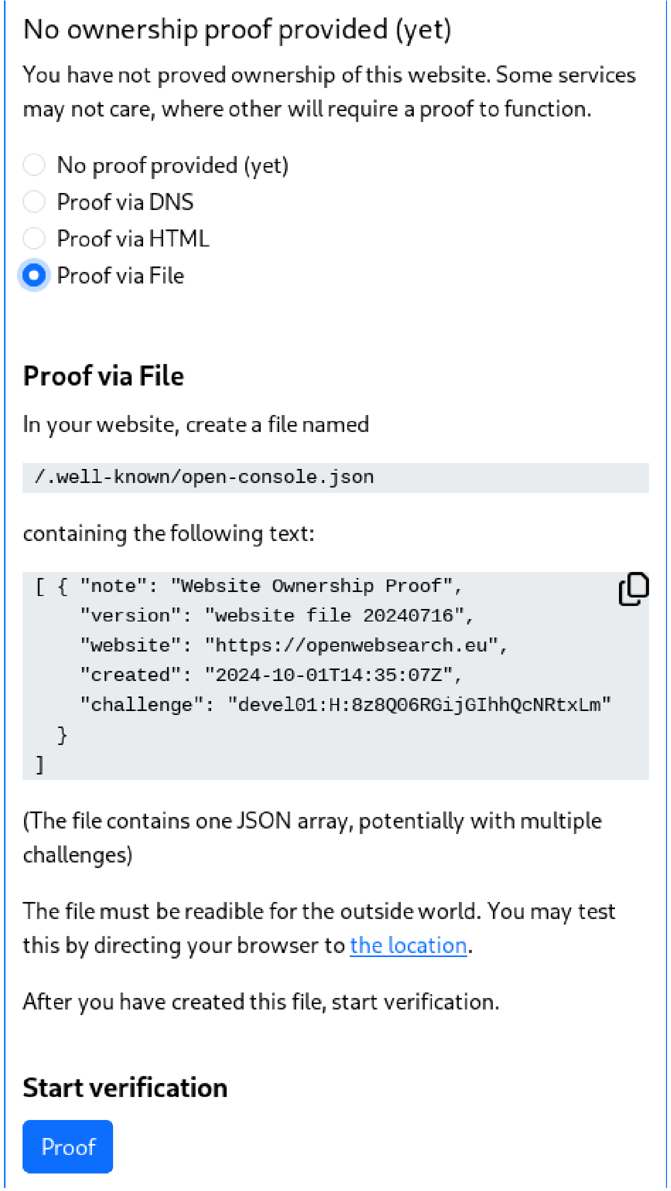
Check ✓ ?

The website address you provided looks valid and working. You may now save your claim, but better immediately add a proof, below.

Proof website ownership

Pick any of these to proof that you own this website:

+ via DNS + in HTML + add File



No ownership proof provided (yet)

You have not proved ownership of this website. Some services may not care, where other will require a proof to function.

○ No proof provided (yet)
○ Proof via DNS
○ Proof via HTML
● Proof via File

Proof via File

In your website, create a file named

```
/.well-known/open-console.json
```

containing the following text:

```
[ { "note": "Website Ownership Proof",
    "version": "website file 20240716",
    "website": "https://openwebsearch.eu",
    "created": "2024-10-01T14:35:07Z",
    "challenge": "devel01:H:8z8Q06RGijGIhhQcNRtxLm"
  }
]
```

(The file contains one JSON array, potentially with multiple challenges)

The file must be readible for the outside world. You may test this by directing your browser to the location.

