Overview and Intro Guide

Quickly get started to empower your email users with DANE SMIME

What is DANE portal

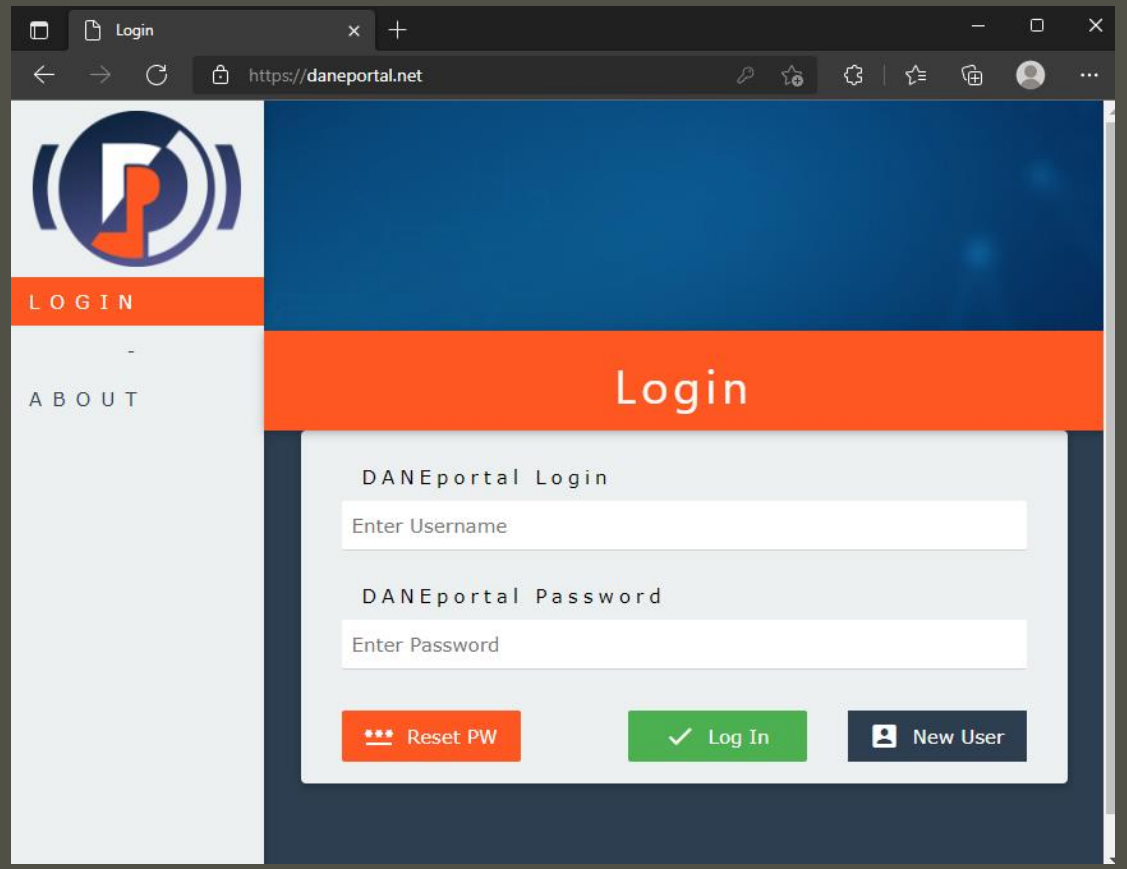
- DANE portal is a DNS-based certificate management infrastructure which allows zone admins to easily enable DANE for email users under their domains
- It currently supports S/MIME protocol for certificates
- Zone admins need a DNSSEC-enabled zone which they wish to delegate
  - The parent zone can be with any DNS provider –
    DANE portal will only manage the DANE sub-domain *(more info on that in the walkthrough)*

Overview

- We will show off the main features on DANE portal, from two perspectives
- Admins
  - Create an account
  - Claim and verify your zone
  - Hook up your zone
  - Add email users (so they can handle their own certs)
- Email users
  - Access the email addresses under DANE portal
  - Add and control DANE records (SMIME certificates) for their email addresses

Getting Started

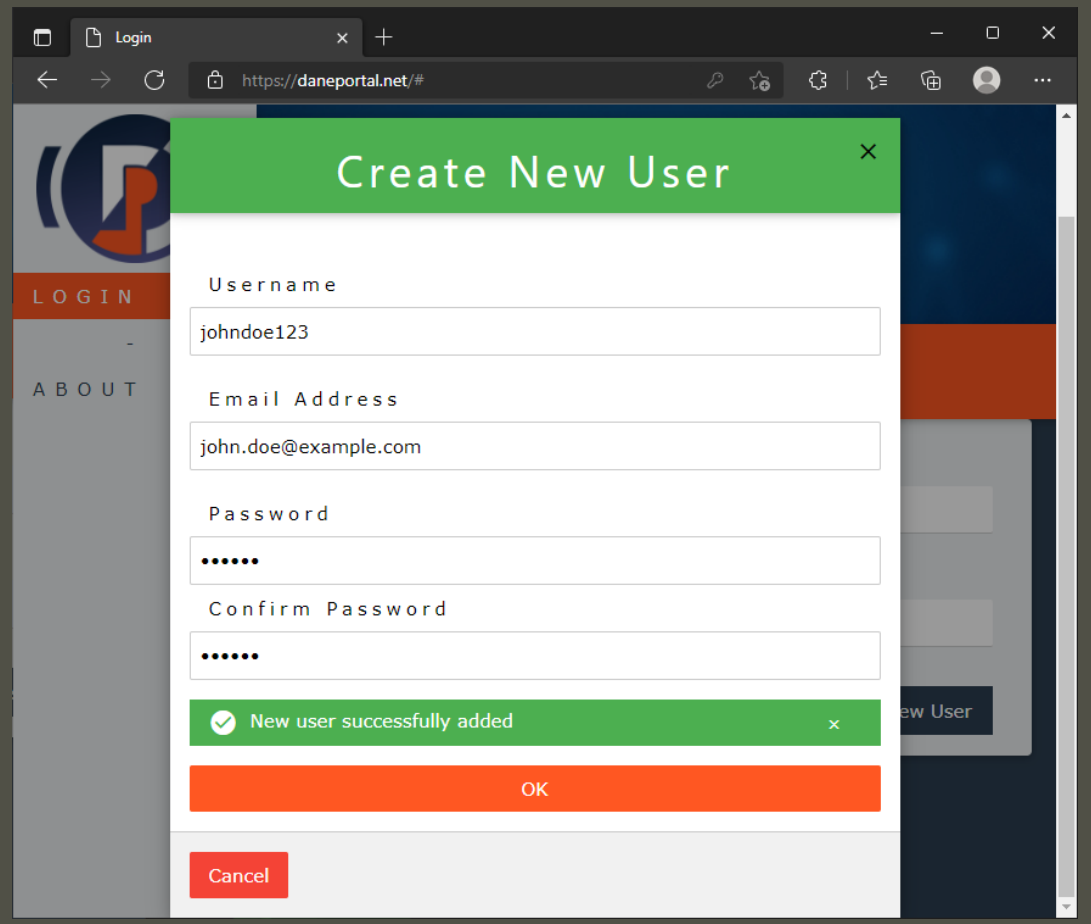
- Lets look at adding DANE support for a zone you administer
- Hop on to DANE portal at [daneportal.net]



Create a new user

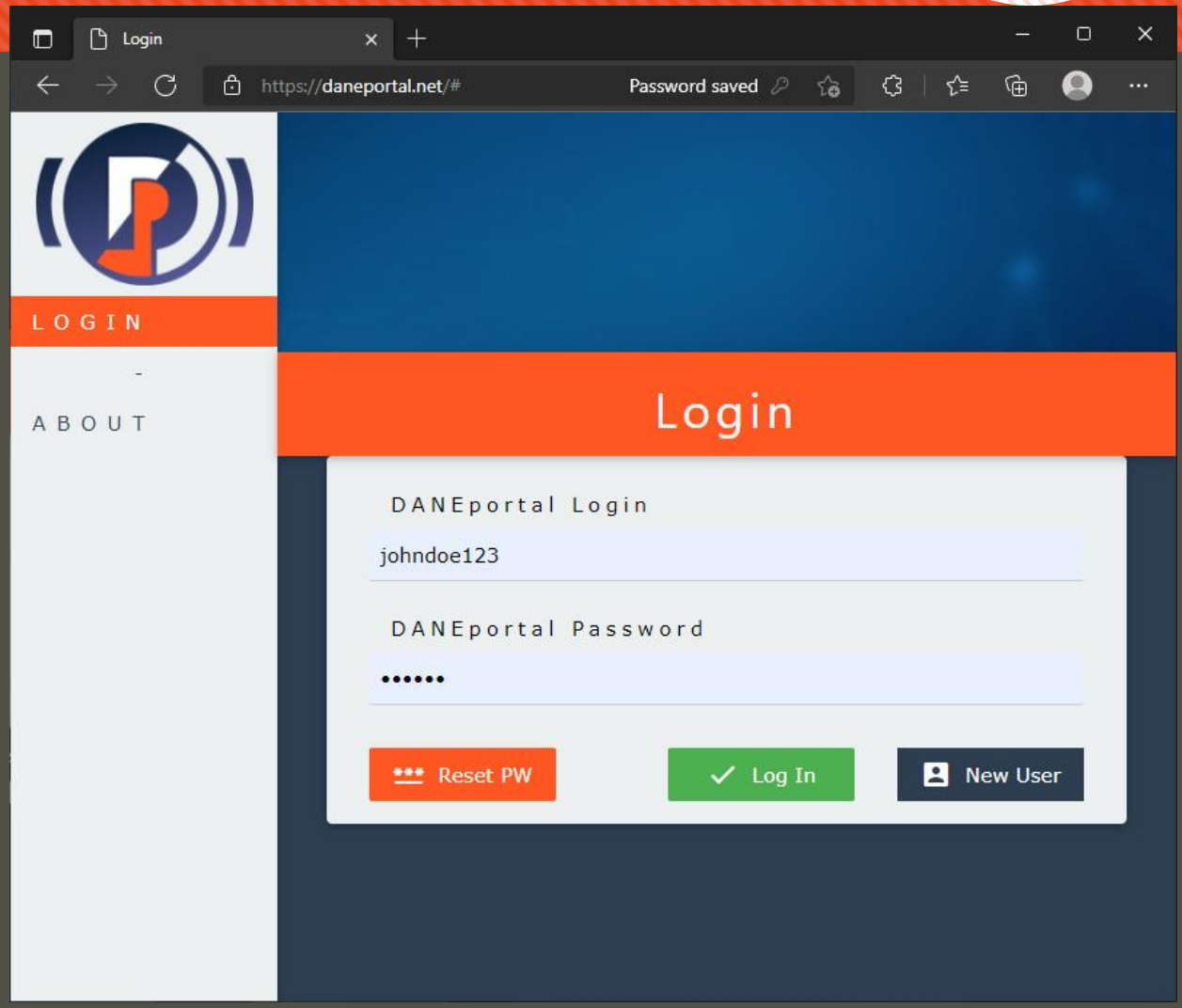
- Click [New User]
- Enter desired credentials
- Click [Create User]
- Click [OK] to close modal

- This will make a login account through which you can access DANE portal
- Every email user will need their own login
- Third-party OAuth logins are a planned feature, as is automated bulk account creation



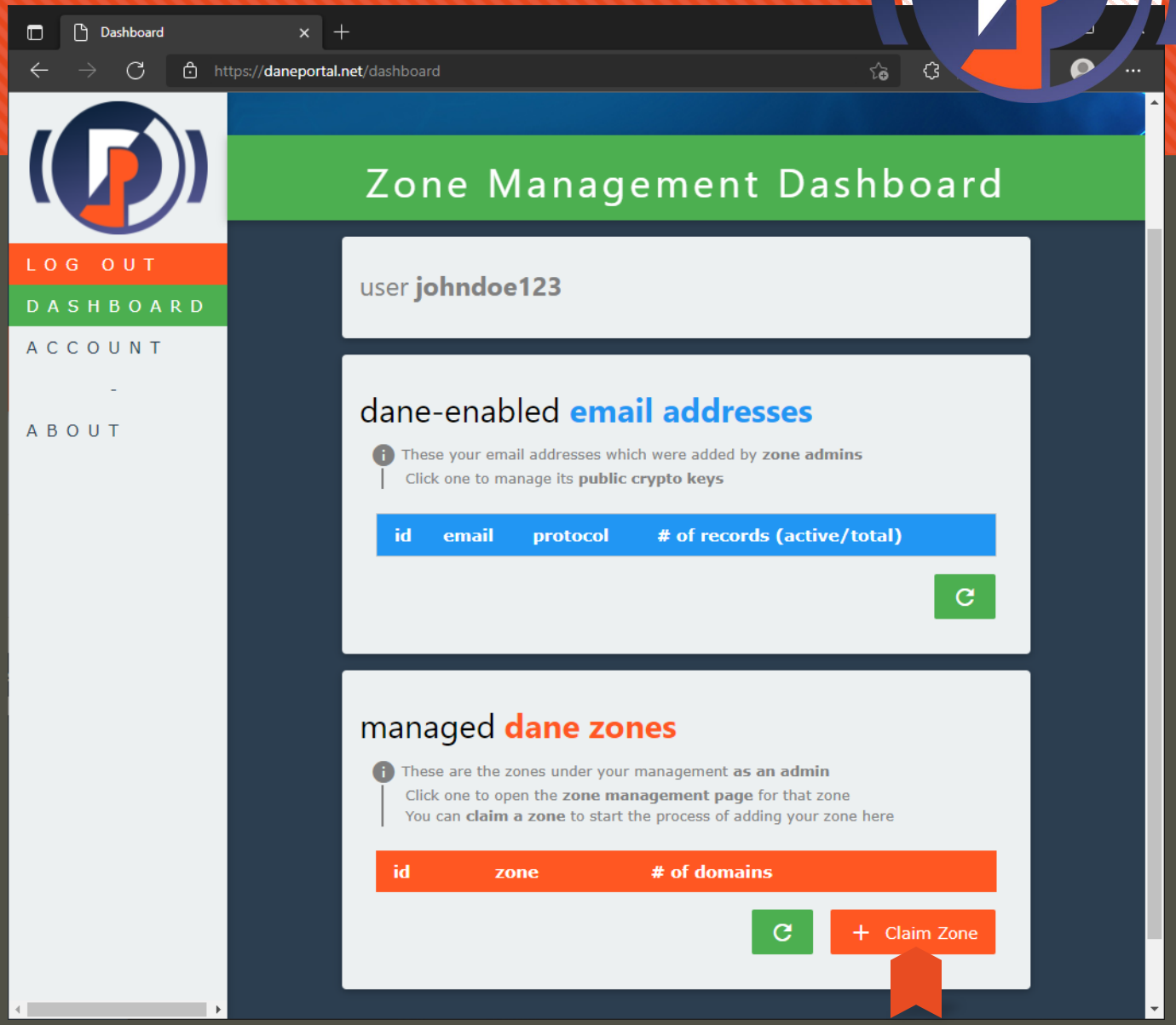
Log In

- Enter your credentials
- Click [Log In]



Dashboard

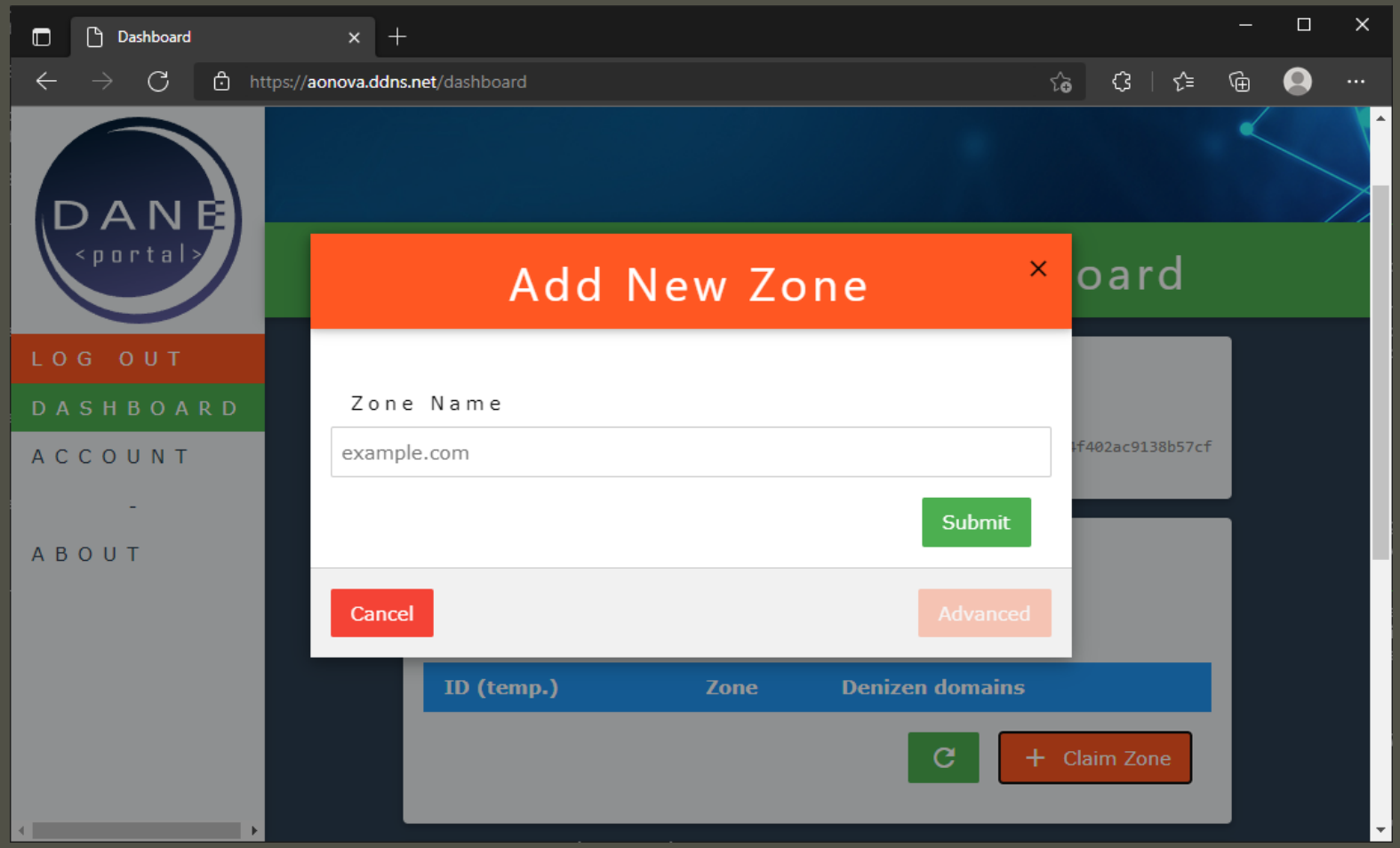
- This is the landing page for users
- Under [managed dane zones] section admins can view the zones managed under the portal
- Click [Claim Zone] to add your zone



Add a new zone

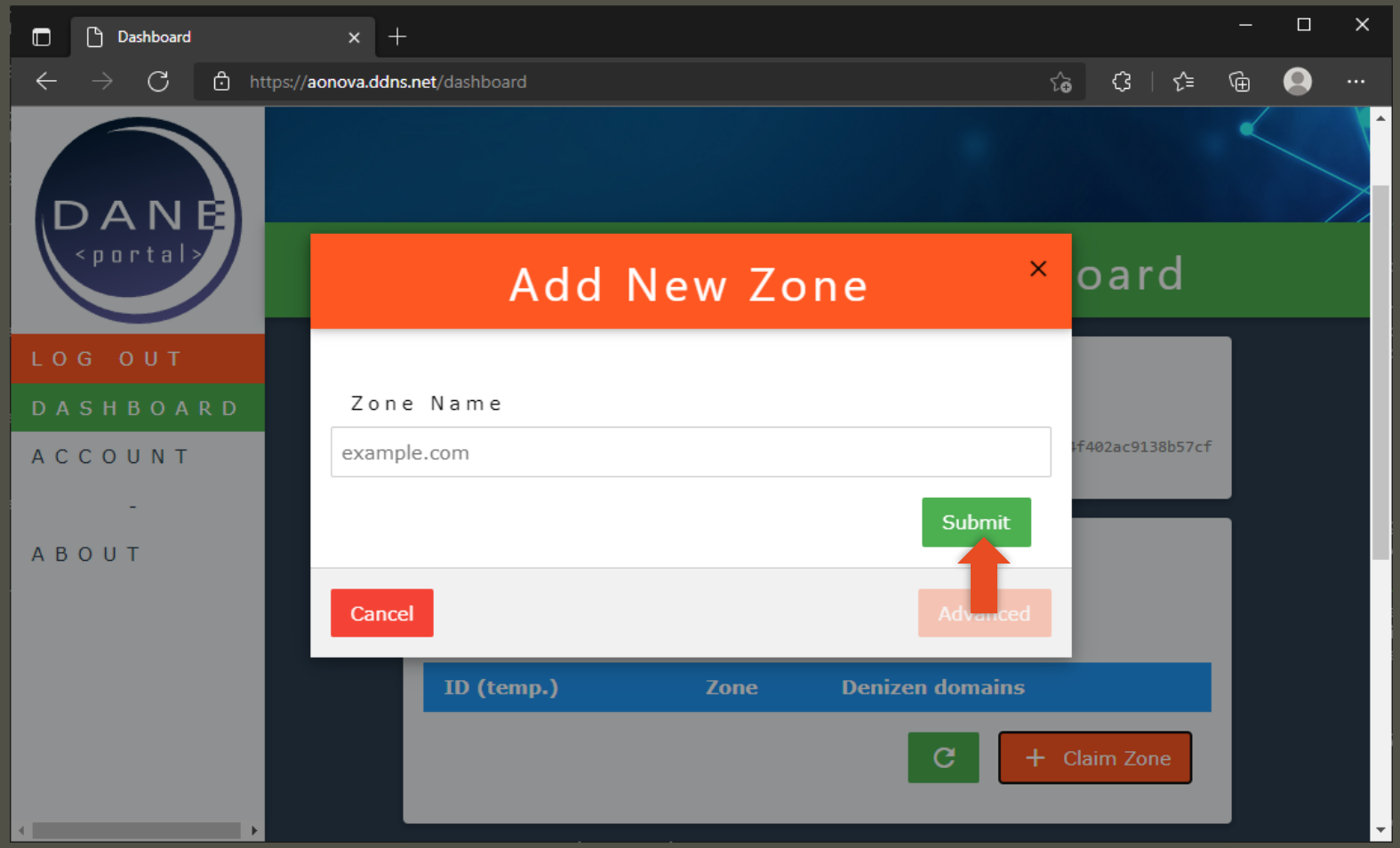
- Here you can add a zone which you administer to be managed under your user on DANE portal
- This will let you manage DANE support for that zone

- **Important note**: it is a prerequisite of DANE that **your zone must be DNSSEC enabled**
- Use your DNS provider's interface to check and enable DNSSEC before adding it on DANE portal



