

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

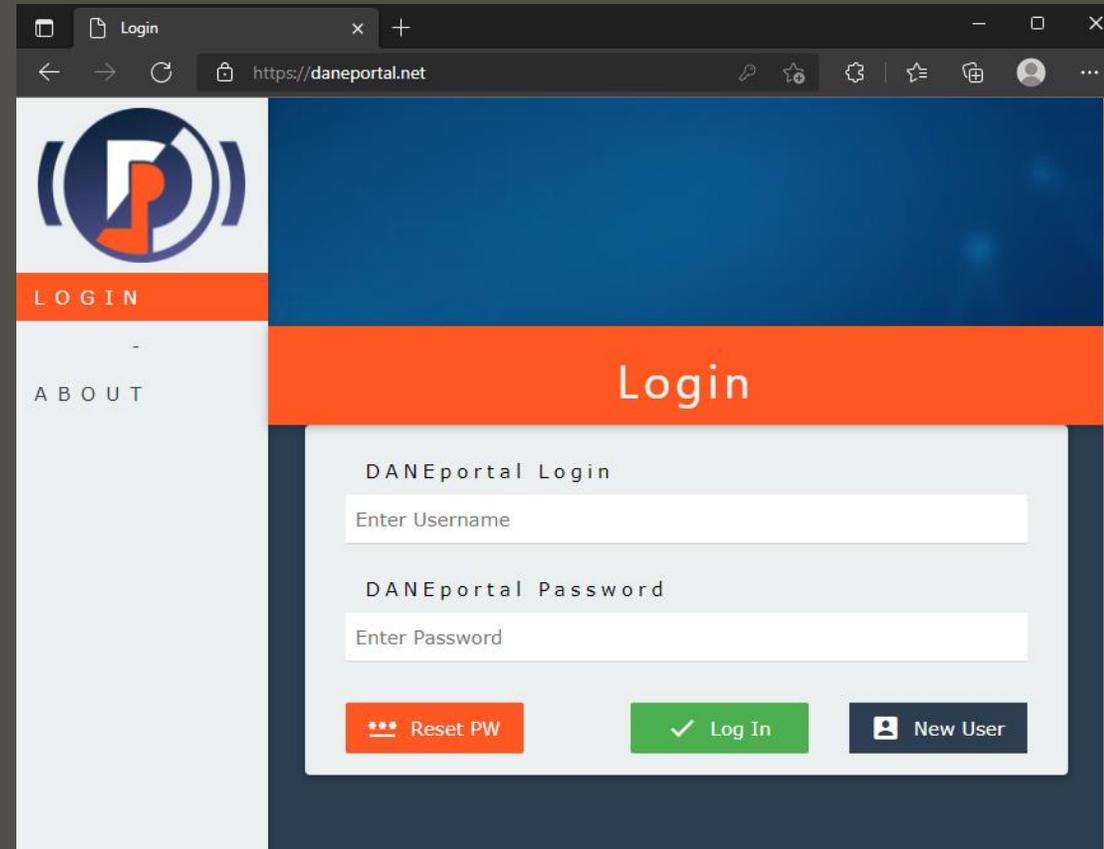


- We will show off the main features on DANE portal, from **two perspectives**
- Admins
 - Create an account
 - Claim and verify your zone
 - Hook up your zone
 - Add email users (so they can handle their own certs)
- Email users
 - Access the email addresses under DANE portal
 - Add and control DANE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

A screenshot of a web browser showing the 'Create New User' modal form. The browser address bar shows 'https://daneportal.net/#'. The modal has a green header with the title 'Create New User' and a close button. It contains four input fields: 'Username' with the value 'johndoe123', 'Email Address' with the value 'john.doe@example.com', 'Password' with masked characters '.....', and 'Confirm Password' with masked characters '.....'. Below the fields is a green success message: 'New user successfully added' with a checkmark icon and a close button. At the bottom of the modal are two buttons: an orange 'OK' button and a red 'Cancel' button. The background of the browser shows a navigation menu with 'LOGIN' and 'ABOUT' options.

Log In



- Enter your credentials
- Click [Log In]

A screenshot of a web browser displaying the login page for DANEportal. The browser's address bar shows the URL 'https://daneportal.net/#'. The page features a dark blue header with the DANEportal logo on the left and the word 'Login' in white on the right. Below the header, there is a white sidebar with 'LOGIN' and 'ABOUT' links. The main content area has a dark blue background with a white login form. The form contains two input fields: 'DANEportal Login' with the text 'johndoe123' and 'DANEportal Password' with masked characters '*****'. At the bottom of the form, there are three buttons: a red 'Reset PW' button, a green 'Log In' button, and a dark blue 'New User' button.