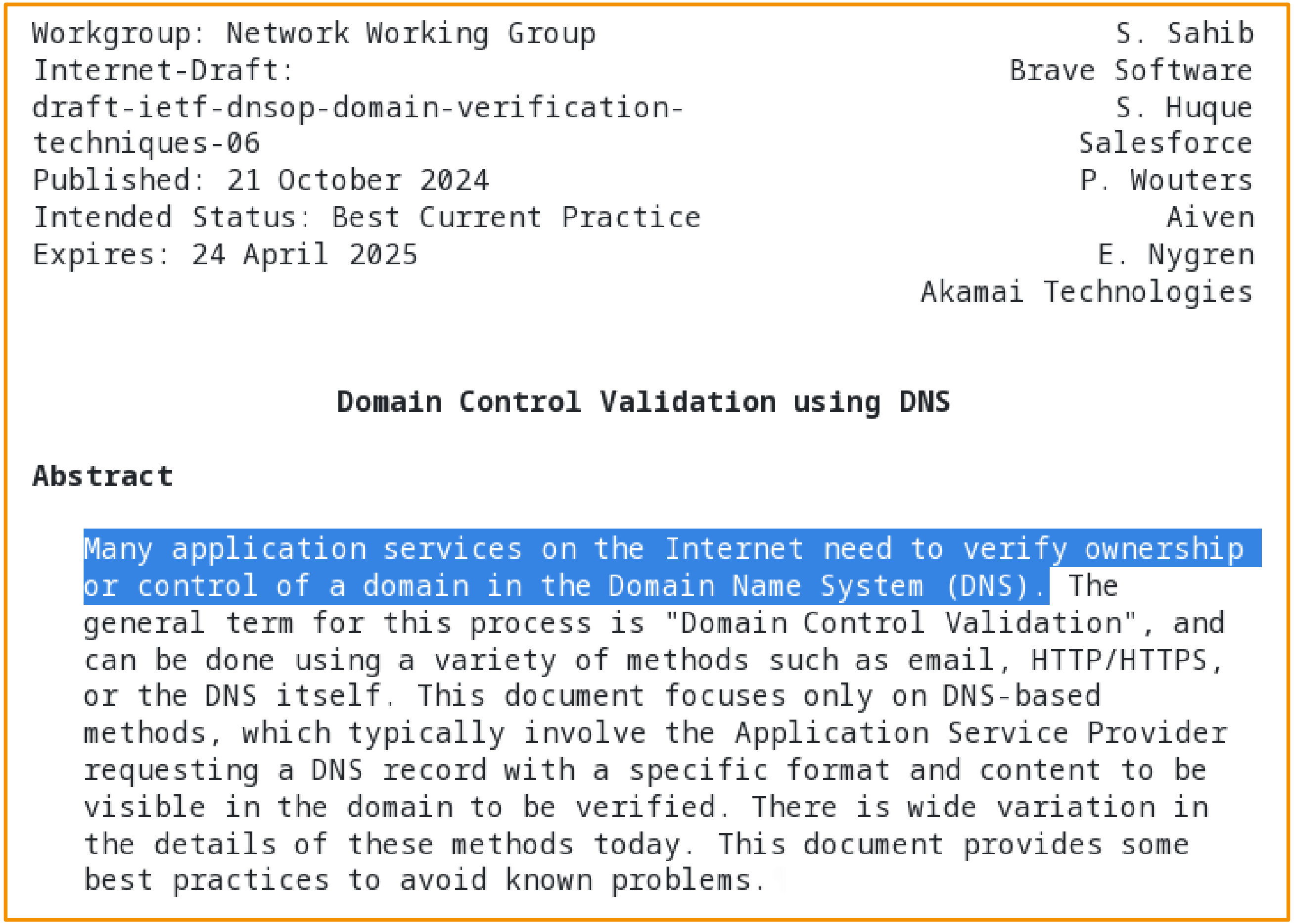
After you have created this file, start verification.

Start verification

Proof

Domain ownership proof

- RFC shows various TXT and CNAME based solutions.



```
Workgroup: Network Working Group                          S. Sahib
Internet-Draft:                                     Brave Software
draft-ietf-dnsop-domain-verification-                     S. Huque
techniques-06                                           Salesforce
Published: 21 October 2024                              P. Wouters
Intended Status: Best Current Practice                       Aiven
Expires: 24 April 2025                                   E. Nygren
                                              Akamai Technologies
```

Domain Control Validation using DNS

Abstract

Many application services on the Internet need to verify ownership or control of a domain in the Domain Name System (DNS). The general term for this process is "Domain Control Validation", and can be done using a variety of methods such as email, HTTP/HTTPS, or the DNS itself. This document focuses only on DNS-based methods, which typically involve the Application Service Provider requesting a DNS record with a specific format and content to be visible in the domain to be verified. There is wide variation in the details of these methods today. This document provides some best practices to avoid known problems.

Domain ownership proof

- DNS names

```
_<SERVICE>-challenge.example.com
_<FEATURE>._<SERVICE>-challenge.example.com
_<RANDOM>._<SERVICE>-challenge.example.com
_<SERVICE>-host-challenge.example.com
_<SERVICE>-wildcard-challenge.example.com
_<SERVICE>-domain-challenge.example.com
```