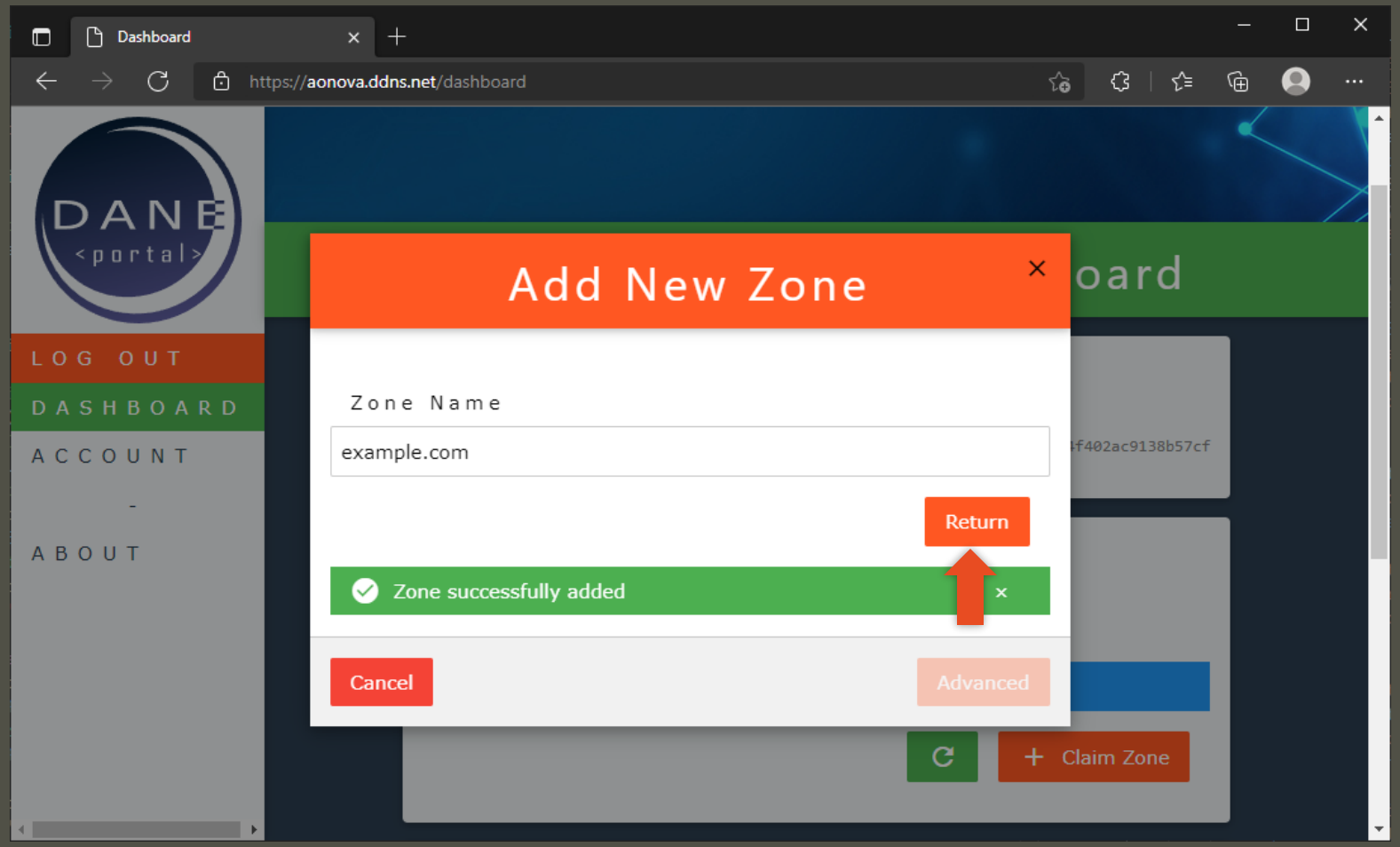
Add a new zone

- Enter the *Fully Qualified Domain Name* of the zone you would like to administer
- Click [Submit] to add the zone *on a claimed basis*
- Anyone can claim any zone, but to complete you will need to prove ownership of the zone using the ACME protocol (shown next)



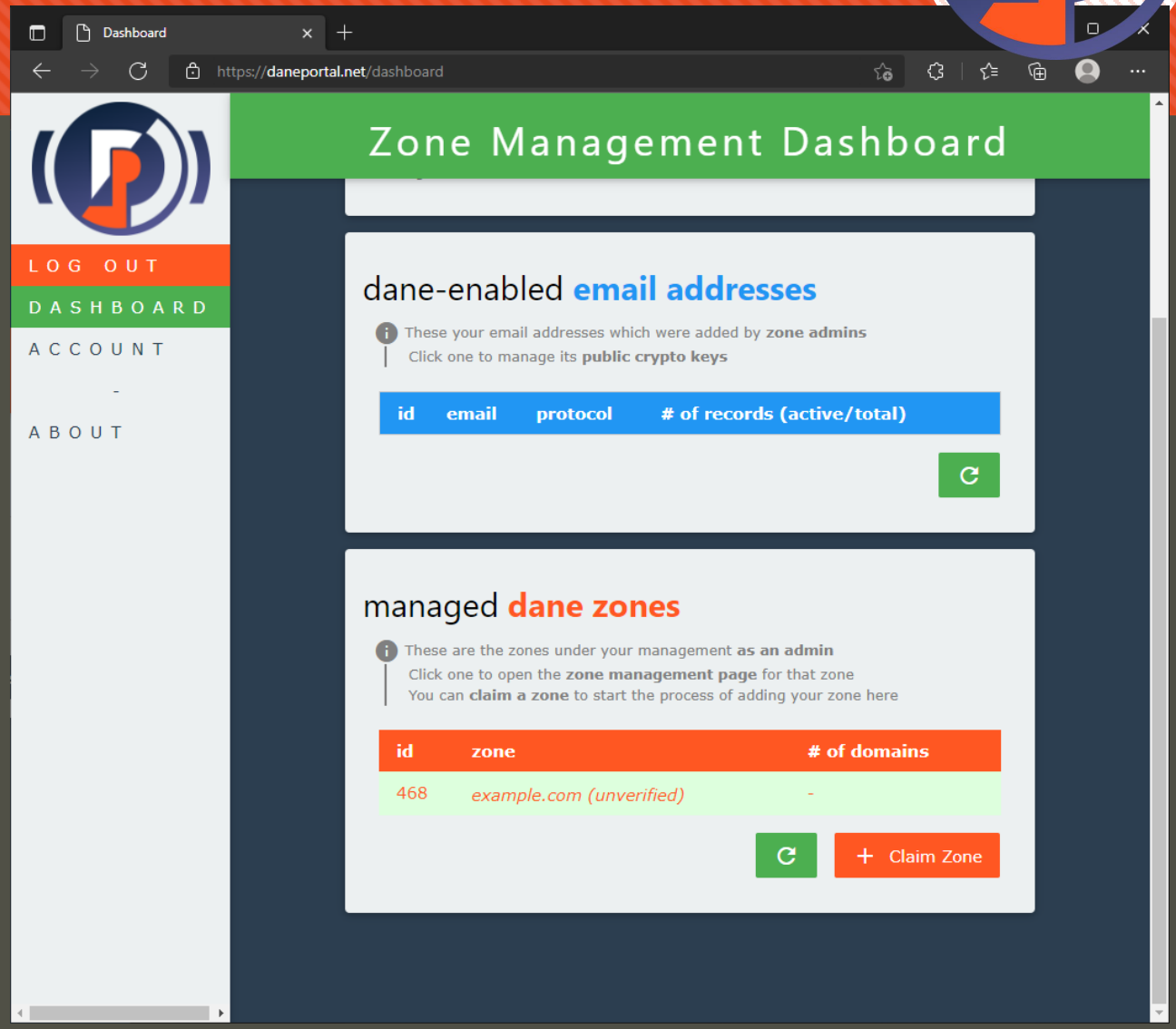
Add a new zone

- Enter the *Fully Qualified Domain Name* of the zone you would like to administer
- Click [Submit] to add the zone *on a claimed basis*
- Click [Return] to close the modal and see the newly added zone claim



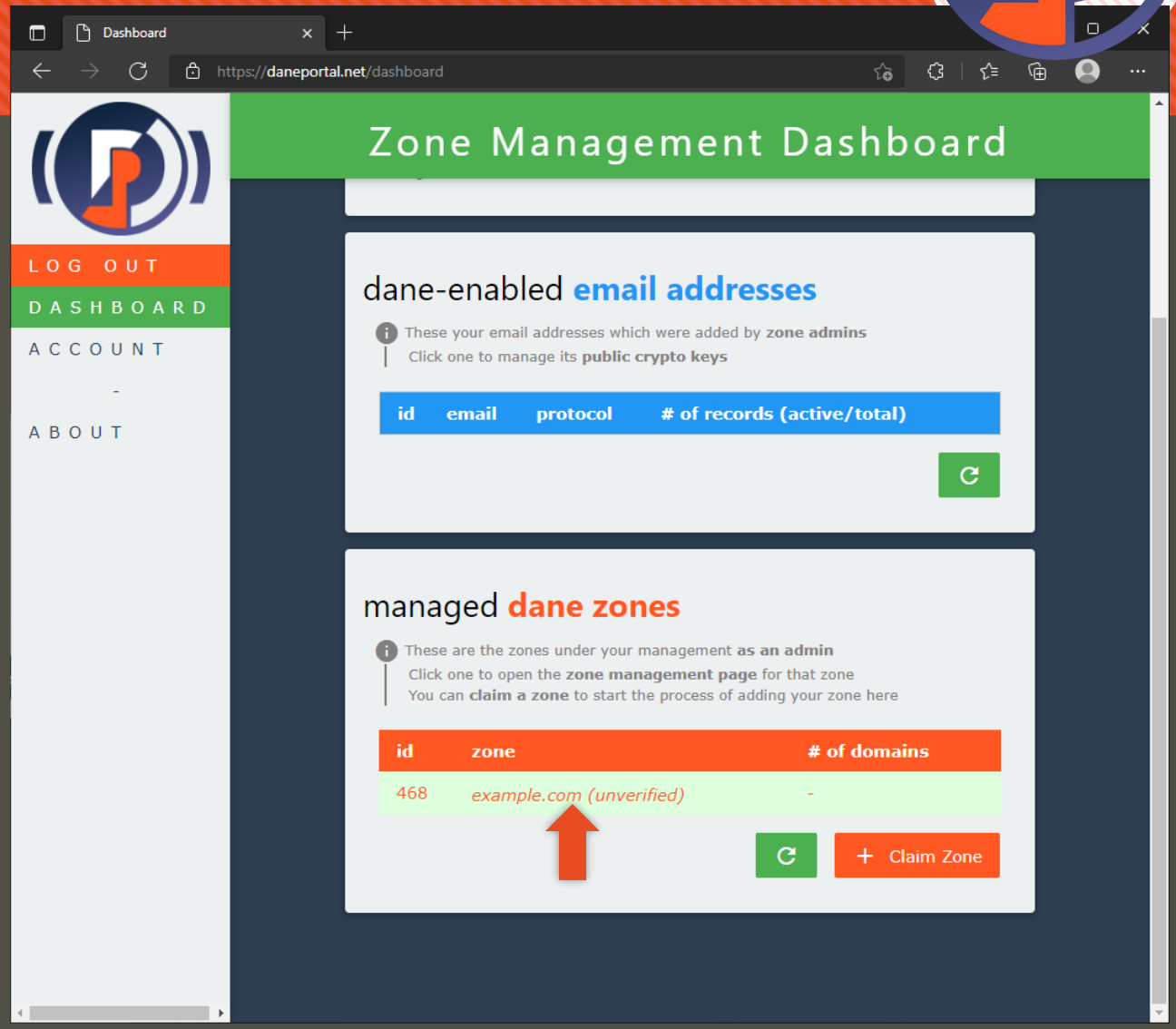
Add a new zone

- Enter the *Fully Qualified Domain Name* of the zone you would like to administer
- Click [Submit] to add the zone *on a claimed basis*
- Click [Return] to close the modal and see the newly added zone claim



Verify zone claim

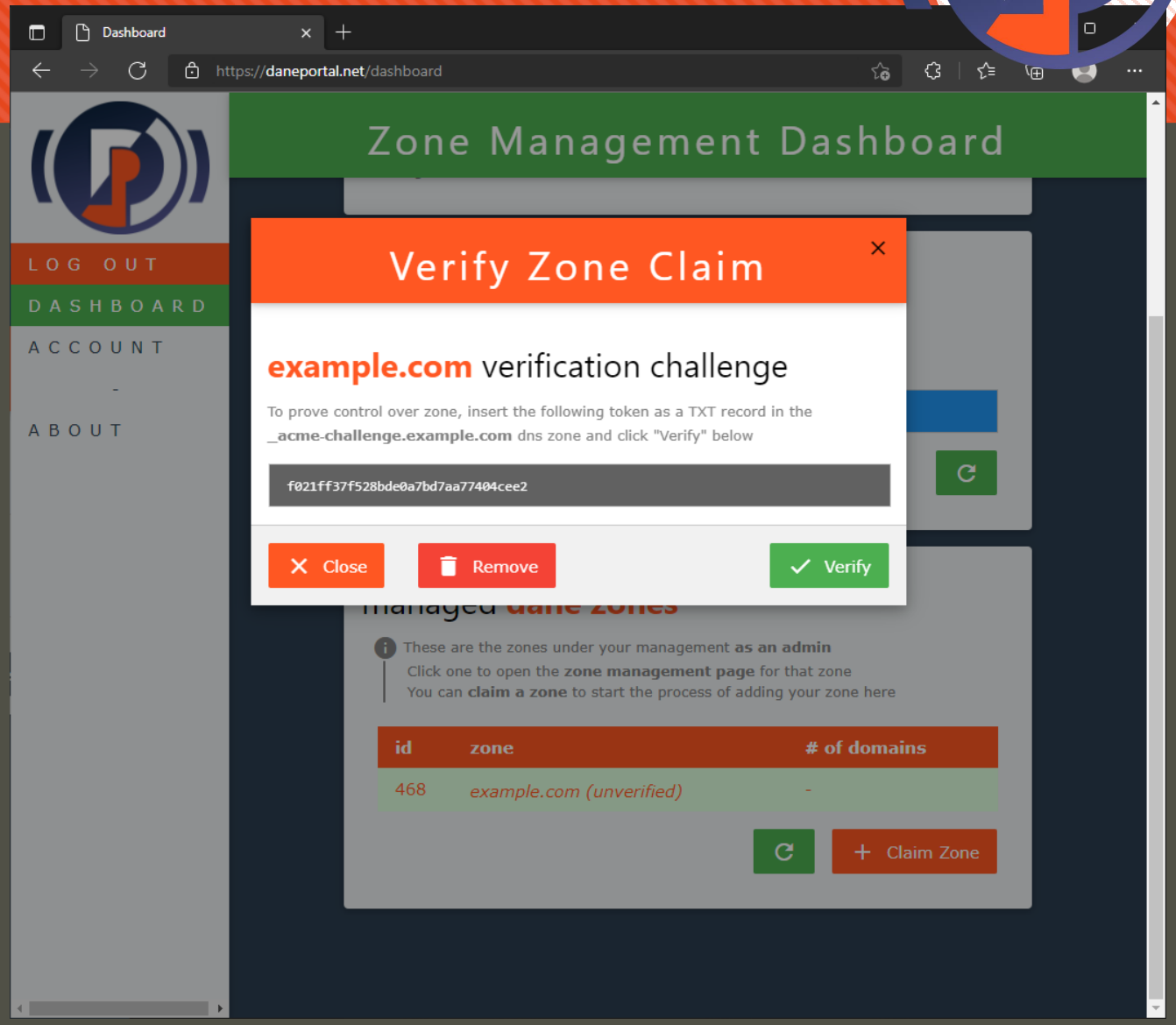
- Click on the unverified zone from the list to start verification challenge



Verify zone claim

- Click on the unverified zone from the list to start verification challenge

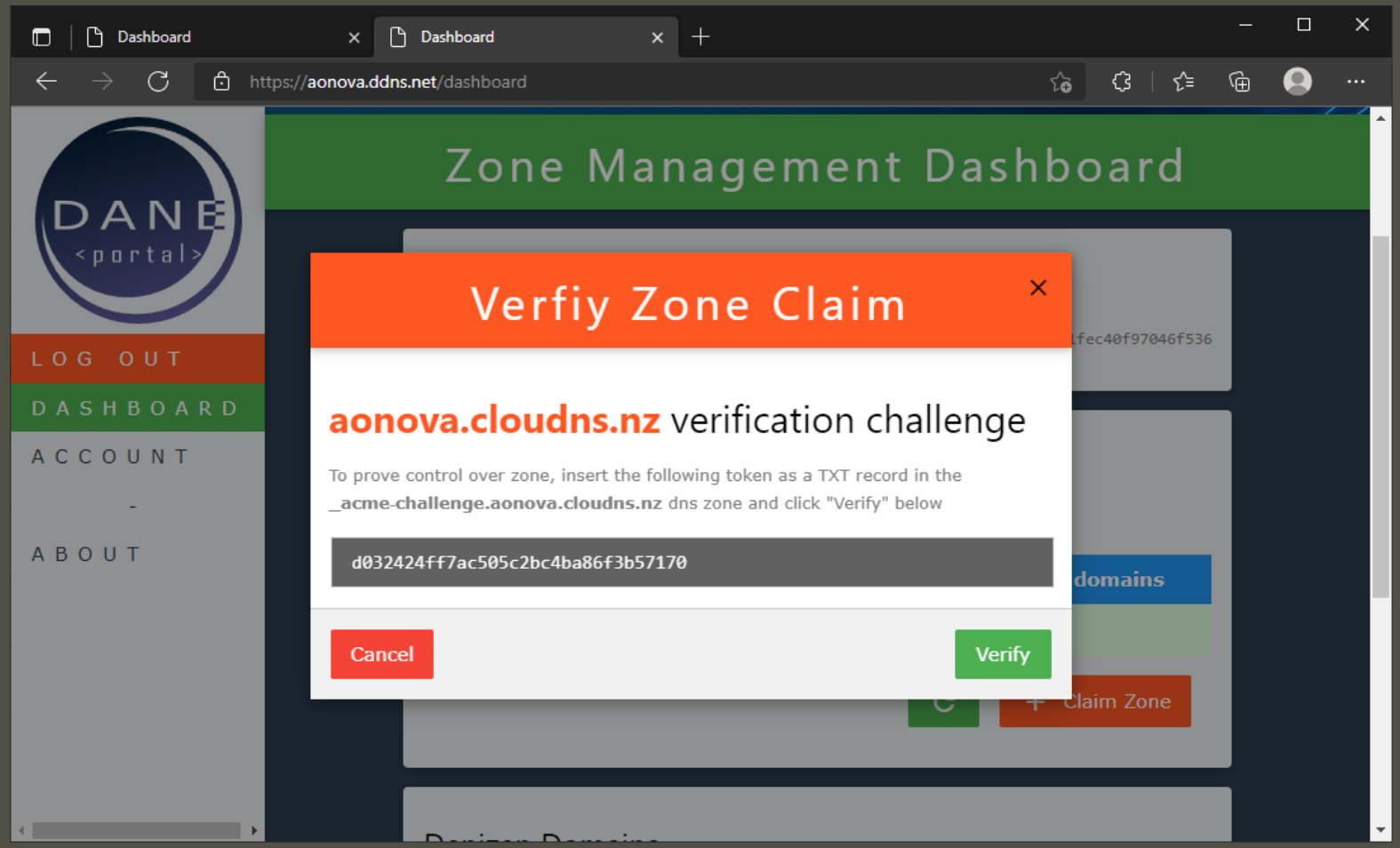
- This challenge helps to prove that you have real-world authority over the zone and prevents bad actors from squatting on the portal



Verify zone claim (example)

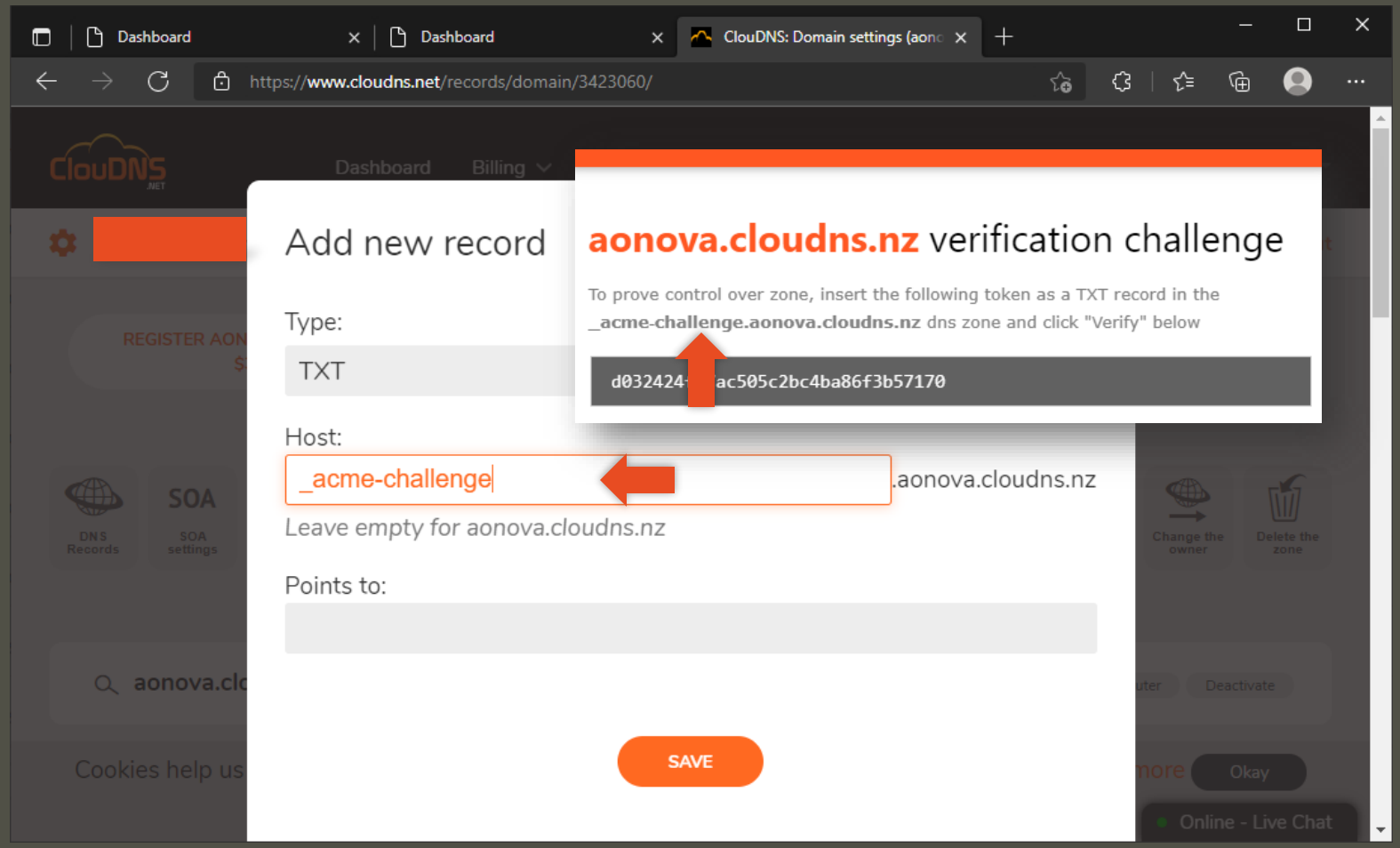
- Follow the directions to complete the verification challenge

- This process differs slightly based on your DNS service provider. The example pictures are simply a reference – follow the procedures according to your service interface