Browser: Login | Password saved

URL: https://daneportal.net/#

Navigation: LOGIN | ABOUT

Page Title: Login

DANEportal Login

johndoe123

DANEportal Password

Buttons: Reset PW | Log In | New User

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

The screenshot shows a web browser window with the URL <https://daneportal.net/dashboard>. The page title is "Zone Management Dashboard". The user is logged in as "user johndoe123".

The left sidebar contains the following navigation items:

- LOG OUT
- DASHBOARD (highlighted)
- ACCOUNT
-
- ABOUT

The main content area is divided into two sections:

dane-enabled email addresses

These are your email addresses which were added by zone admins
Click one to manage its public crypto keys

id	email	protocol	# of records (active/total)
----	-------	----------	-----------------------------

Refresh button:

managed dane zones

These are the zones under your management as an admin
Click one to open the zone management page for that zone
You can claim a zone to start the process of adding your zone here

id	zone	# of domains
----	------	--------------

Refresh button: Claim Zone button: Claim 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

The screenshot shows the DANE portal dashboard at <https://aonova.ddns.net/dashboard>. The dashboard includes a sidebar with navigation links: LOG OUT, DASHBOARD, ACCOUNT, and ABOUT. The main content area displays a table with columns for ID (temp.), Zone, and Denizen domains. A modal window titled "Add New Zone" is open, containing a form with a "Zone Name" input field (containing "example.com"), a "Submit" button, a "Cancel" button, and an "Advanced" button. Below the table, there is a refresh button and a "+ Claim Zone" button.

ID (temp.)	Zone	Denizen domains
------------	------	-----------------

Buttons: Refresh, + Claim Zone



Add a new zone

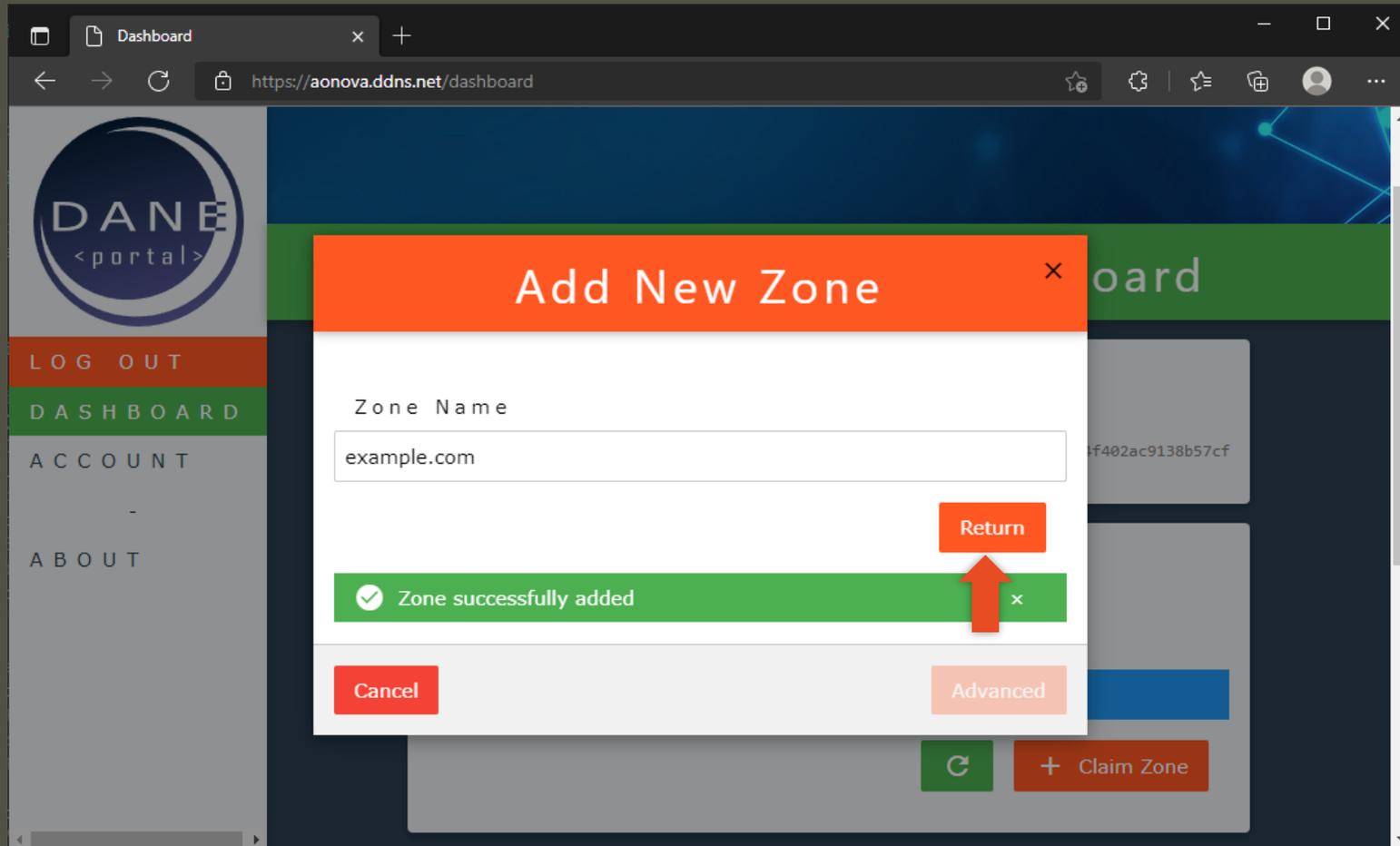
- Enter the *Fully Qualified Domain Name* of the zone you would like to administer
- Click [**Submit**] to add the zone *on a claimed basis*
- Anyone can claim any zone, but to complete you will need to prove ownership of the zone using the ACME protocol (shown next)