- TXT content

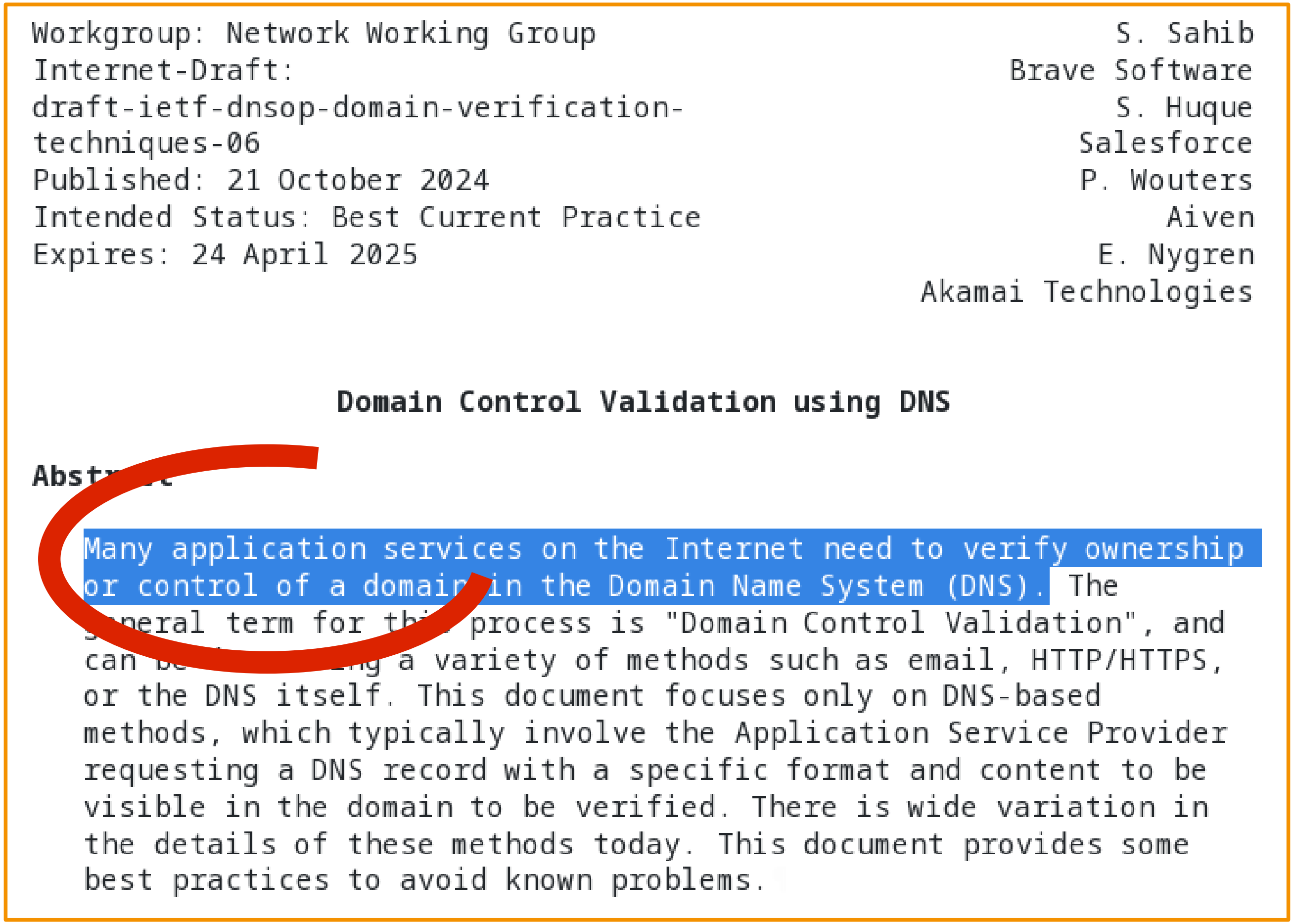
```
_foo-challenge.example.com. TXT  "3419...3d206c4"
TXT "token=3419...3d206c4 expiry=2023-02-08"
```

- CNAME content

```
CNAME  <RANDOM>.dcv.example.com
```

Domain ownership proof

- How often do you want to provide an ownership proof?
- Difference between website and domain ownership?
- DNS Admin vs Legal owner?
- Other methods?



```
Workgroup: Network Working Group                              S. Sahib
Internet-Draft:                                         Brave Software
draft-ietf-dnsop-domain-verification-                         S. Huque
techniques-06                                               Salesforce
Published: 21 October 2024                                  P. Wouters
Intended Status: Best Current Practice                           Aiven
Expires: 24 April 2025                                       E. Nygren
                                                    Akamai Technologies
```

Domain Control Validation using DNS

Abstract

Many application services on the Internet need to verify ownership or control of a domain in the Domain Name System (DNS). The general term for this process is "Domain Control Validation", and can be performed using a variety of methods such as email, HTTP/HTTPS, or the DNS itself. This document focuses only on DNS-based methods, which typically involve the Application Service Provider requesting a DNS record with a specific format and content to be visible in the domain to be verified. There is wide variation in the details of these methods today. This document provides some best practices to avoid known problems.

Domain ownership proof

- How often do you want to provide an ownership proof?
  - once with expiry? continuous?
  - variation in complexity
- Difference between website and domain ownership?
- DNS Admin vs Legal owner
  - support by TLD providers?
- Other methods?

Network ownership proof

- Nested structure
- Extend the mechanism to the reverse zones with PTR records?
- IPv4 and IPv6 syntax examples
- ASNs? BGP?

- Useful?

Try it soon!

https://open-console.eu
team@open-console.eu