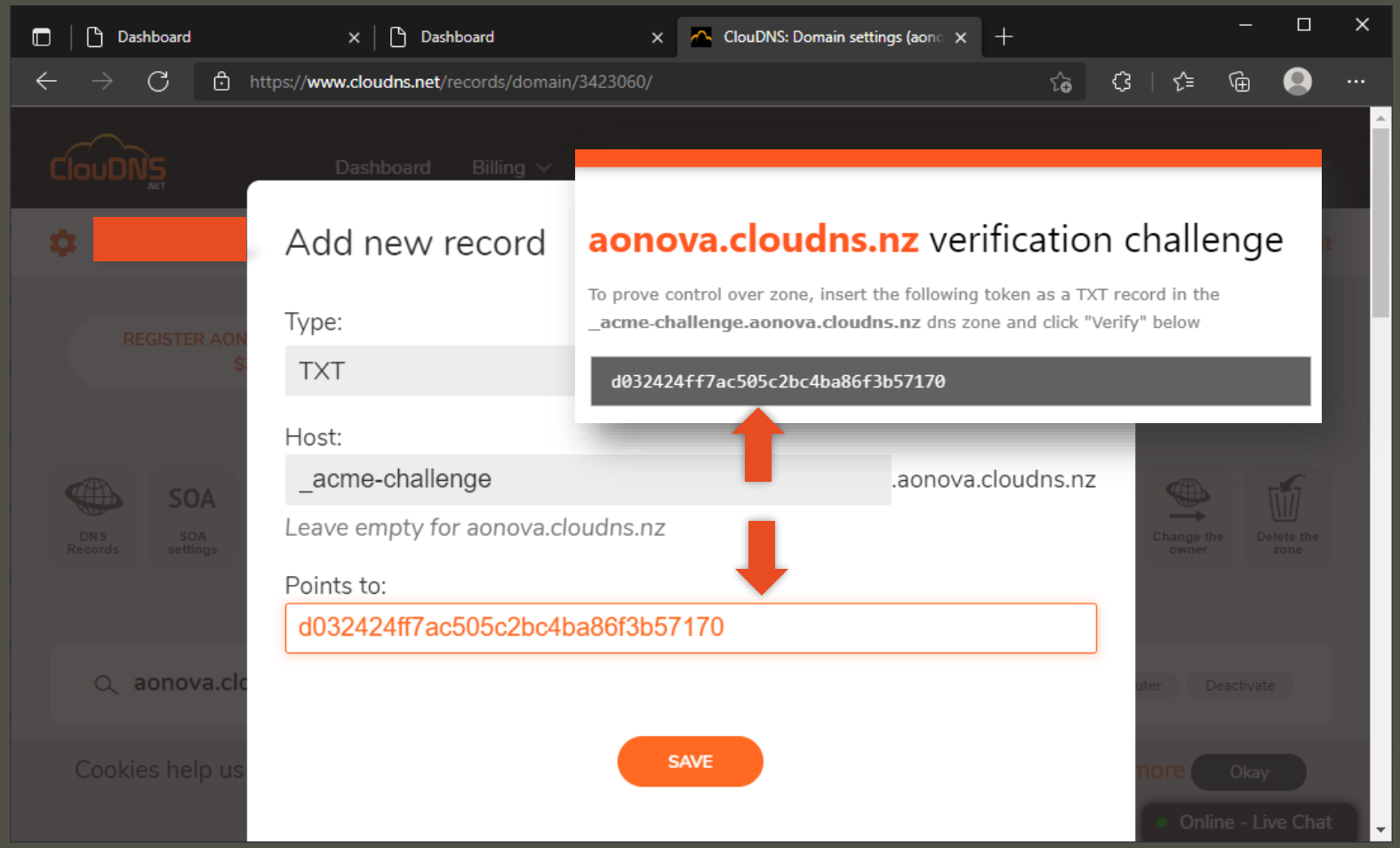
Verify zone claim (example)

- As directed, use your DNS management tools to create a TXT record for the hostname _acme-challenge



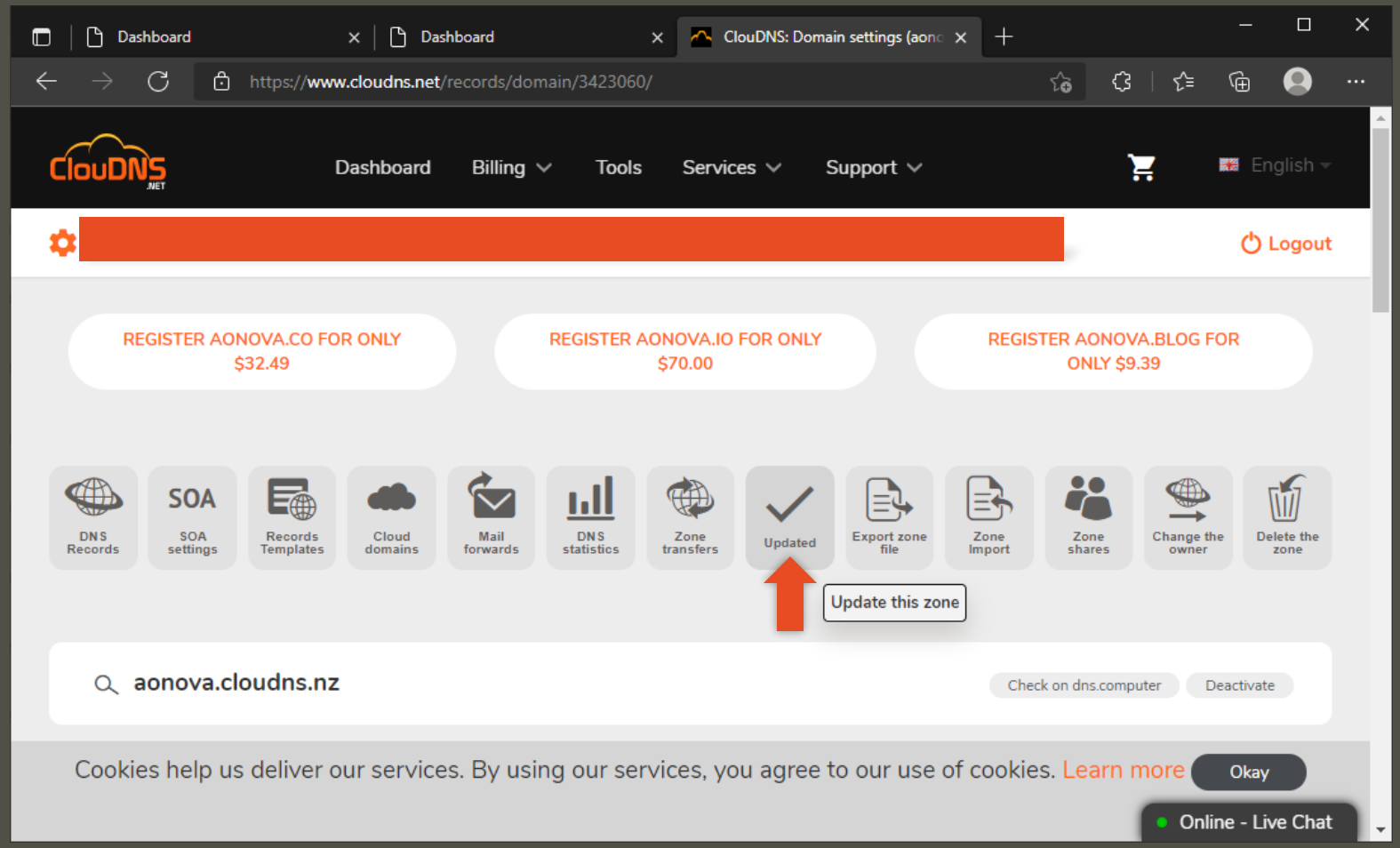
Verify zone claim (example)

- As directed, use your DNS management tools to create a TXT record for the hostname _acme-challenge
- Use the given hex token as the value



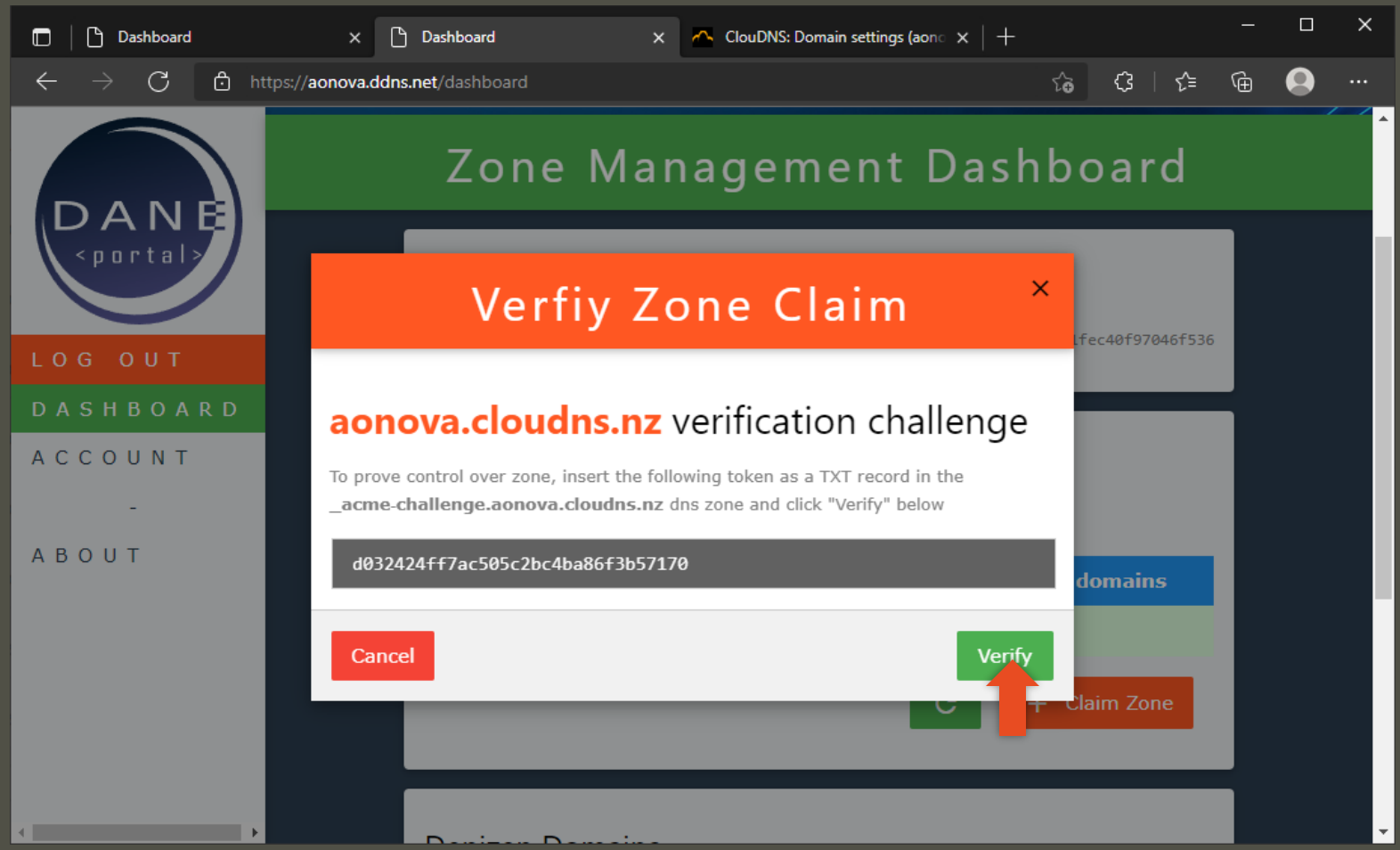
Verify zone claim (example)

- As directed, use your DNS management tools to create a TXT record for the hostname _acme-challenge
- Use the given hex token as the value
- Wait until zone updates



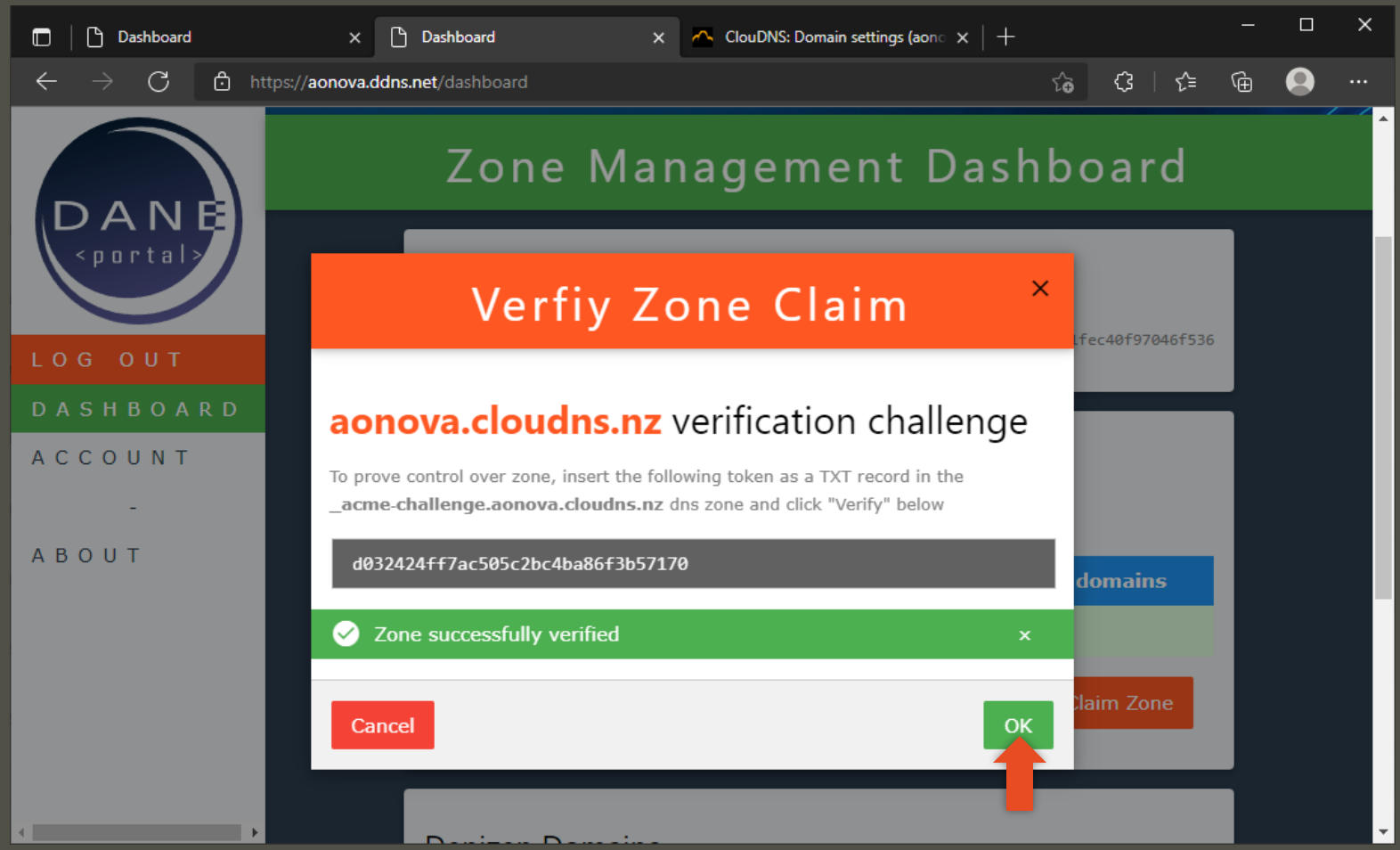
Verify zone claim (example)

- As directed, use your DNS management tools to create a TXT record for the hostname _acme-challenge
- Use the given hex token as the value
- Wait until zone updates
- Click [Verify] to perform the challenge



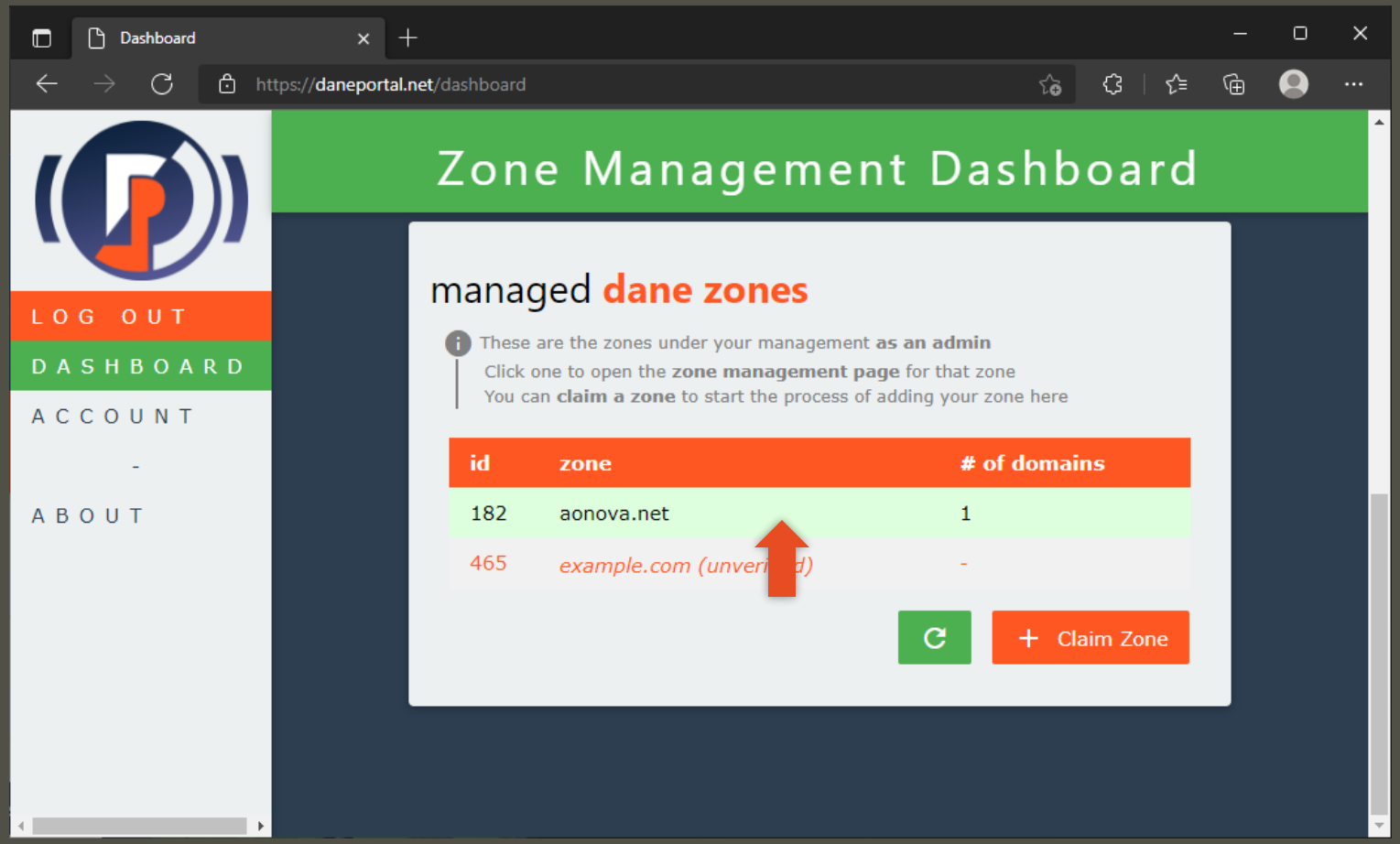
Verify zone claim (example)

- As directed, use your DNS management tools to create a TXT record for the hostname _acme-challenge
- Use the given hex token as the value
- Wait until zone updates
- Click [Verify] to perform the challenge
- Click [OK] to return to the dashboard



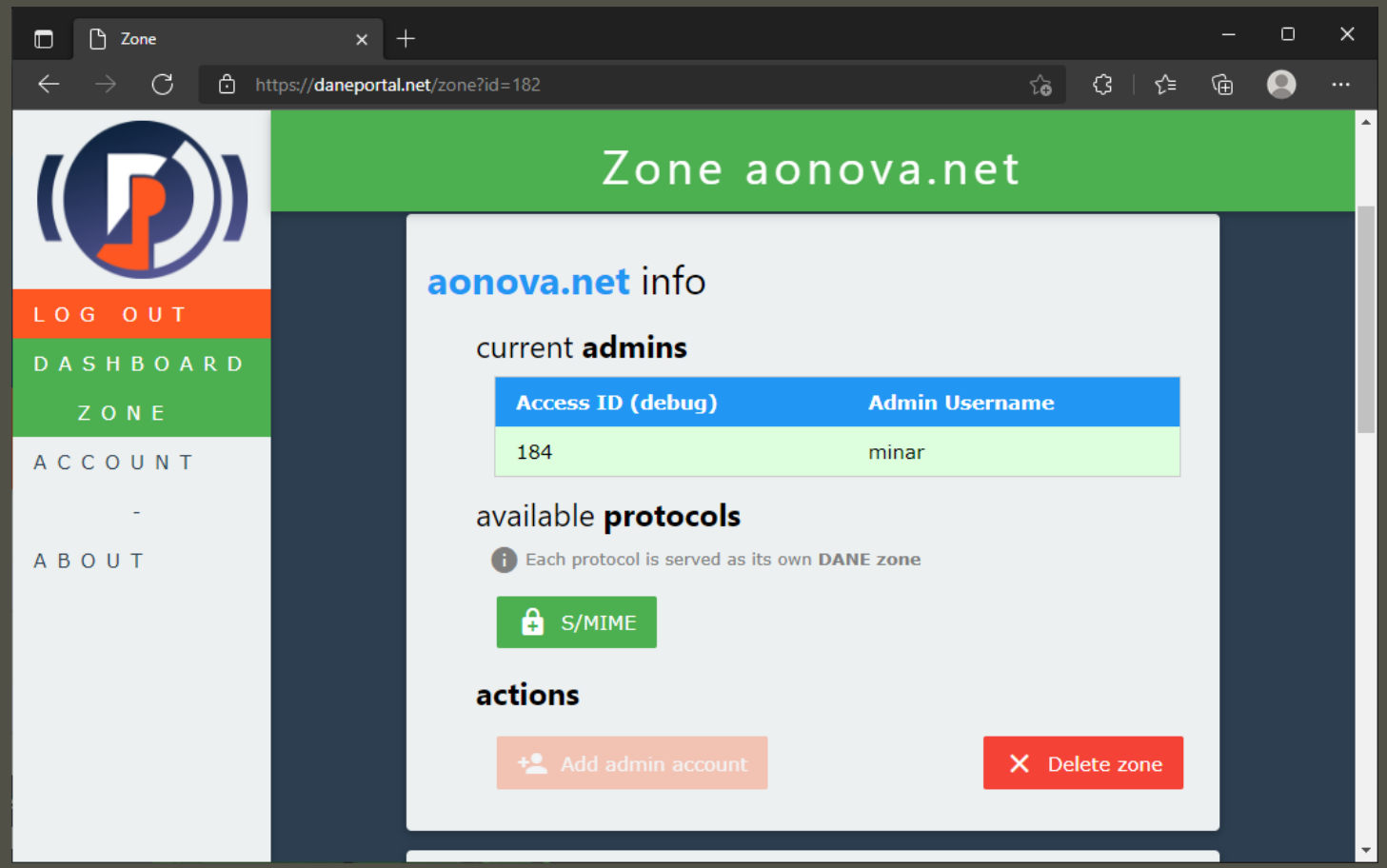
Manage zone

- The dashboard now shows your zone properly under your account's administration
- Click the zone you would like to manage to bring up the Zone Management page



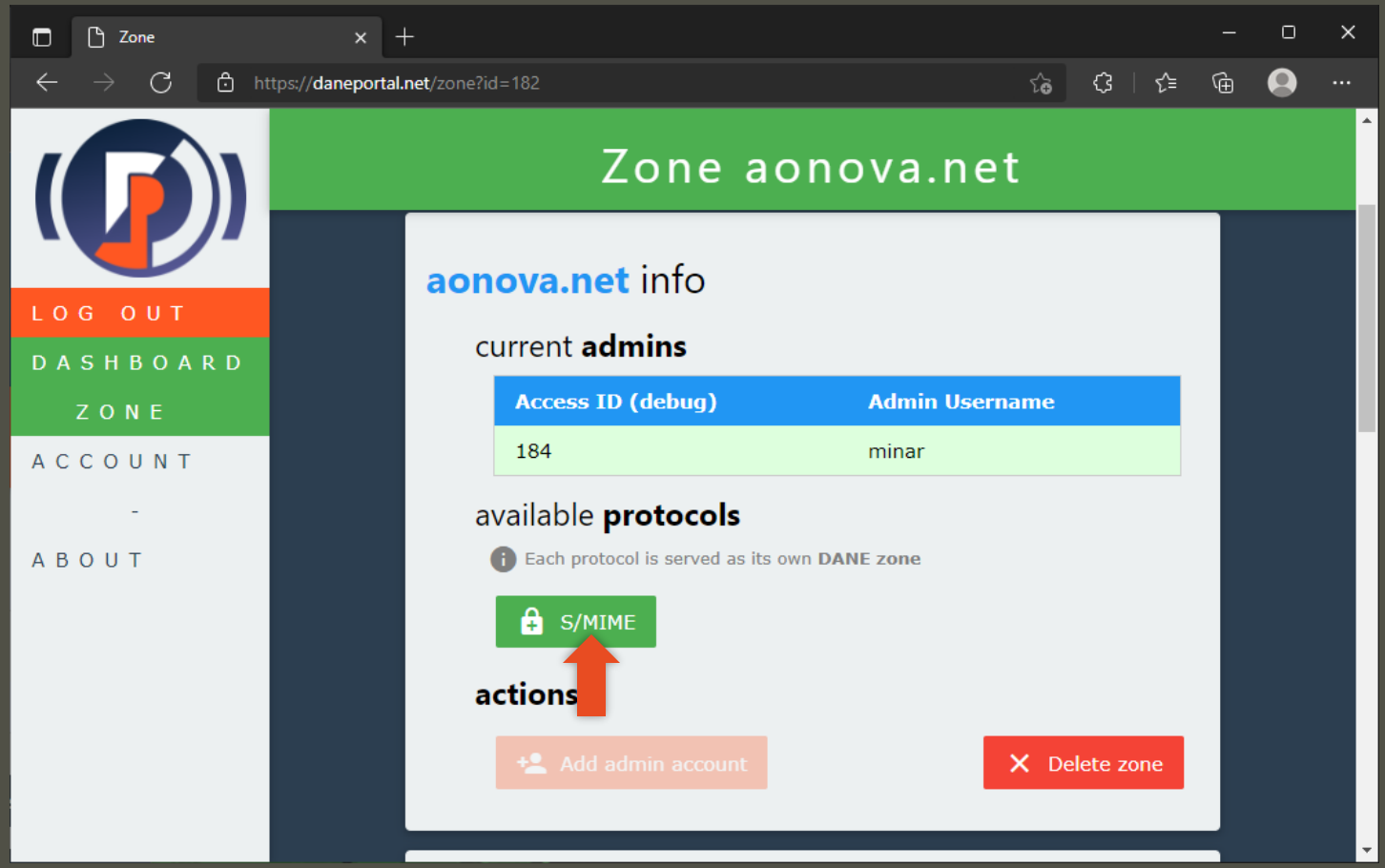
Manage zone

- The dashboard now shows your zone properly under your account's administration
- Click the zone you would like to manage to bring up the Zone Management page
- Here you can see info and take management actions regarding your zone on the DANE portal.



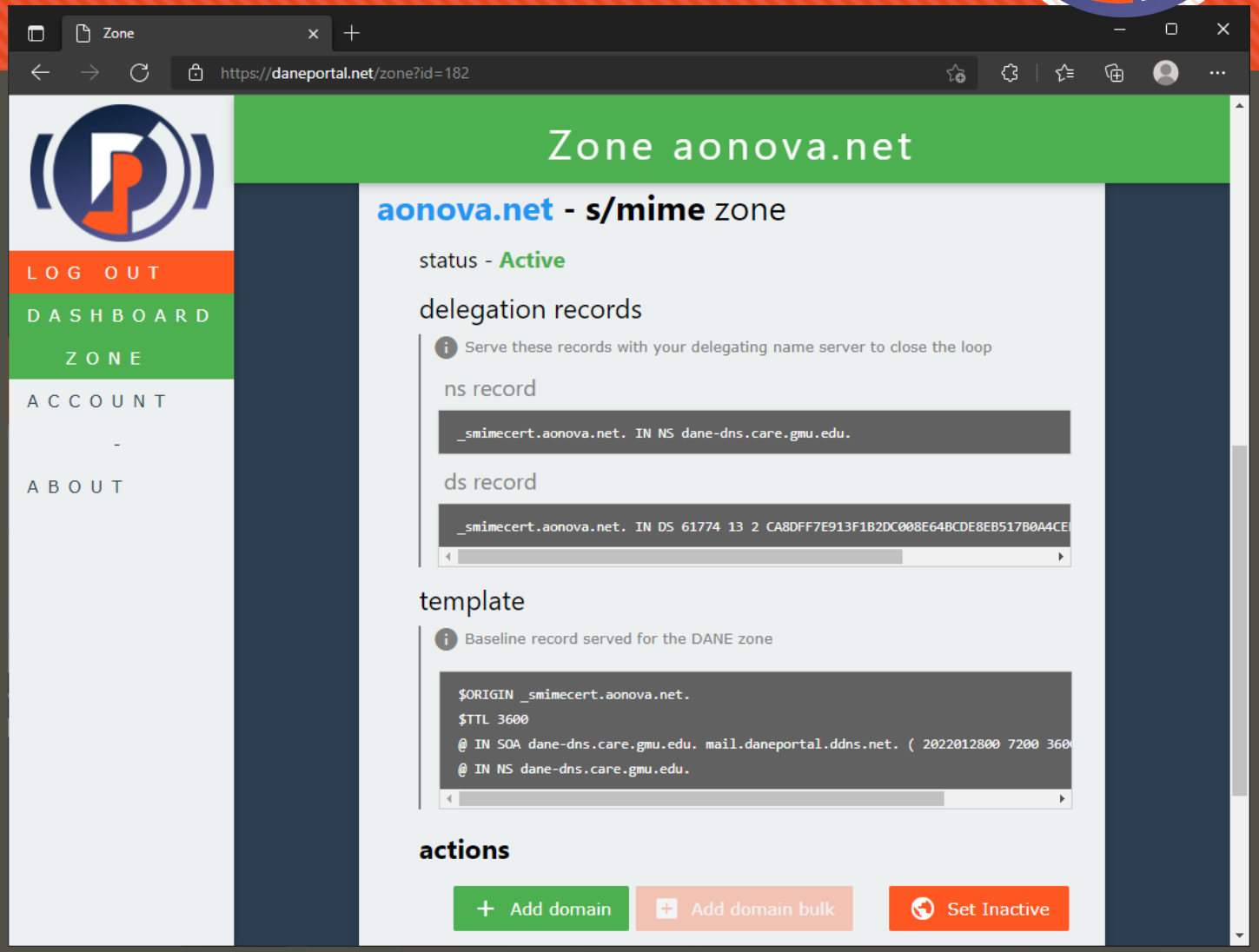
Manage zone

- DANE portal infrastructure will manage **DANE zones** – *DANE protocol-specific zones that you delegate under your zone*.
  - Currently only DANE-SMIME is available and the DANE zone is created by default
- Click the protocol to scroll to that section



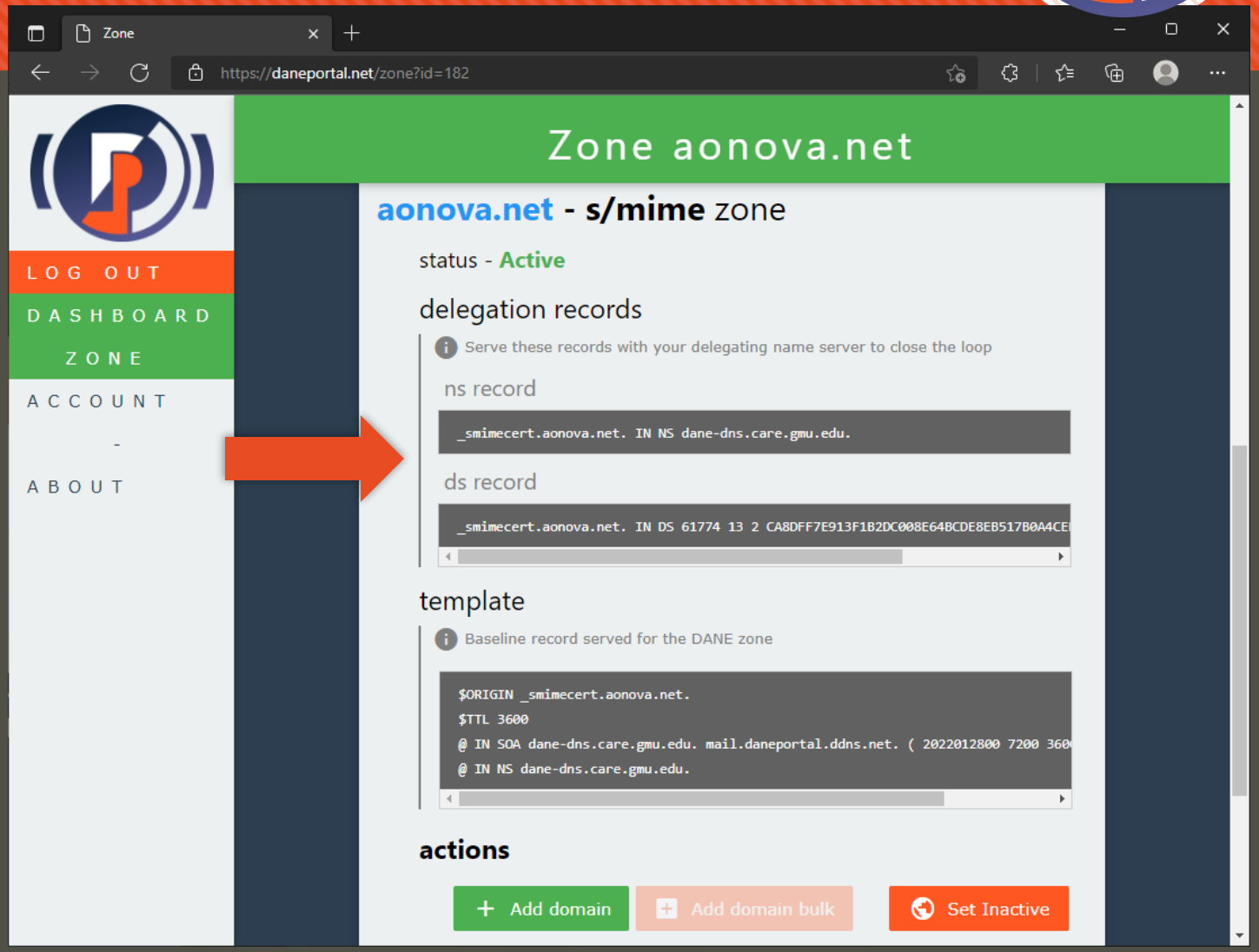
DANE zone

- DANE portal infrastructure will manage **DANE zones** – *DANE protocol-specific zones that you delegate under your zone*.
  - Currently only DANE-SMIME is available and the DANE zone is created by default
- Click the protocol to scroll to that section
- You can see info regarding the DANE zone for that protocol



Delegate DANE zone

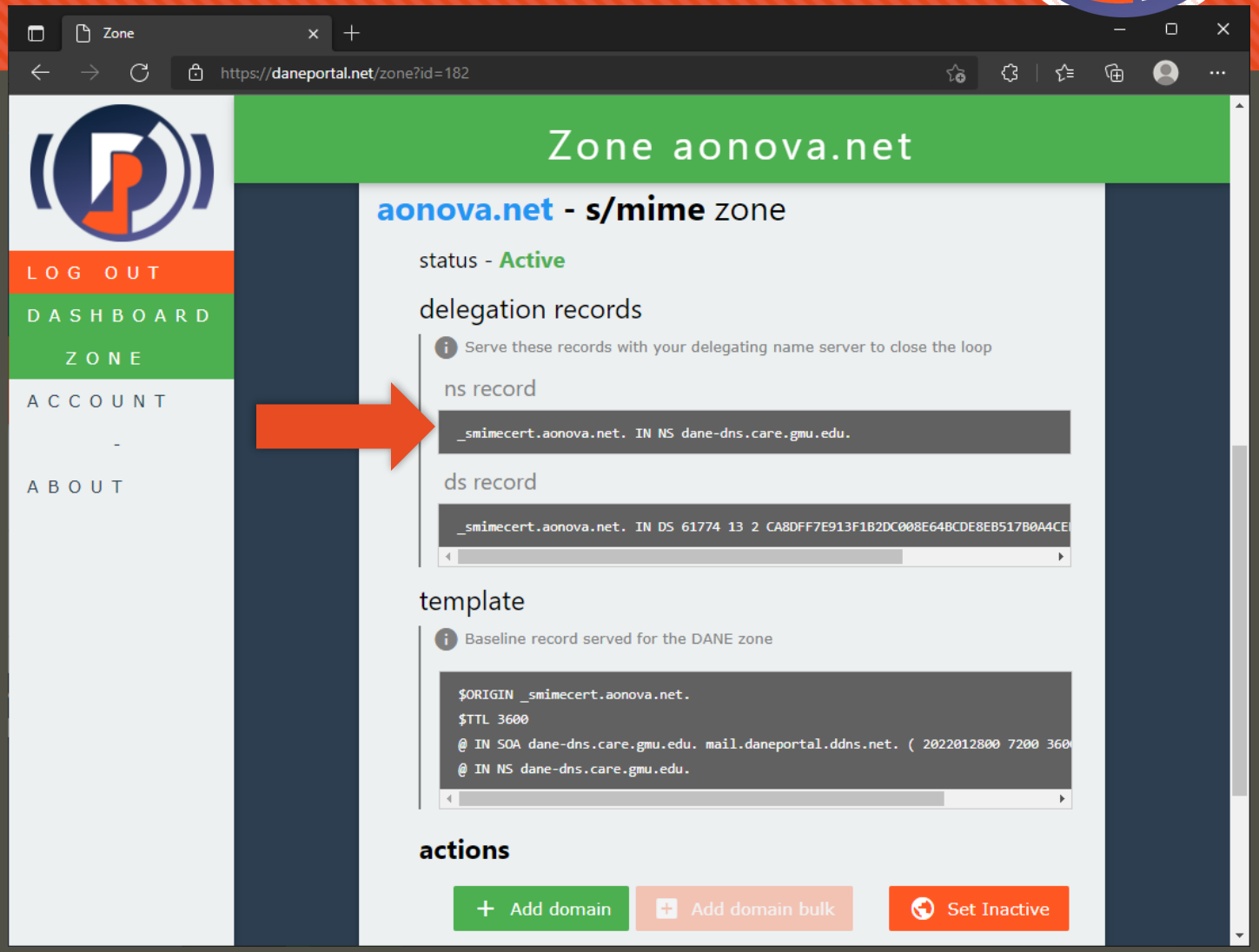
- In order to serve the zone over DNS, you will need to complete the delegation of the DANE zone.
- This involves adding two records (NS and DS) to your zone using your zone management tools.
- Both can be found on the page we are looking at
- The specifics again differ based on your DNS service provider's interface – the following pictures are just for reference



Delegate DANE zone

- The specifics again differ based on your DNS service provider's interface – the pictures are just for reference

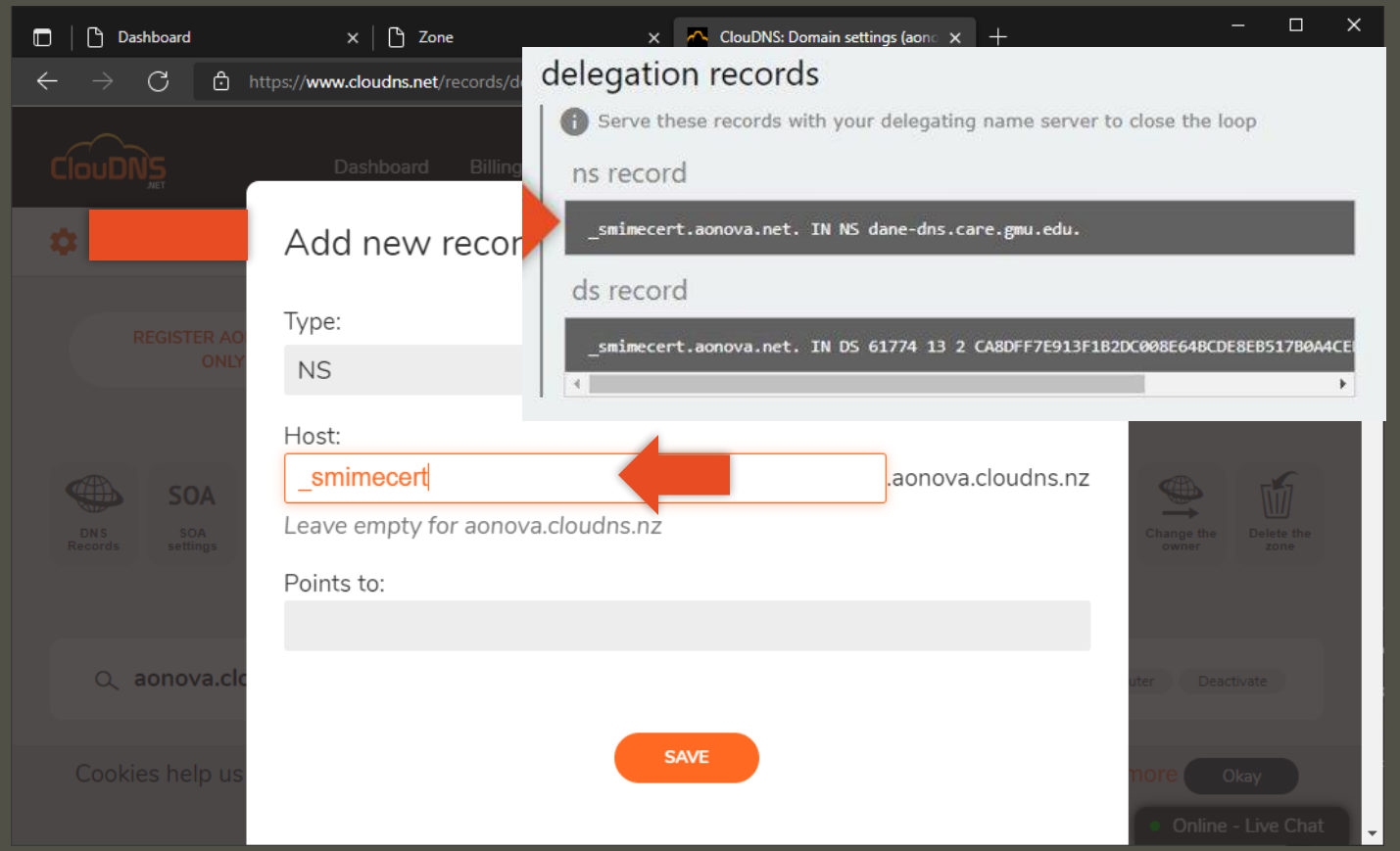
- Step 1: add an NS record for the DANE zone pointing at the DANE portal nameserver.



Delegate DANE zone – add NS rec

- The specifics again differ based on your DNS service provider's interface – the pictures are just for reference

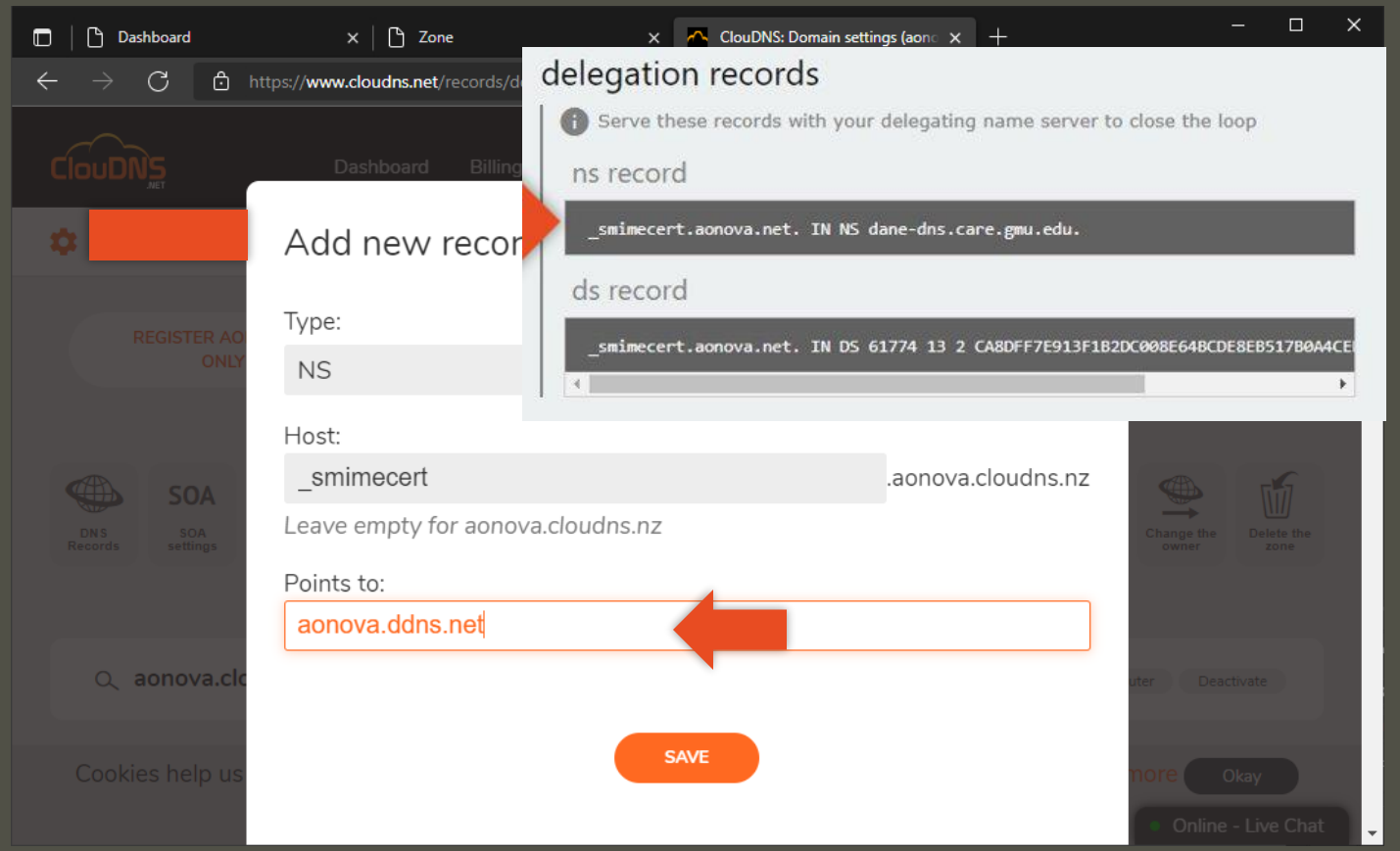
- Step 1: add an NS record for the DANE zone pointing at the DANE portal nameserver.
- You want to basically copy the NS record at the end of the template into your zone
- The DANE zone domain name is dependent on the protocol



Delegate DANE zone – add NS rec

- The specifics again differ based on your DNS service provider's interface – the pictures are just for reference

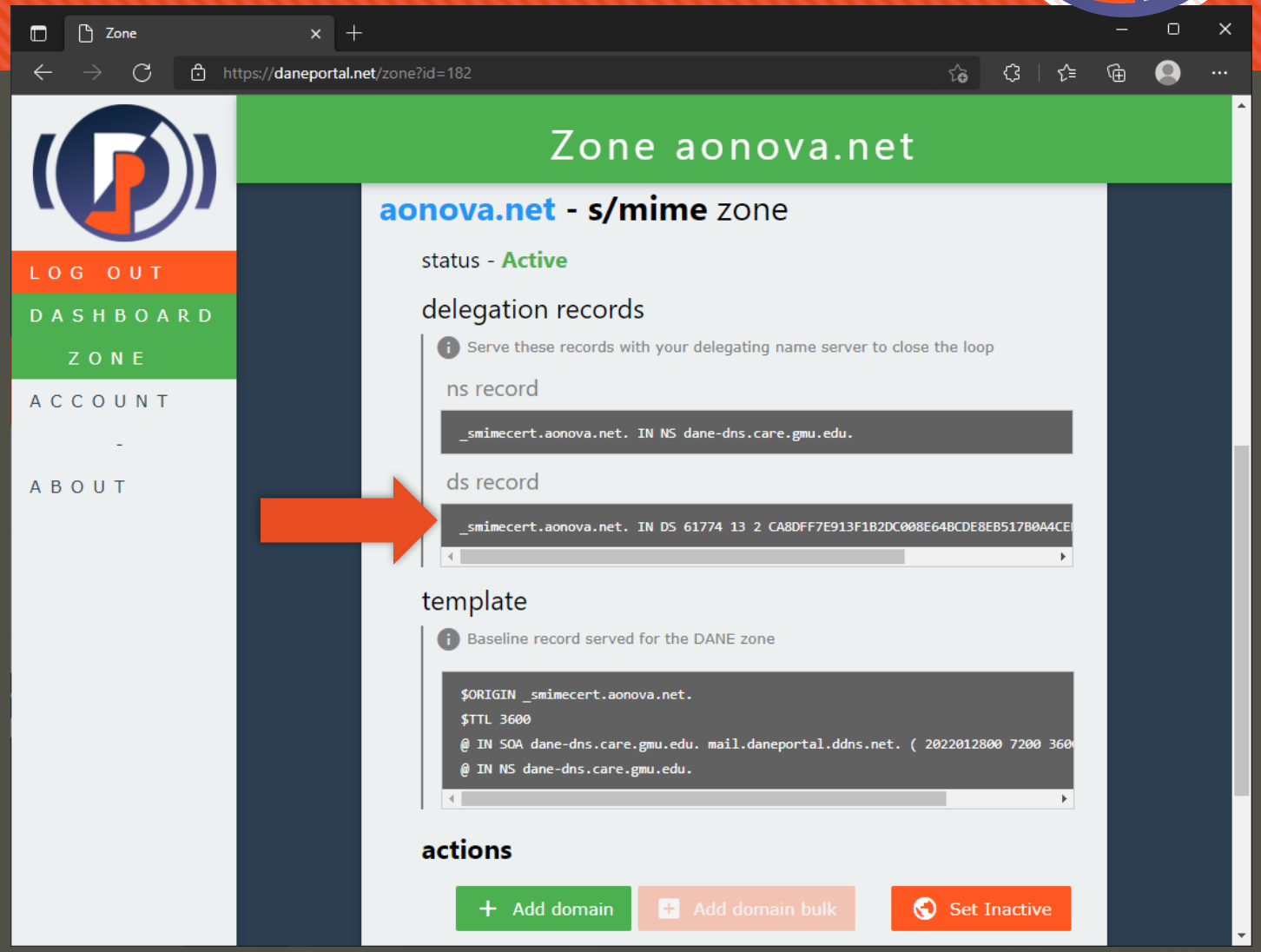
- Step 1: add an NS record for the DANE zone pointing at the DANE portal nameserver.
- You want to basically copy the NS record at the end of the template into your zone



Delegate DANE zone

- The specifics again differ based on your DNS service provider's interface – the pictures are just for reference

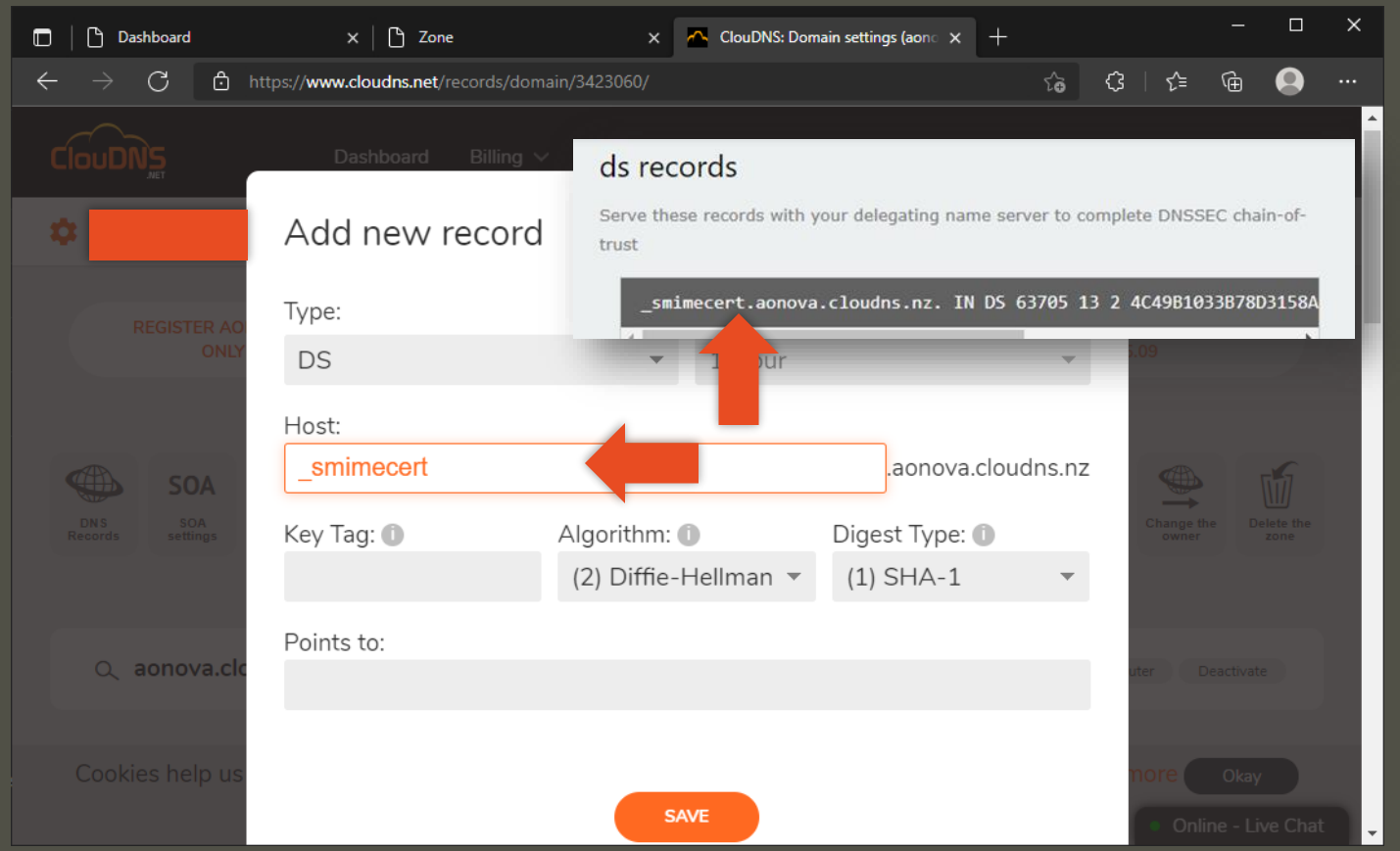
- Step 2: add the DS record for the DANE zone as given in the **ds records section**
- It is possible this wont appear immediately after the zone is made if the system is under load – if so, try refreshing the page until it does.



Delegate DANE zone – add DS rec

- The specifics again differ based on your DNS service provider's interface – the pictures are just for reference

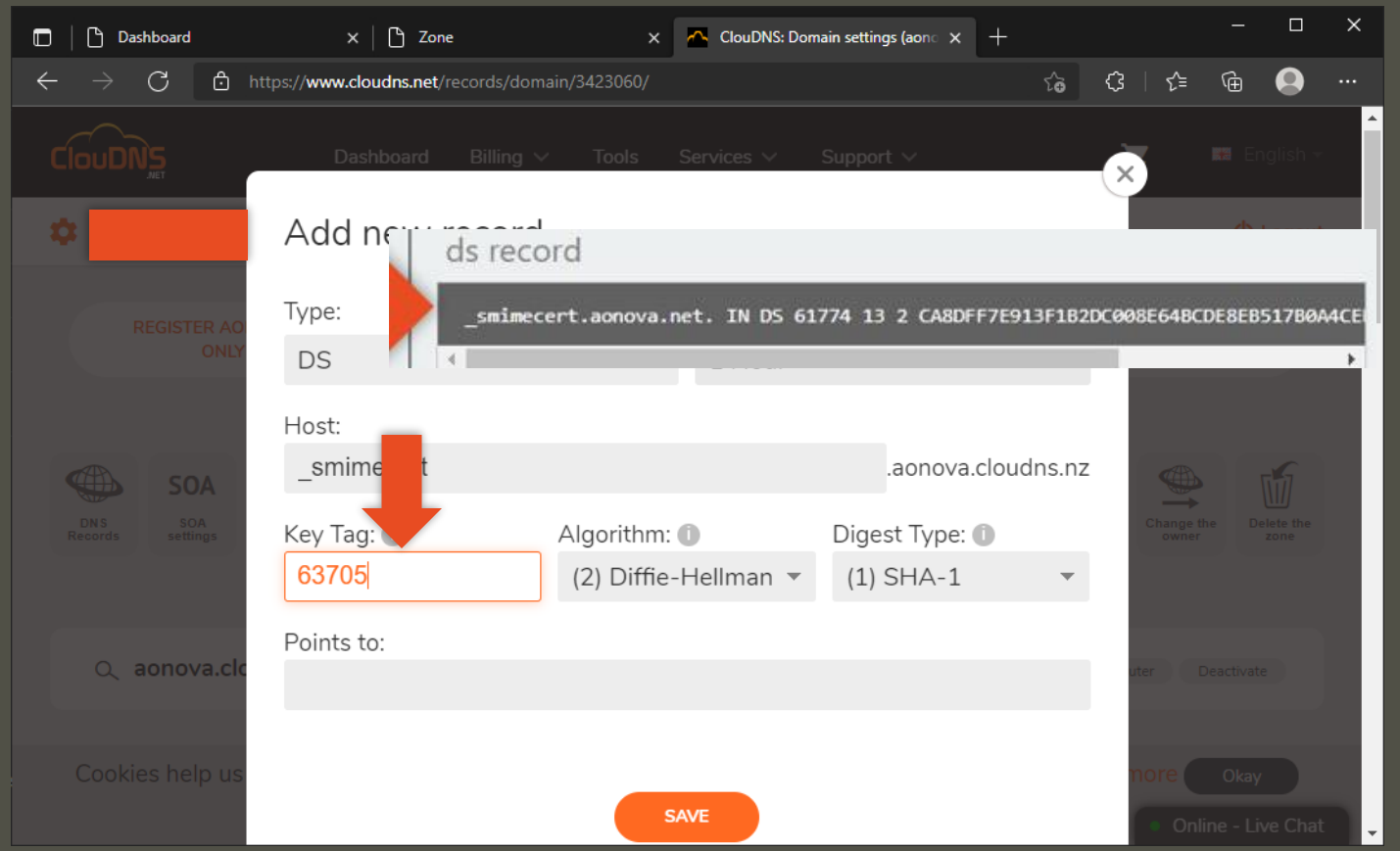
- Step 2: add the DS record for the DANE zone as given in the **ds records section**
- It is possible this wont appear immediately after the zone is made if the system is under load – if so, try refreshing the page until it does.



Delegate DANE zone – add DS rec

- The specifics again differ based on your DNS service provider's interface – the pictures are just for reference

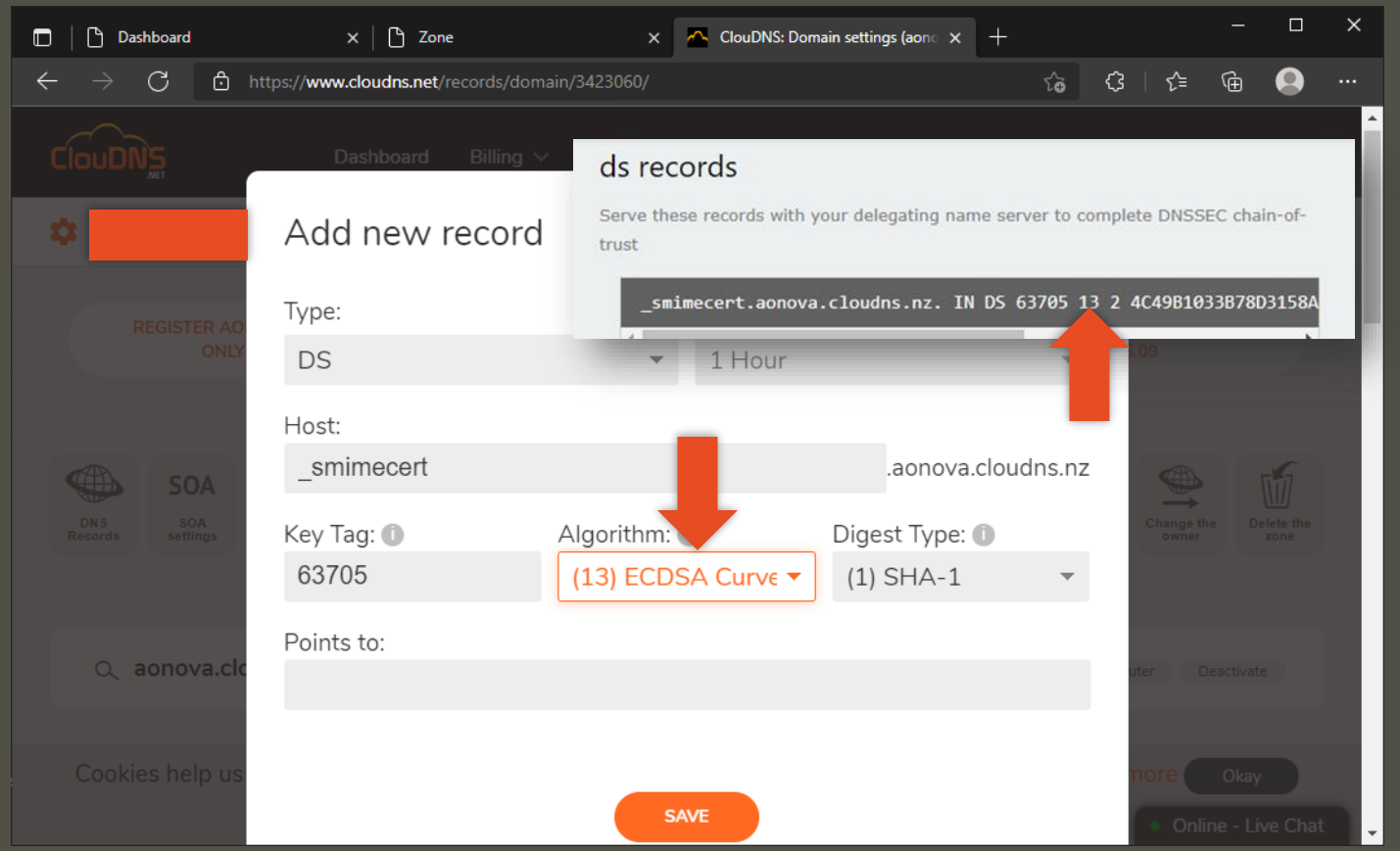
- Step 2: add the DS record for the DANE zone as given in the **ds records section**
- It is possible this wont appear immediately after the zone is made if the system is under load – if so, try refreshing the page until it does.



Delegate DANE zone – add DS rec

- The specifics again differ based on your DNS service provider's interface – the pictures are just for reference

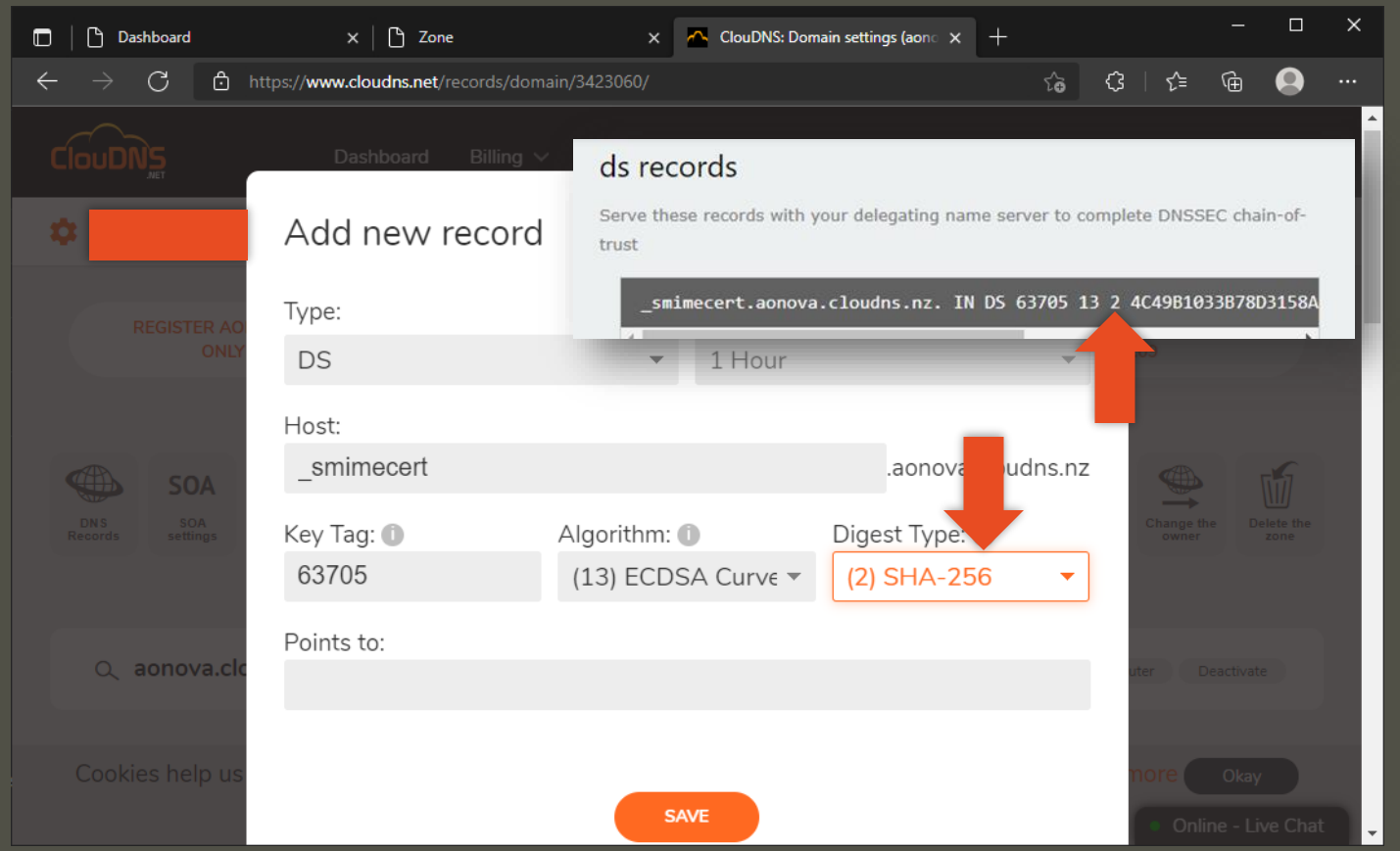
- Step 2: add the DS record for the DANE zone as given in the **ds records section**
- It is possible this wont appear immediately after the zone is made if the system is under load – if so, try refreshing the page until it does.



Delegate DANE zone – add DS rec

- The specifics again differ based on your DNS service provider's interface – the pictures are just for reference

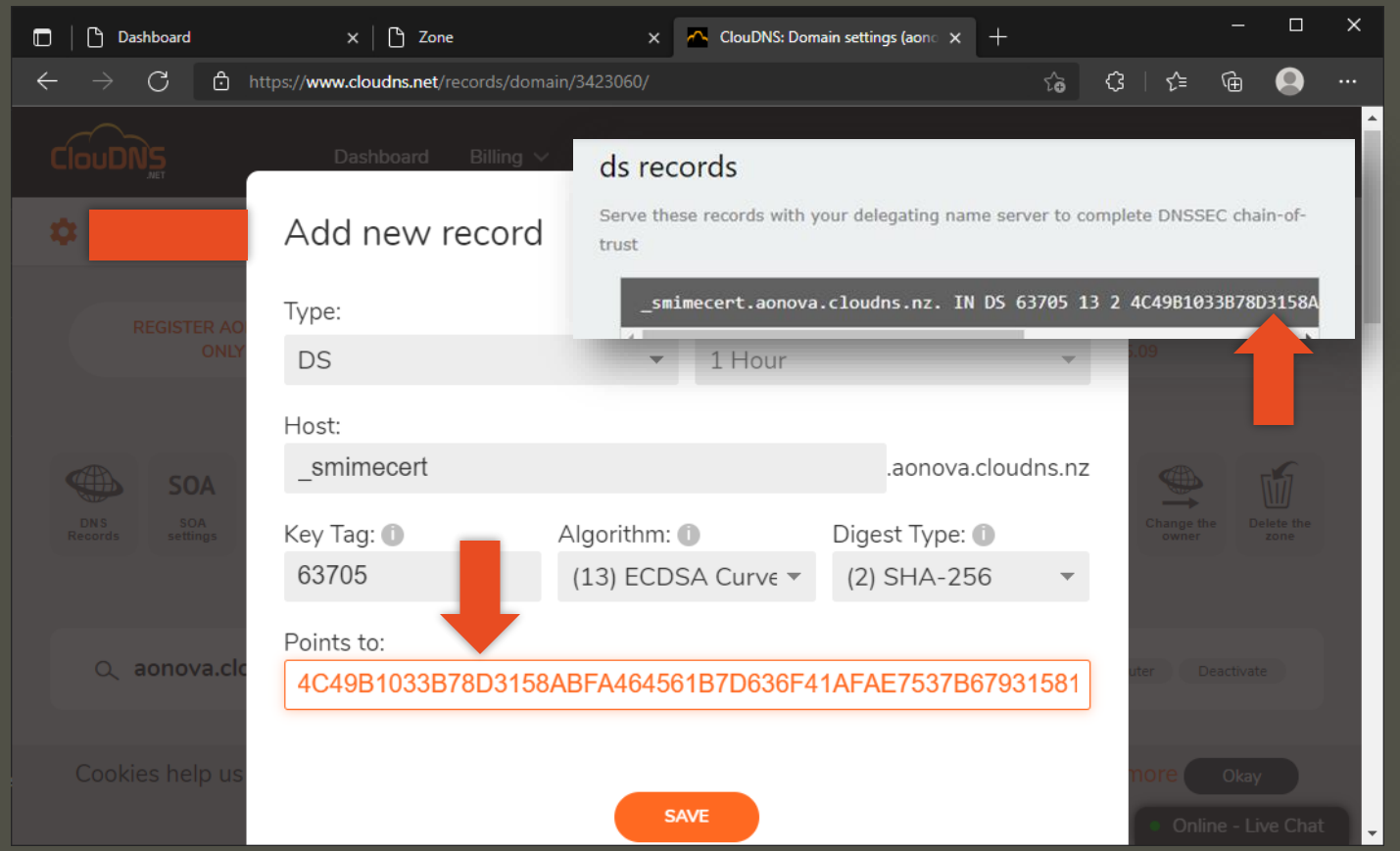
- Step 2: add the DS record for the DANE zone as given in the **ds records section**
- It is possible this wont appear immediately after the zone is made if the system is under load – if so, try refreshing the page until it does.



Delegate DANE zone – add DS rec

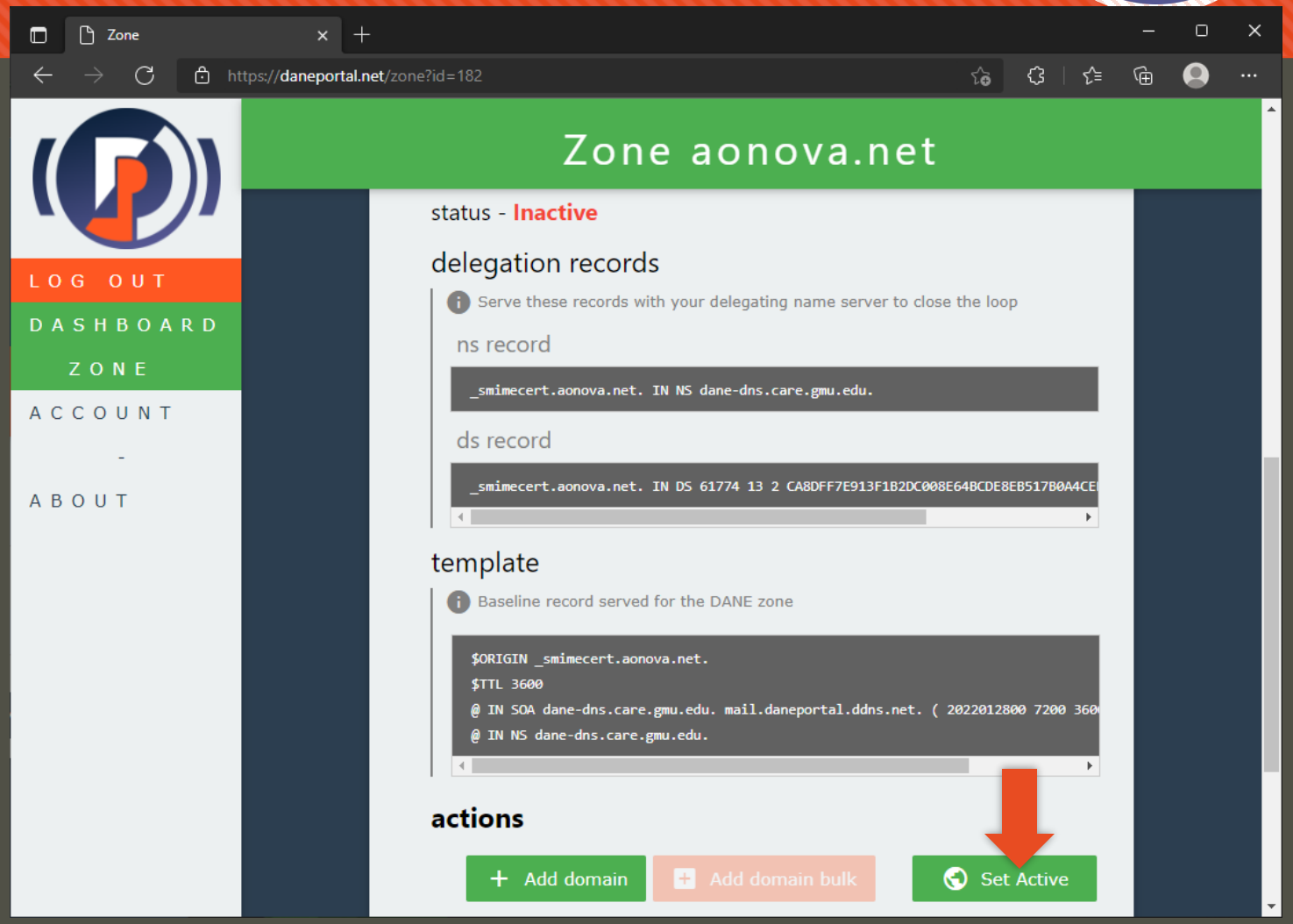
- The specifics again differ based on your DNS service provider's interface – the pictures are just for reference

- Step 2: add the DS record for the DANE zone as given in the **ds records section**
- It is possible this wont appear immediately after the zone is made if the system is under load – if so, try refreshing the page until it does.



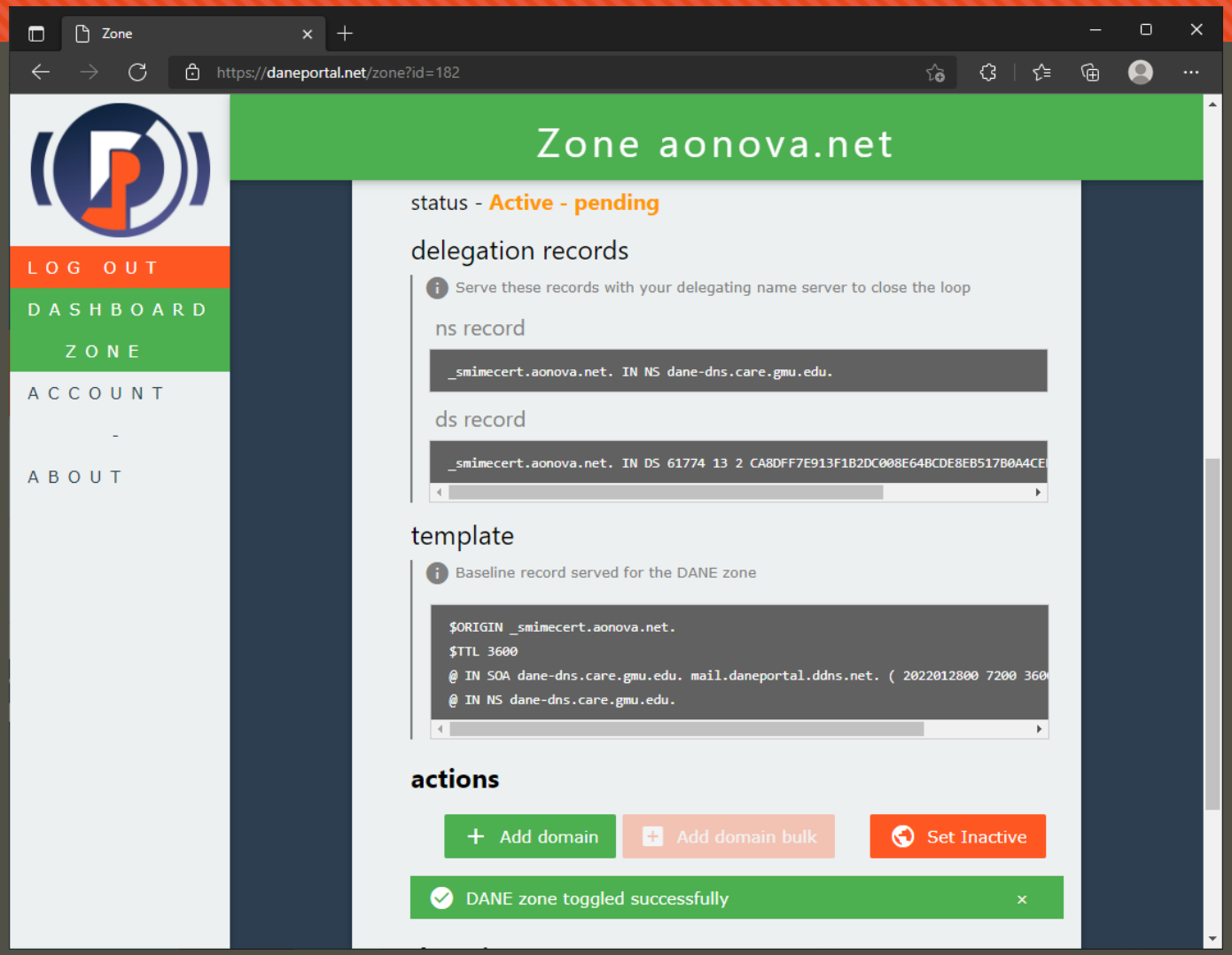
Delegate DANE zone – activate

- To start serving the DANE zone, click [Set Active]
- This will queue the DANE zone to be served by the DANE portal nameservers.
- If this fails or hangs, try refreshing the page. For security the login sessions are time-gated, so you may need to re-log in if you leave this page open too long



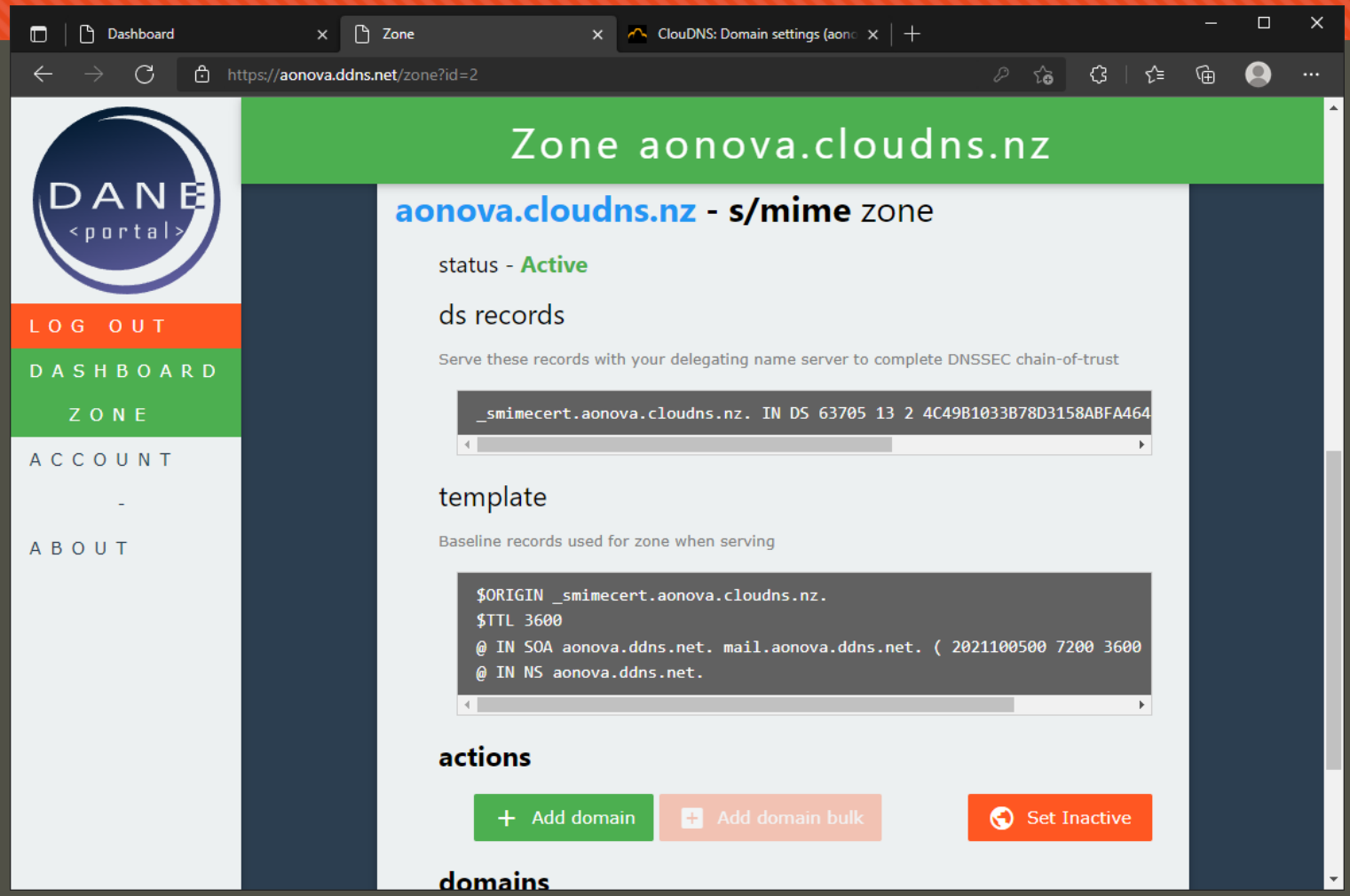
Delegate DANE zone – activate

- To start serving the DANE zone, click [Set Active]
- This will queue the DANE zone to be served by the DANE portal nameservers.
- You can toggle the active state at any time with that button
- When **active**, the DANE zone is accessible on the DNS
- Refresh the page until the **status** says Active



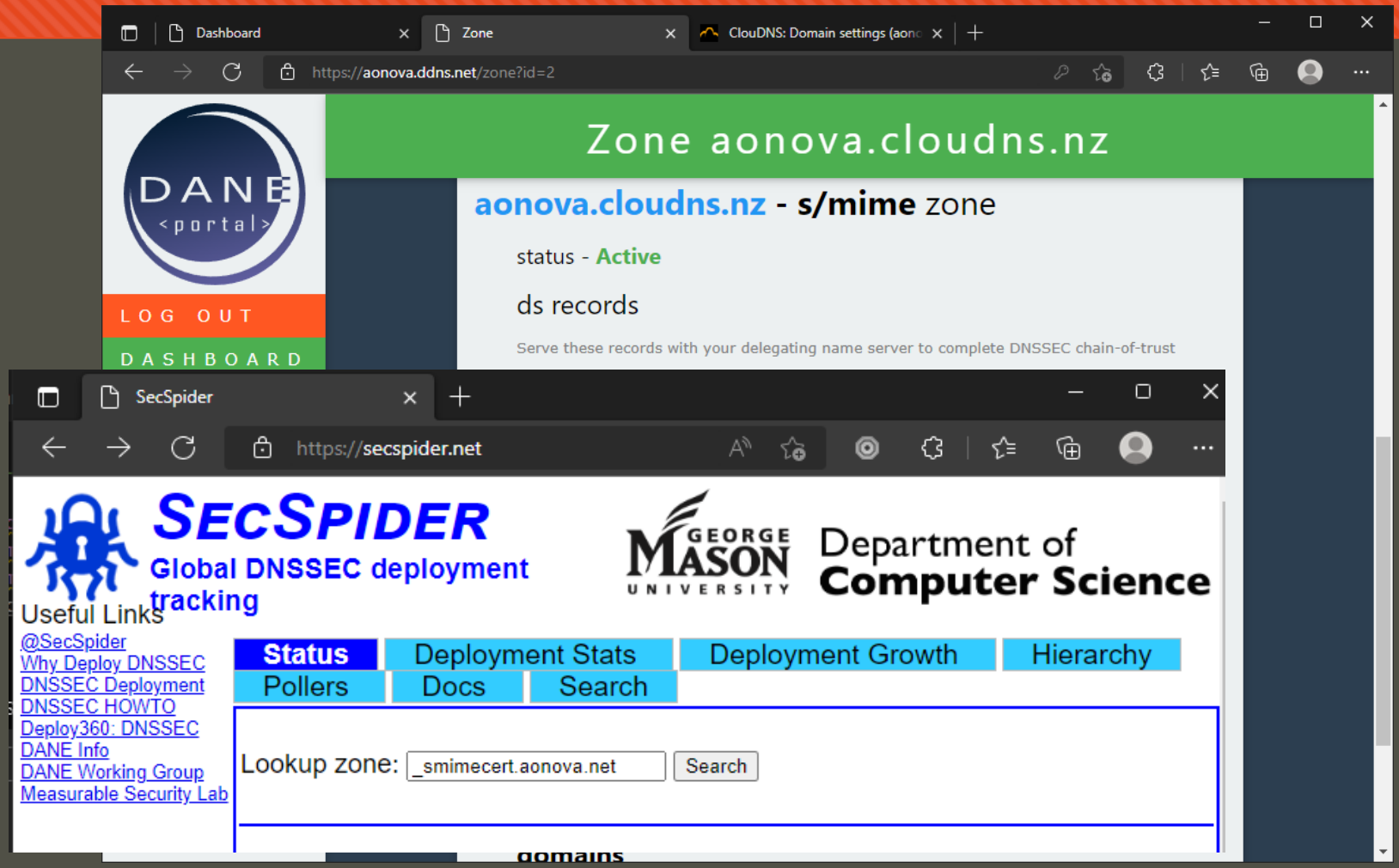
Delegate DANE zone - testing

- It may require refreshing the page before the **status** shows Active
- Now, assuming your delegation works, the DANE zone is public on DNS and available to handle DANE queries.



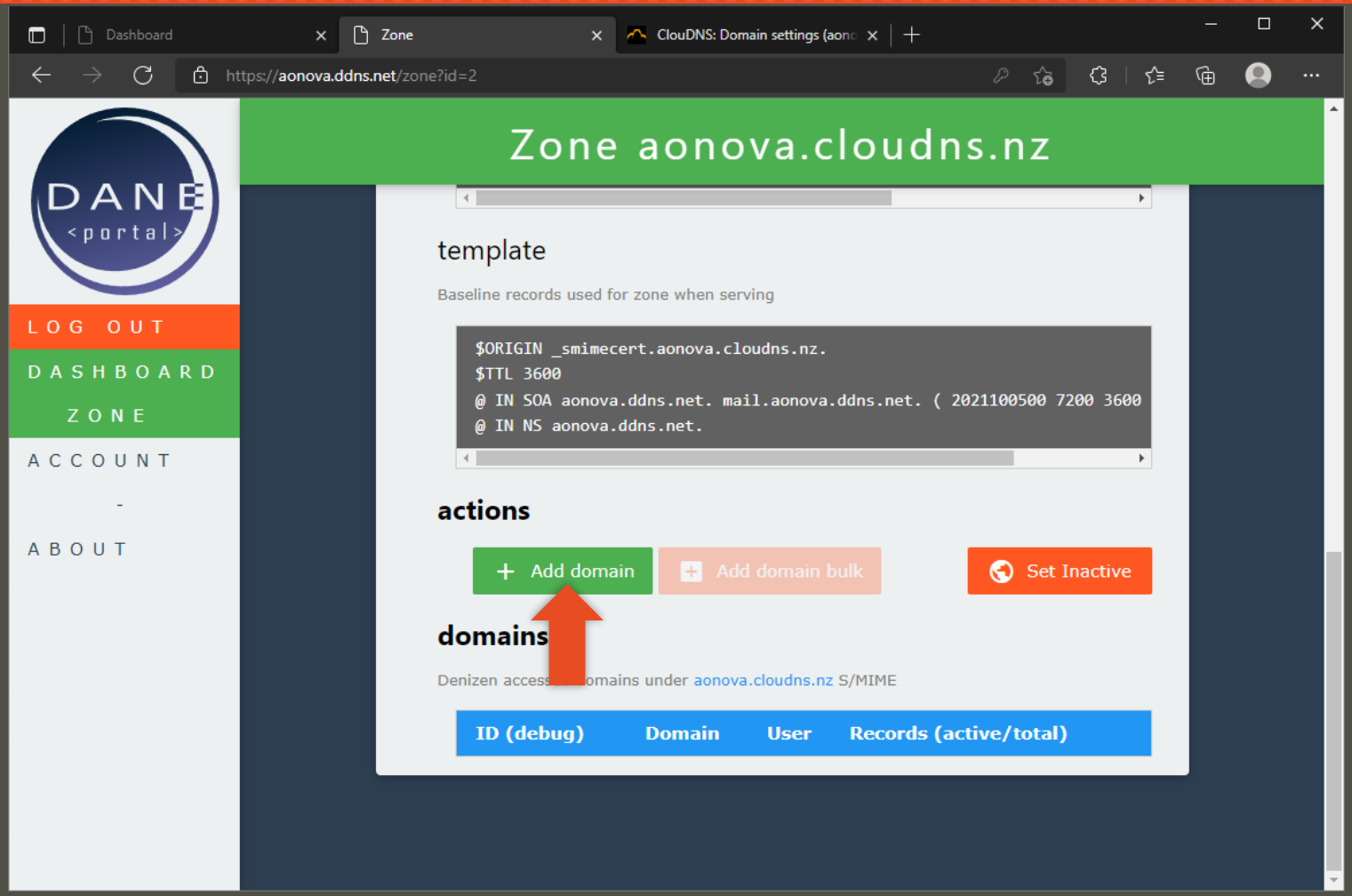
Delegate DANE zone - testing

- It may require refreshing the page before the **status** says Active
- Now, assuming your delegation works, the DANE zone is public on DNS and available to handle DANE queries.
- To check that your delegation was successful, use a tool such as secspider.net, searching for the DANE zone



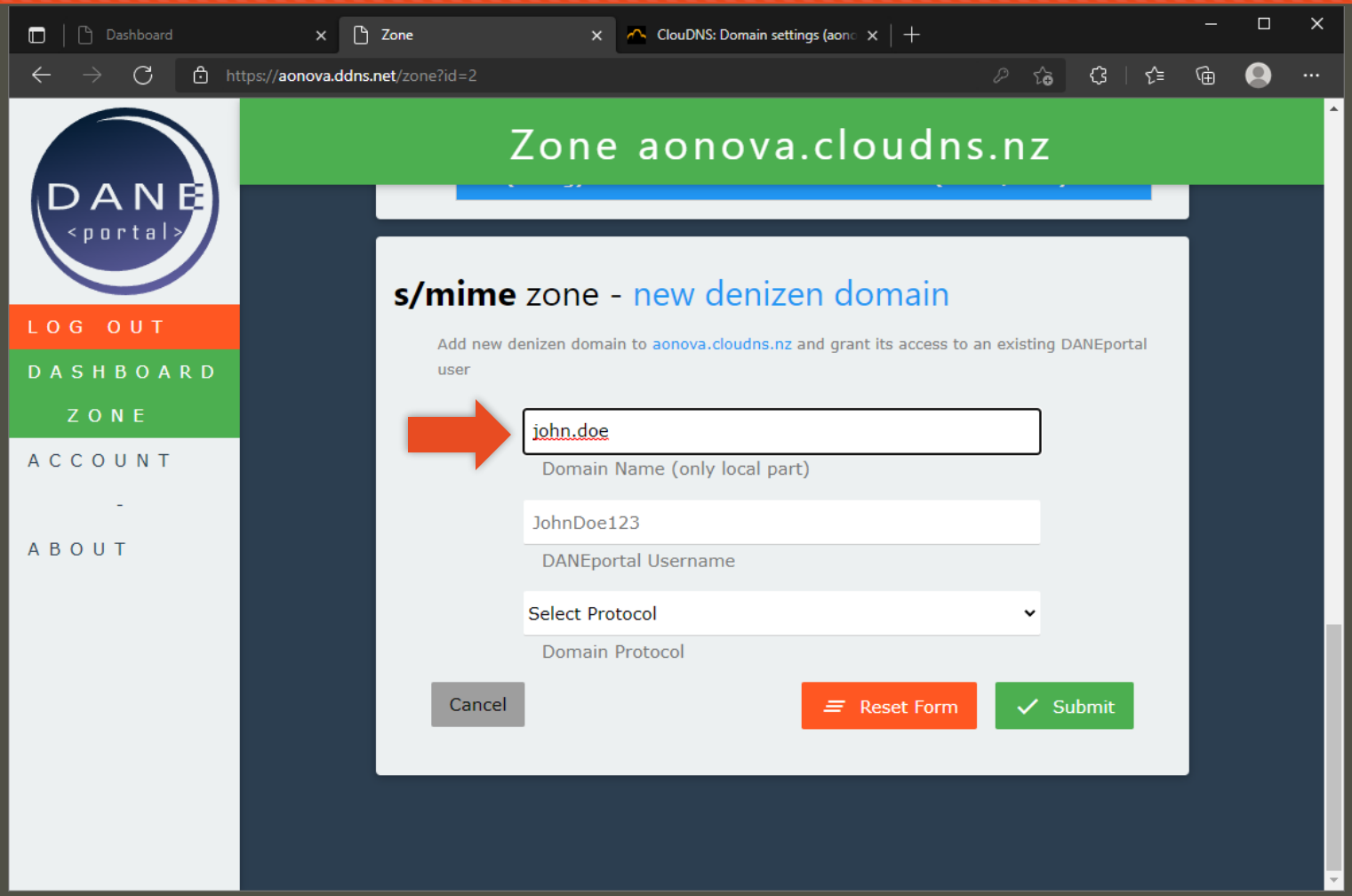
Delegate denizen domain

- **Denizen Users** are non-admin users who are given the ability to add specific records under the DANE zone. This functionality in DANE portal reflects the federated capability of DANE.
- In the context of DANE SMIME, the **denizens are your email users** – you must delegate a domain to allow them to add their SMIME certificates to your DANE zone without you losing any of your control as zone admin.
- Click [Add domain] to open the form



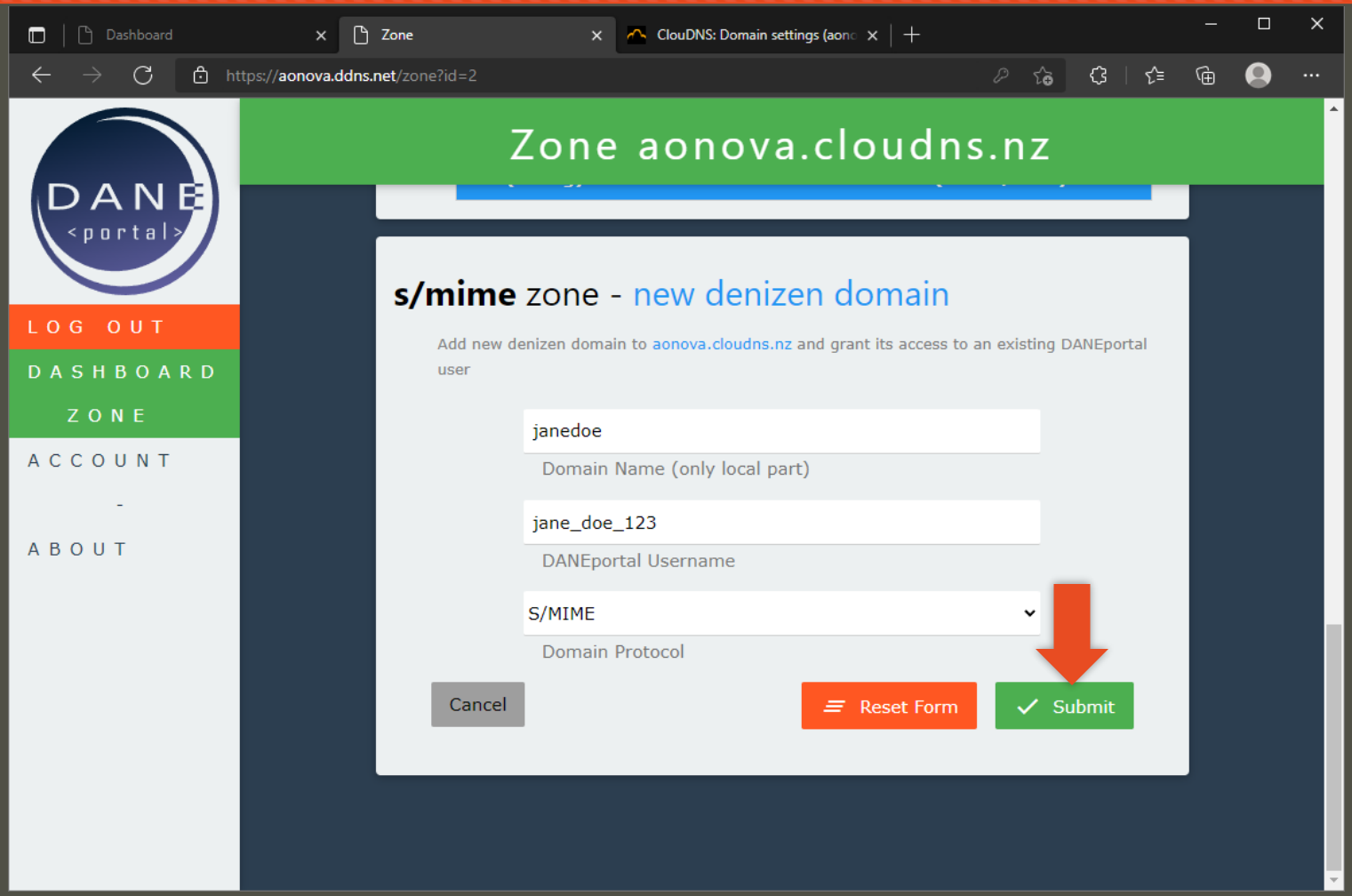
Delegate denizen domain

- Using this form, submit the information for **each email user under your zone** that you would like to use DANE SMIME
- A bulk denizen registration system is in the works – but currently you will need to fill this form for every email user you want to give access
- The denizen domain name should be the left-hand-side of the user's email address
  - e.g. john.doe@aonova.cloudns.nz → john.doe
- Some conversion may be necessary for exotic emails (RFC recommendations) – in the future a more purpose-built registration form will be adopted that handles this.



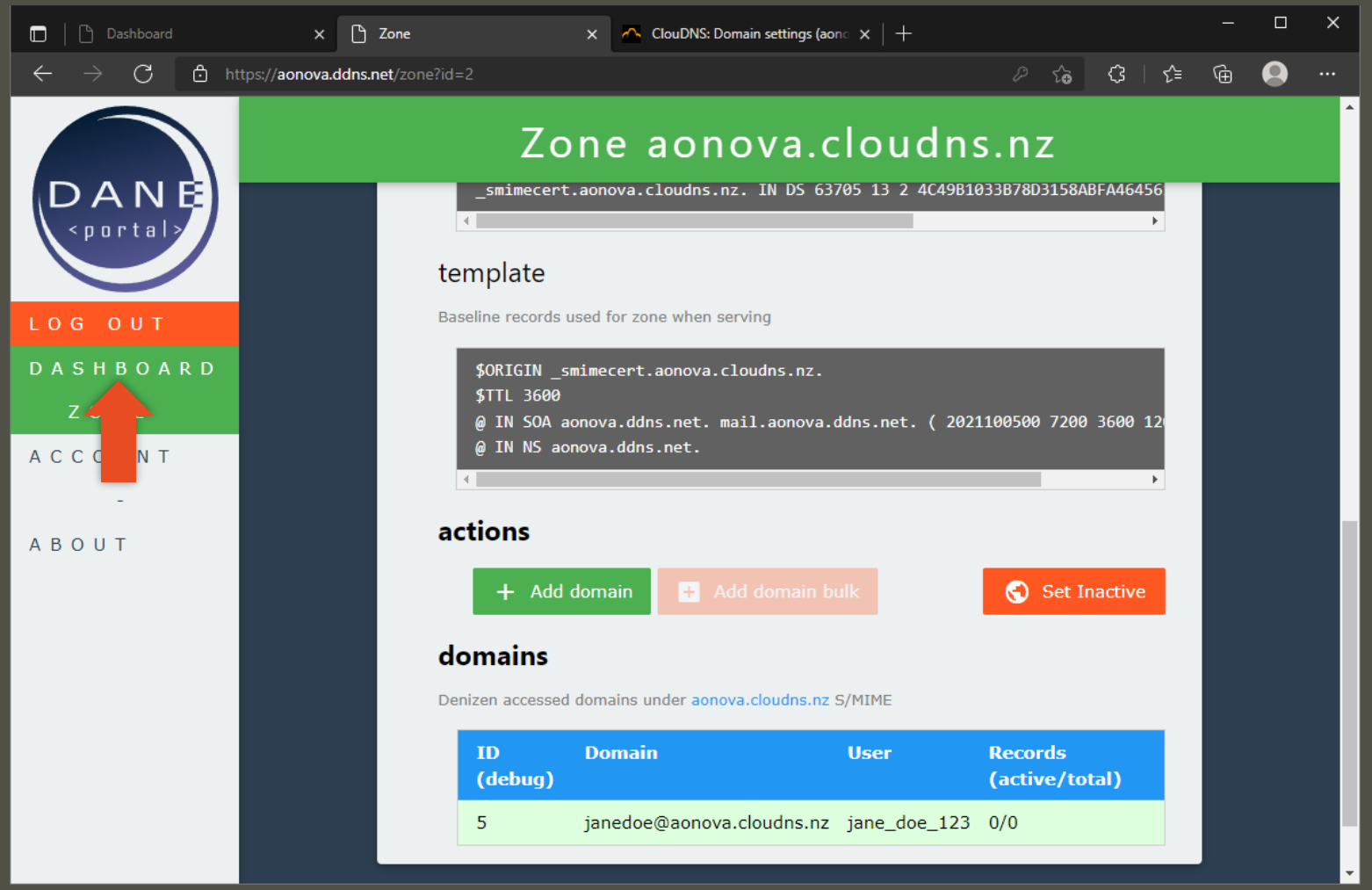
Delegate denizen domain

- Using this form, submit the information for **each email user under your zone** that you would like to use DANE SMIME
- Enter the DANE portal username for your email user if they have an account already
  - You can go back and create a new one for them and give them the credentials out-of-band. An automated bulk registration flow is anticipated as a future development
- Be your first user! Add your own email and username for this example
- Click [Submit] to add the denizen



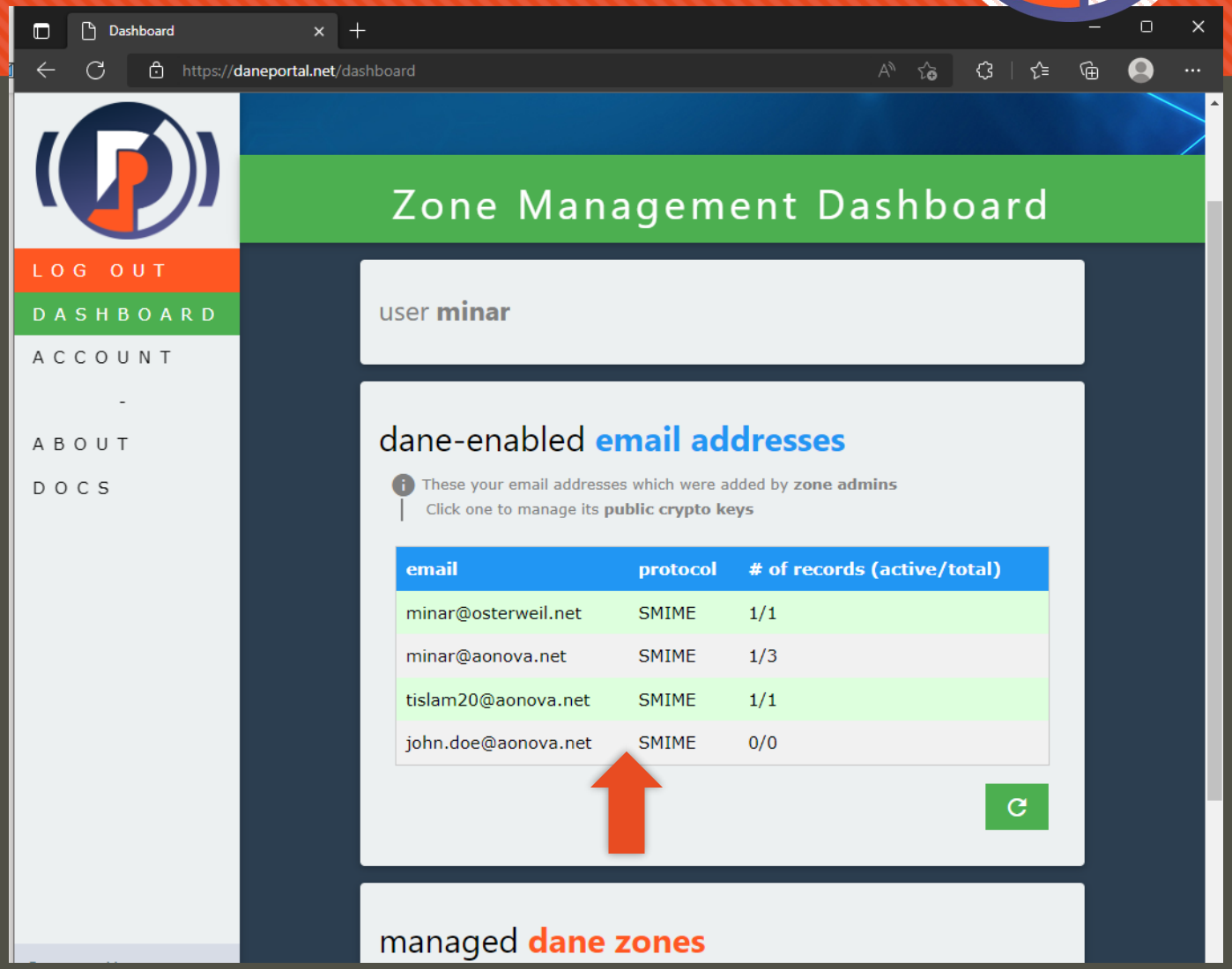
Delegate denizen domain

- You should now see the domain listed
- At this point the user of that denizen domain would have access to it on their own DANE portal dashboard
- Since you added yourself, go back to the dashboard by clicking [Dashboard] on the navbar



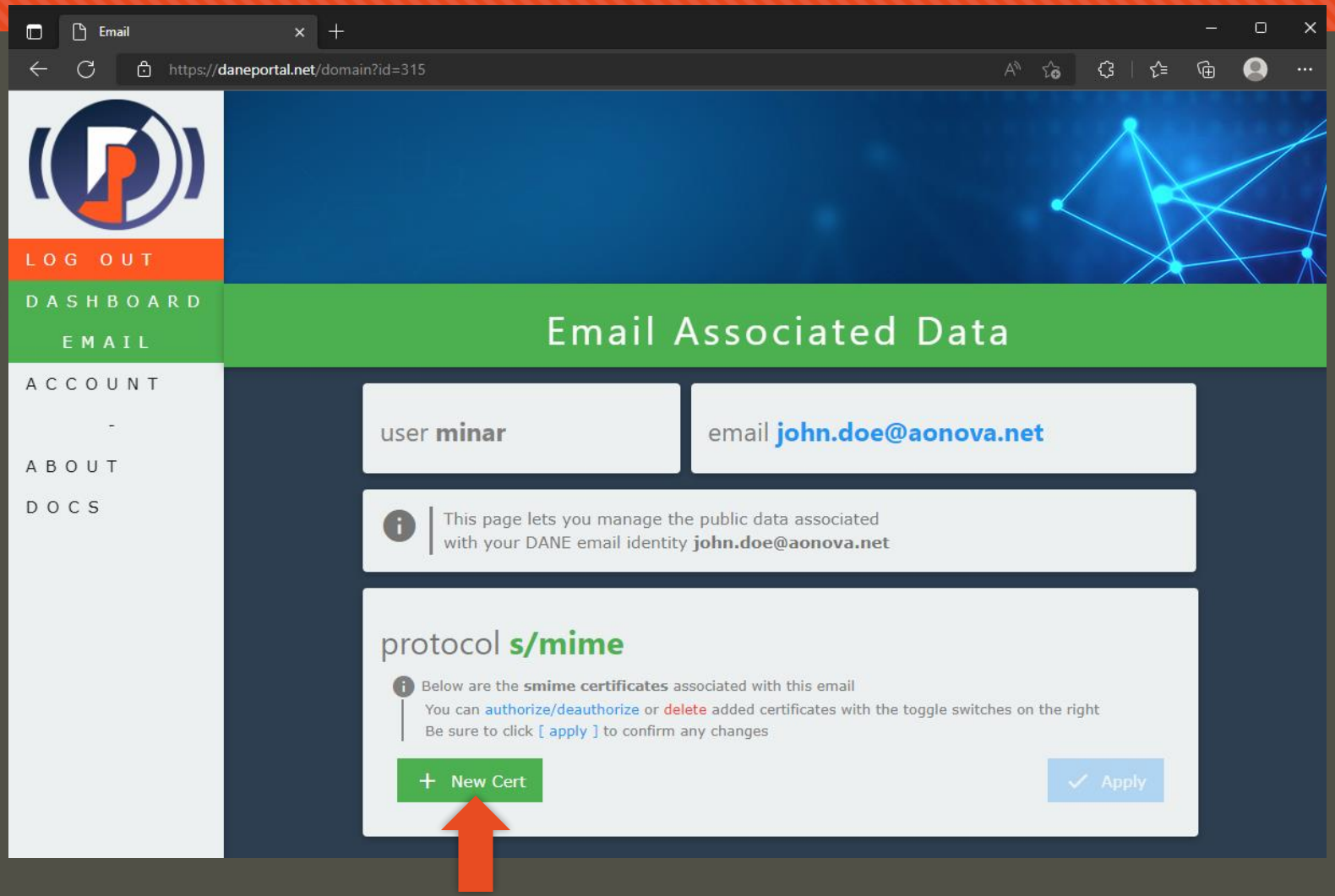
Access denizen domain

- On the main dashboard, you should now see the email listed under the **dane-enabled email addresses** list
- Clicking the item will open the email certificate management page
- For the purpose of this guide, we will now assume the perspective of a **denizen user**



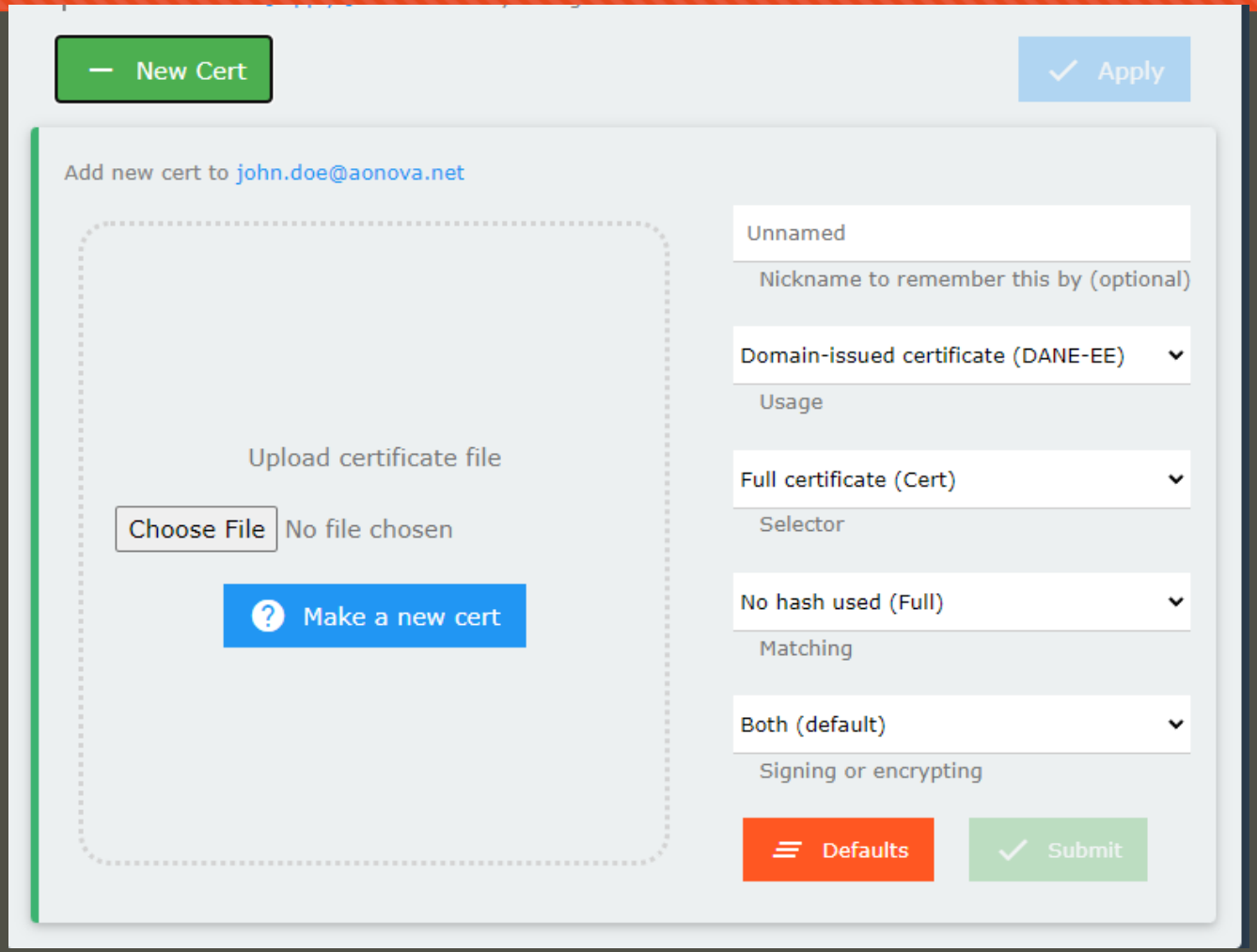
Access denizen domain

- Here email users can add / remove and view the data visible under their denizen domain
- In this case the data are DANE SMIME records representing certs or hashes
- Click [Add cert] to open the form



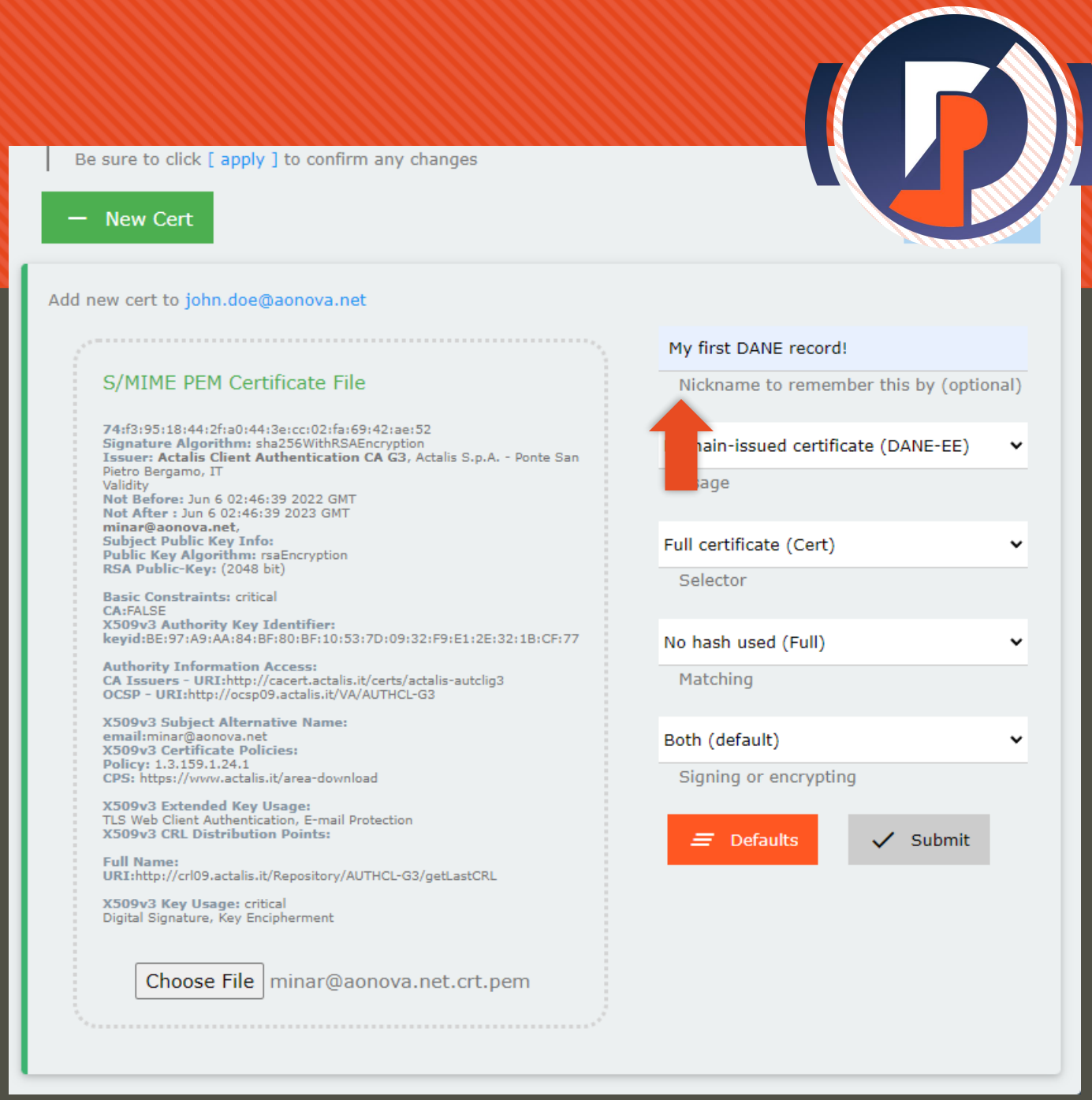
Add record

- Fill in the info for your SMIME DANE record
- If you need a simple SMIME cert/key for testing, feel free to generate one online using the [Make a new cert] tool
- Certificate files can be in the standard PEM or DER format



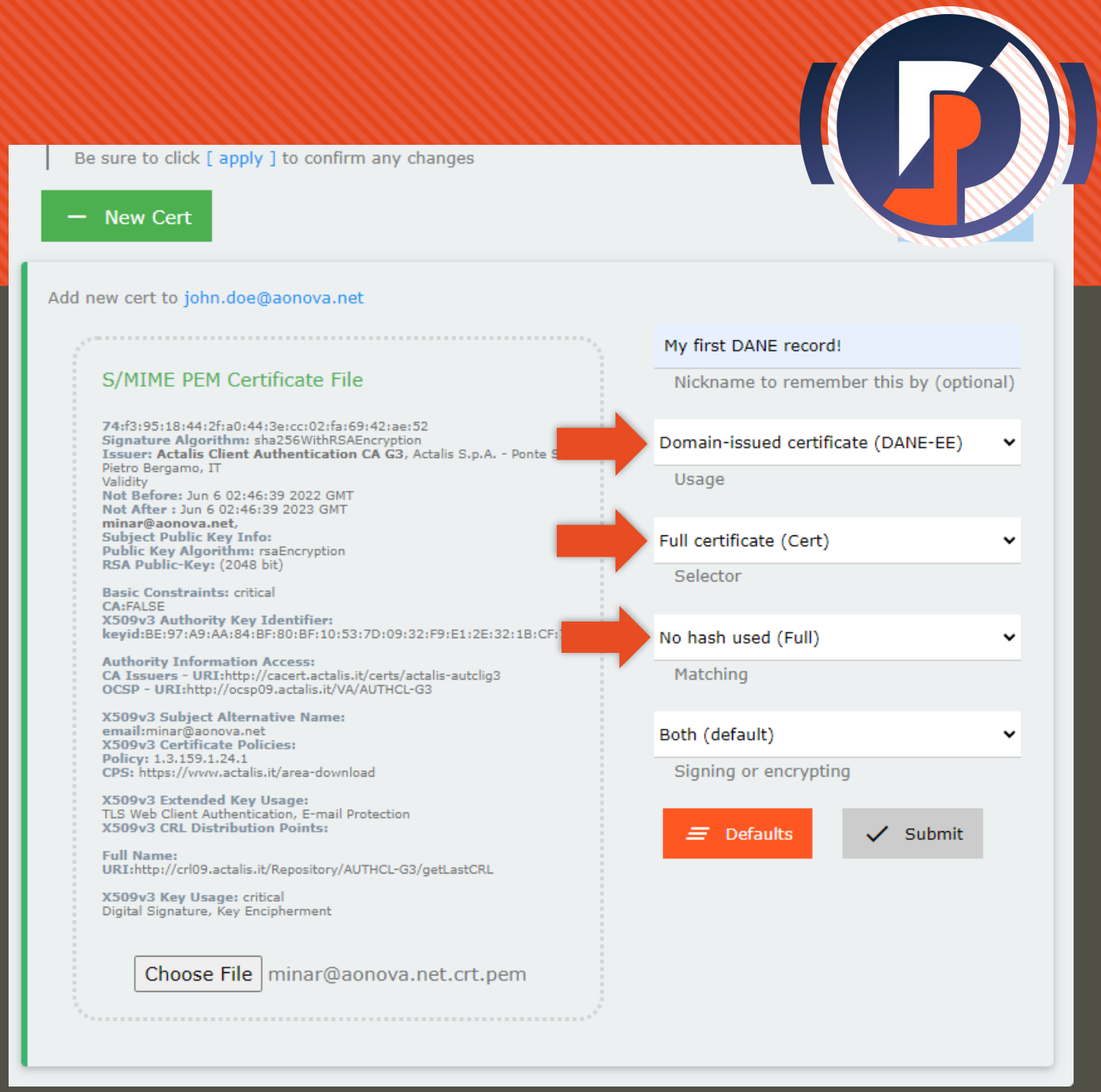
Add record

- Fill in the info for your SMIME DANE record
- Give it a memorable nickname that will be used when dealing with the record on the portal in the future



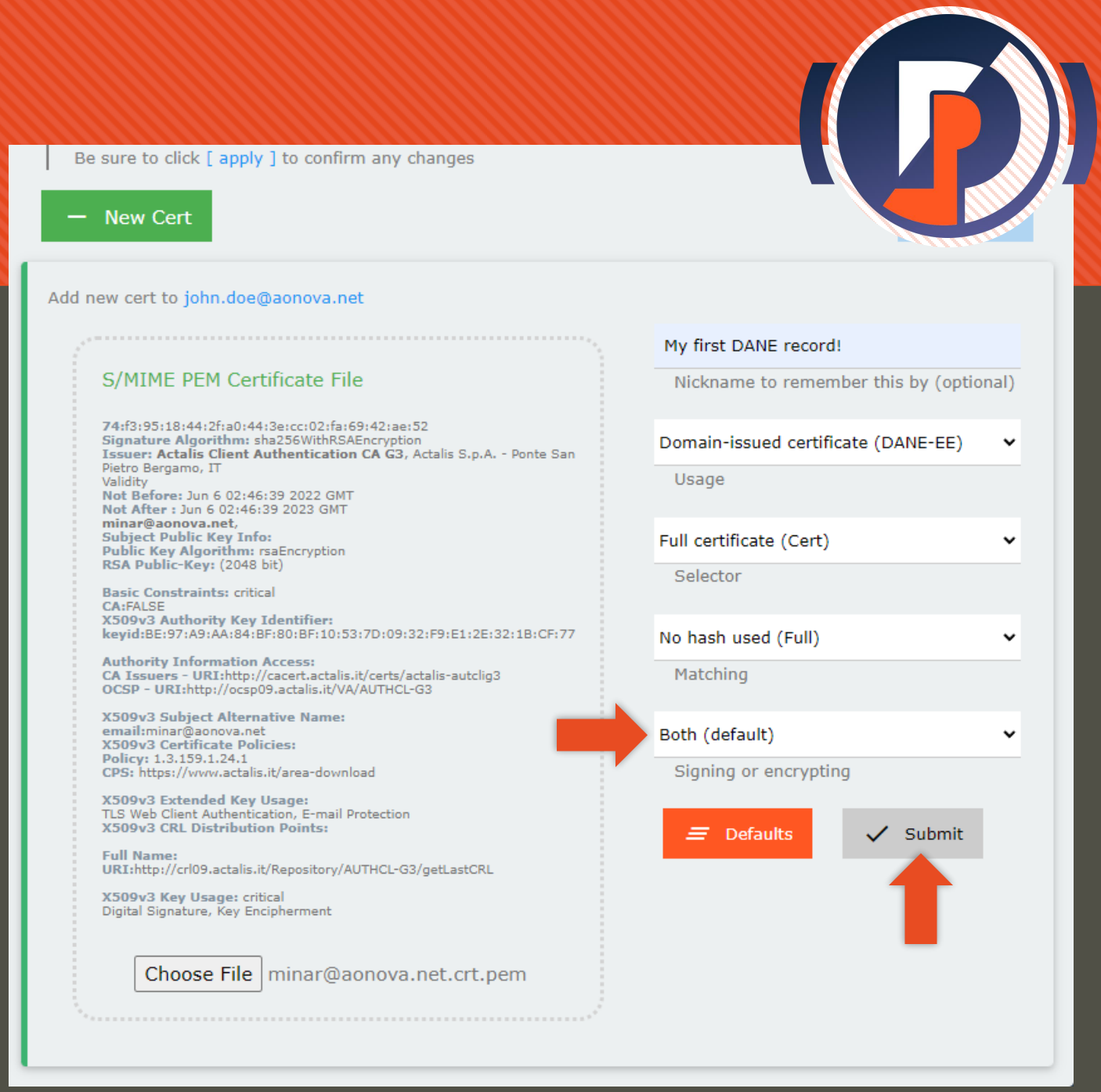
Add record

- Fill in the info for your SMIME DANE record
- Choose the DANE record options that match the cert you uploaded
- Using the defaults for **Usage**, **Selector**, and **Matching** is good for testing as it is most expressive and permissive



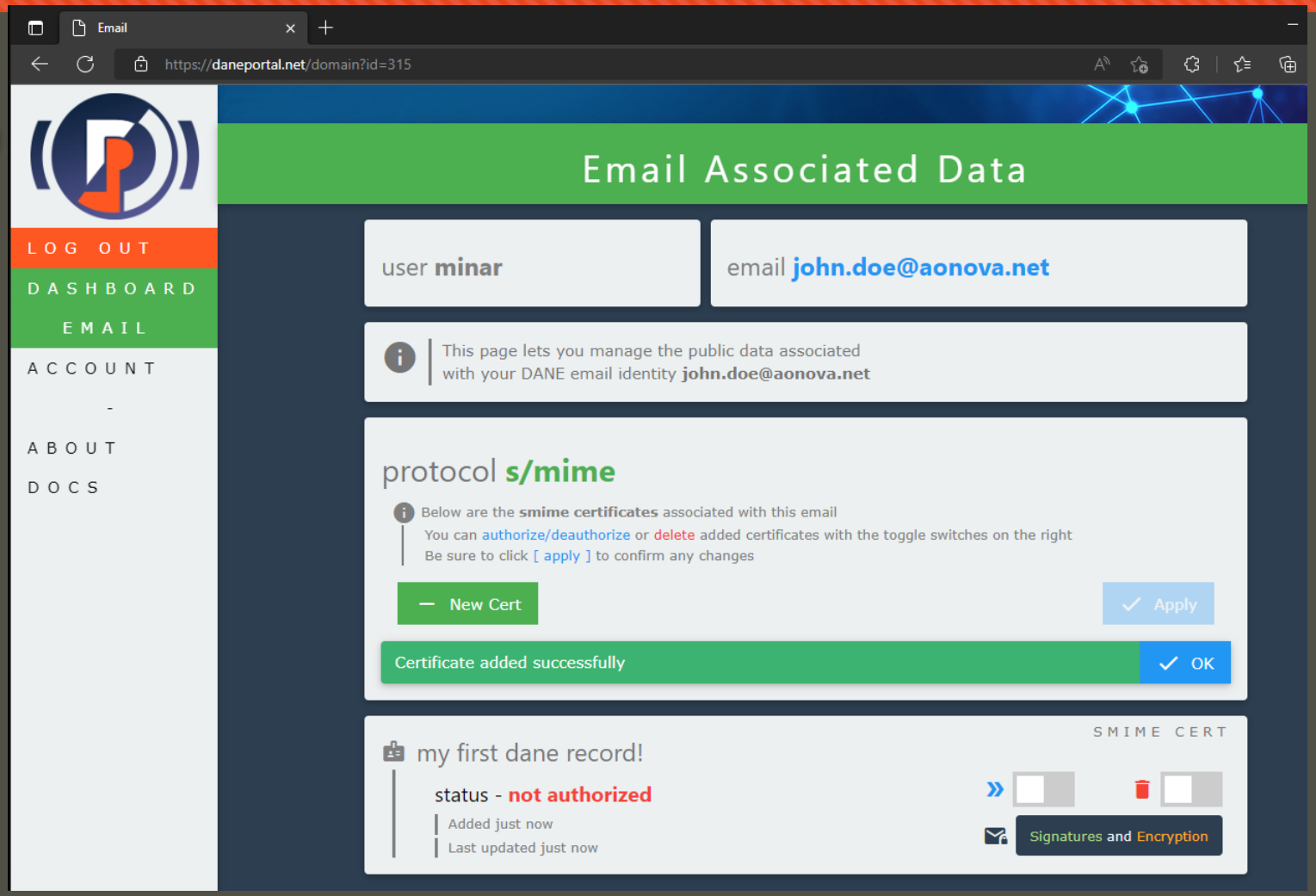
Add record

- Fill in the info for your SMIME DANE record
- Specify if this cert should only be used for verifying your signatures or encrypting messages for you
- This option can be changed at any time after the cert is added as well
- Click [Submit] once done



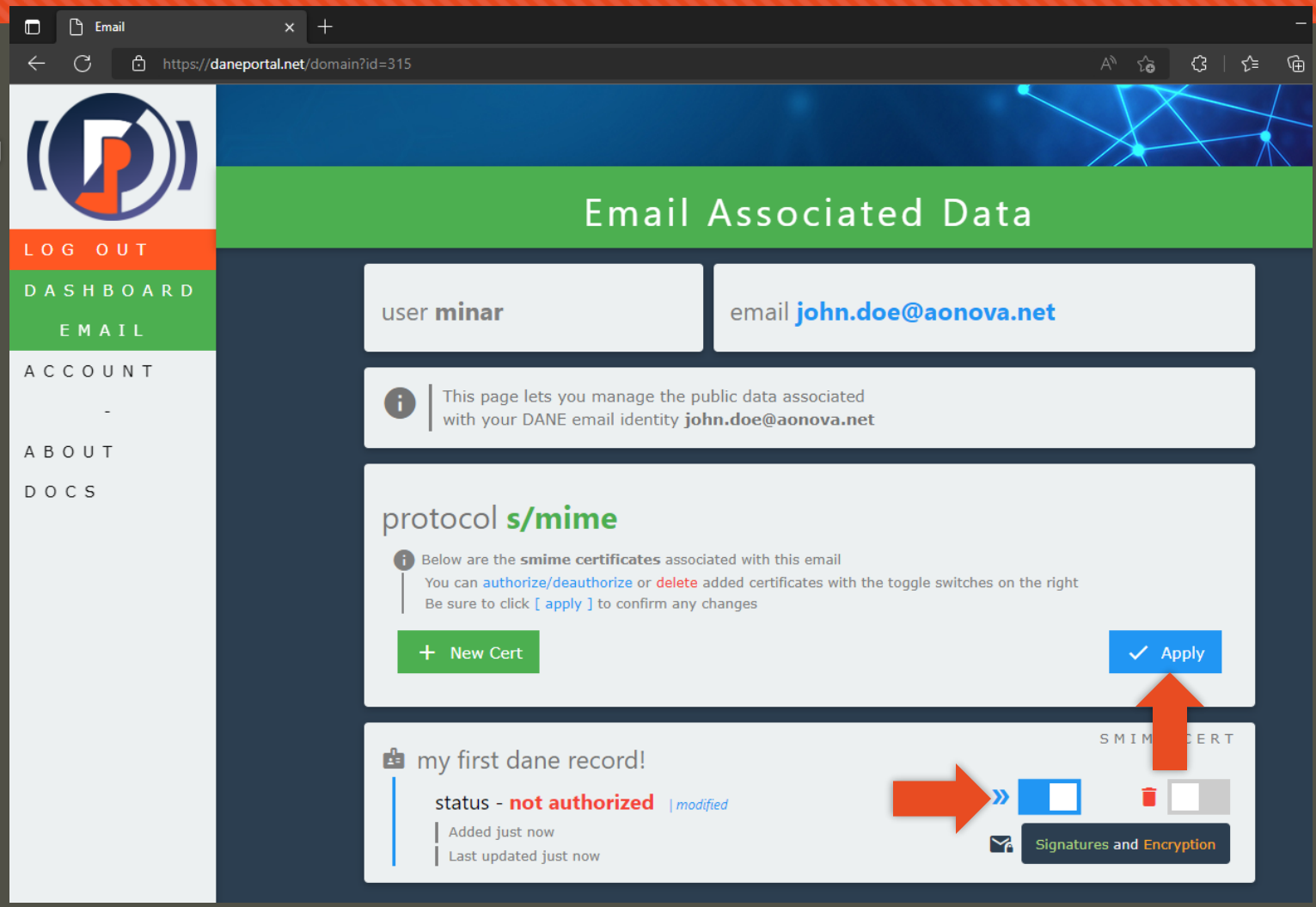
View record

- You should now see a **card representing the record you just added**
- You can manage records here, by toggling its authorization state or deleting it permanently



View record

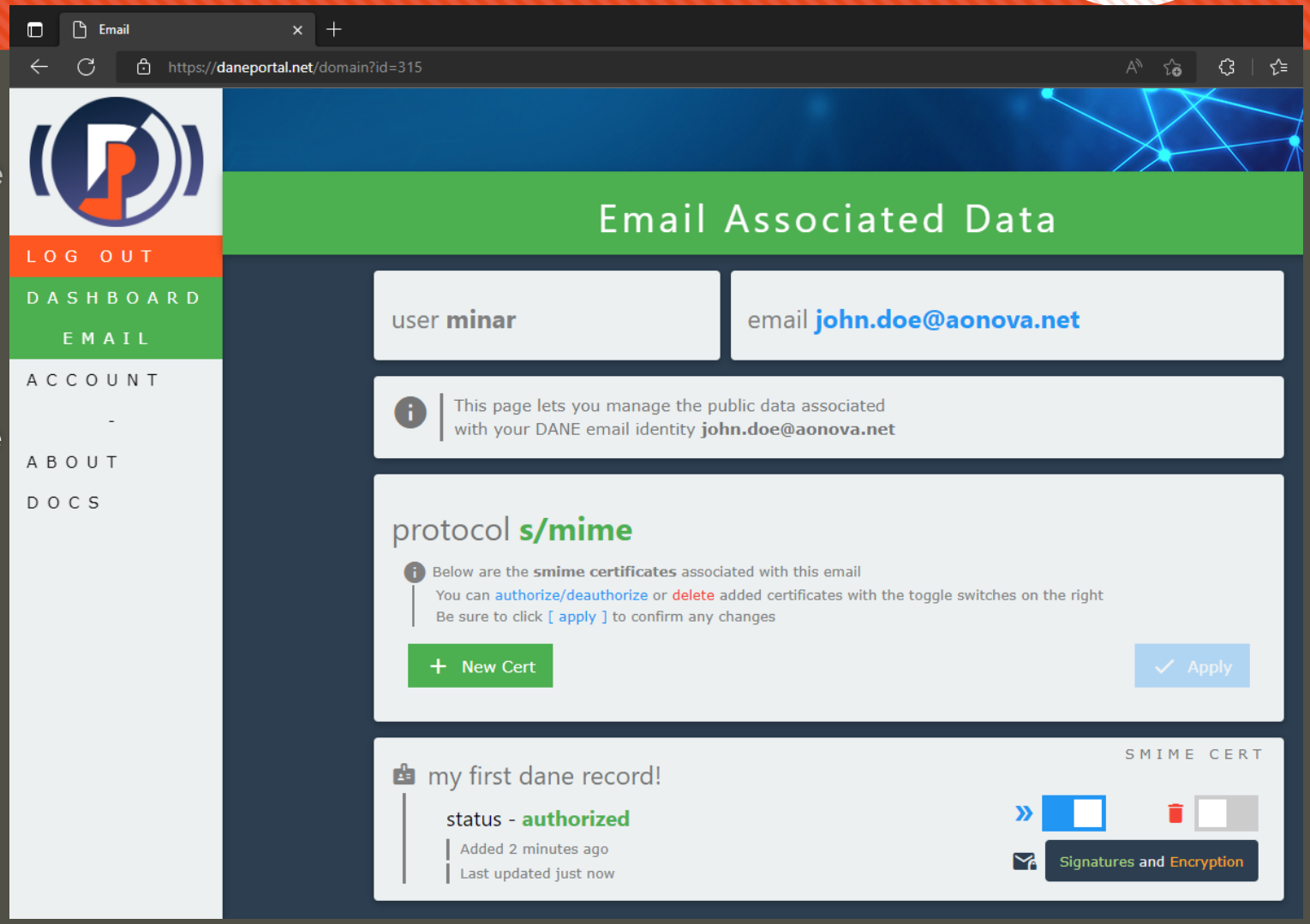
- You should now see a **card representing the record you just added**
- You can manage records here, by toggling its authorization state or deleting it permanently
- For now, toggle the **authorize** switch to the right and click [Apply]



Authorize record

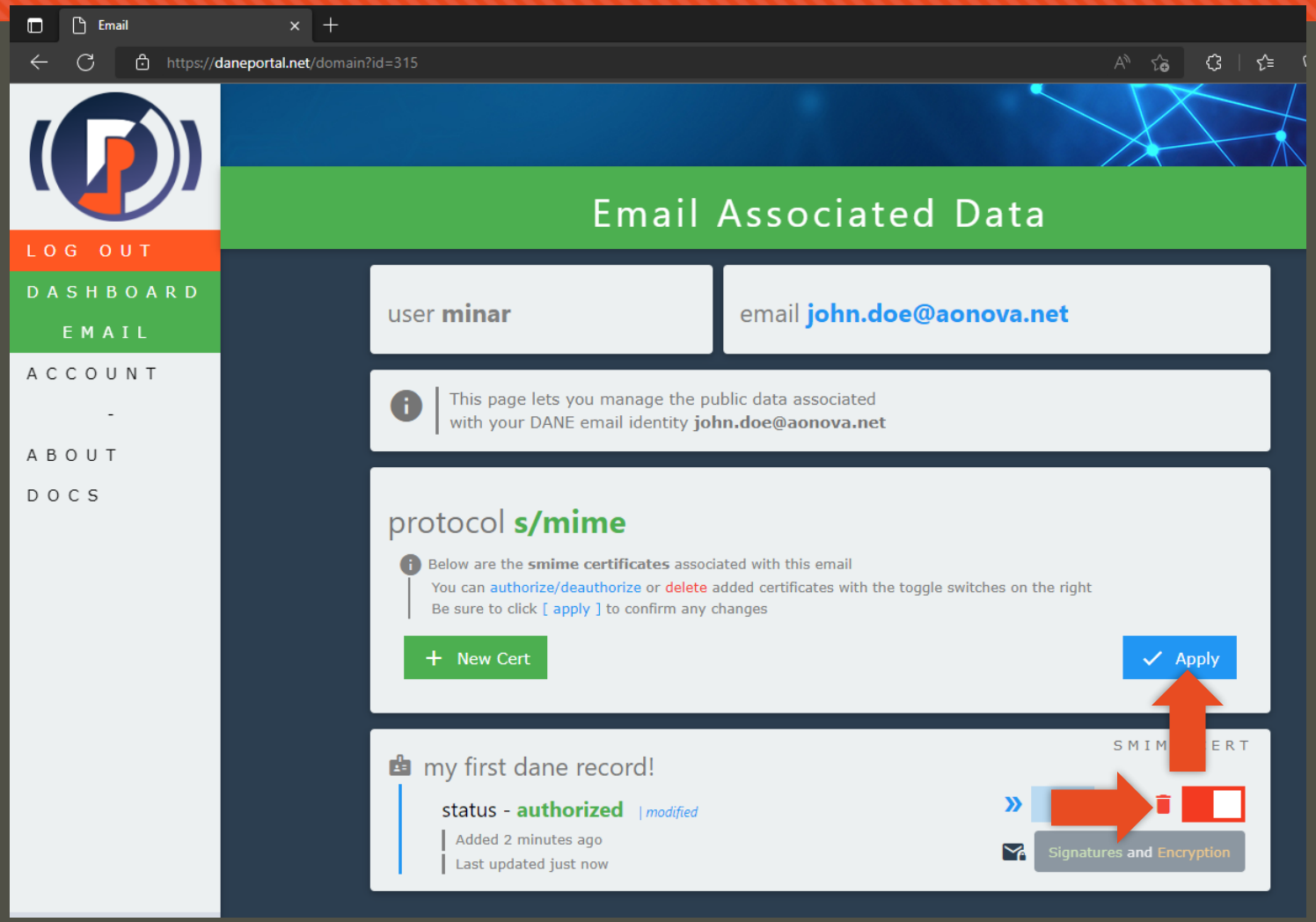
- **Authorizing a record** means you – as the operator of this denizen domain – **allow DANE portal to serve the record on DNS** under the given DANE zone

- If the status says Authorized it means the record is out there and accessible for DANE-smart crypto clients to resolve



Authorize record

- Test and see now if the record is being served up properly with a DANE-smart user mail agent
  - Check out **Kurer:** open-source DANE-SMIME enhancement for Outlook and Thunderbird
    - *https://kurer.daneportal.net*
- Note: since the DANE protocol calls for the domain to be hashed in a particular format, you can't just do a blind DNS query for the name
- Feel free to delete any test records after you are satisfied by toggling the **delete** switch and clicking [Apply]



Completed

- We saw how:
  - Admins
    - Create an account
    - Claim and verify zone
    - Hook up your zone by delegation
    - Add denizen domains (email user addresses so they can add their own certs)
  - Email users
    - Access the email addresses under DANE portal
    - Add and control DANE records (SMIME certificates) for their email addresses

Check out the Source

https://github.com/gmu-msl/dane-portal