The screenshot shows a web browser window with the URL `https://aonova.ddns.net/dashboard`. The page features a sidebar with the DANE portal logo and navigation links: LOG OUT, DASHBOARD, ACCOUNT, and ABOUT. The main content area displays a table with columns for ID (temp.), Zone, and Denizen domains. A modal window titled "Add New Zone" is open, containing a text input field for "Zone Name" with the value "example.com". Below the input field are three buttons: "Submit" (green), "Cancel" (red), and "Advanced" (orange). A red arrow points to the "Submit" button. At the bottom right of the dashboard, there is a green refresh button and a red "Claim Zone" button.



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

The screenshot shows a web browser window with the URL <https://daneportal.net/dashboard>. The page title is "Zone Management Dashboard". On the left, there is a navigation menu with the following items: LOG OUT, DASHBOARD, ACCOUNT, and ABOUT. The main content area is divided into two sections:

dane-enabled email addresses

These are your email addresses which were added by zone admins. Click one to manage its public crypto keys.

id	email	protocol	# of records (active/total)

managed dane zones

These are the zones under your management as an admin. Click one to open the zone management page for that zone. You can claim a zone to start the process of adding your zone here.

id	zone	# of domains
468	example.com (unverified)	-

At the bottom right of the "managed dane zones" section, there is a green refresh button and a red "Claim Zone" button.

Verify zone claim



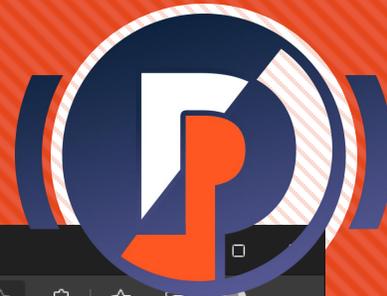
- Click on the unverified zone from the list to **start verification challenge**

The screenshot shows the 'Zone Management Dashboard' interface. The left sidebar contains navigation links: LOG OUT, DASHBOARD, ACCOUNT, and ABOUT. The main content area is divided into two sections:

- dane-enabled email addresses**: A section with an information icon and text: 'These your email addresses which were added by zone admins. Click one to manage its public crypto keys'. Below this is a table with columns: id, email, protocol, # of records (active/total). A green refresh button is present.
- managed dane zones**: A section with an information icon and text: 'These are the zones under your management as an admin. Click one to open the zone management page for that zone. You can claim a zone to start the process of adding your zone here'. Below this is a table with columns: id, zone, # of domains. One row is highlighted in green: '468 example.com (unverified)'. A red arrow points to this row. A green refresh button and an orange '+ Claim Zone' button are also present.

id	zone	# of domains
468	example.com (unverified)	-

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

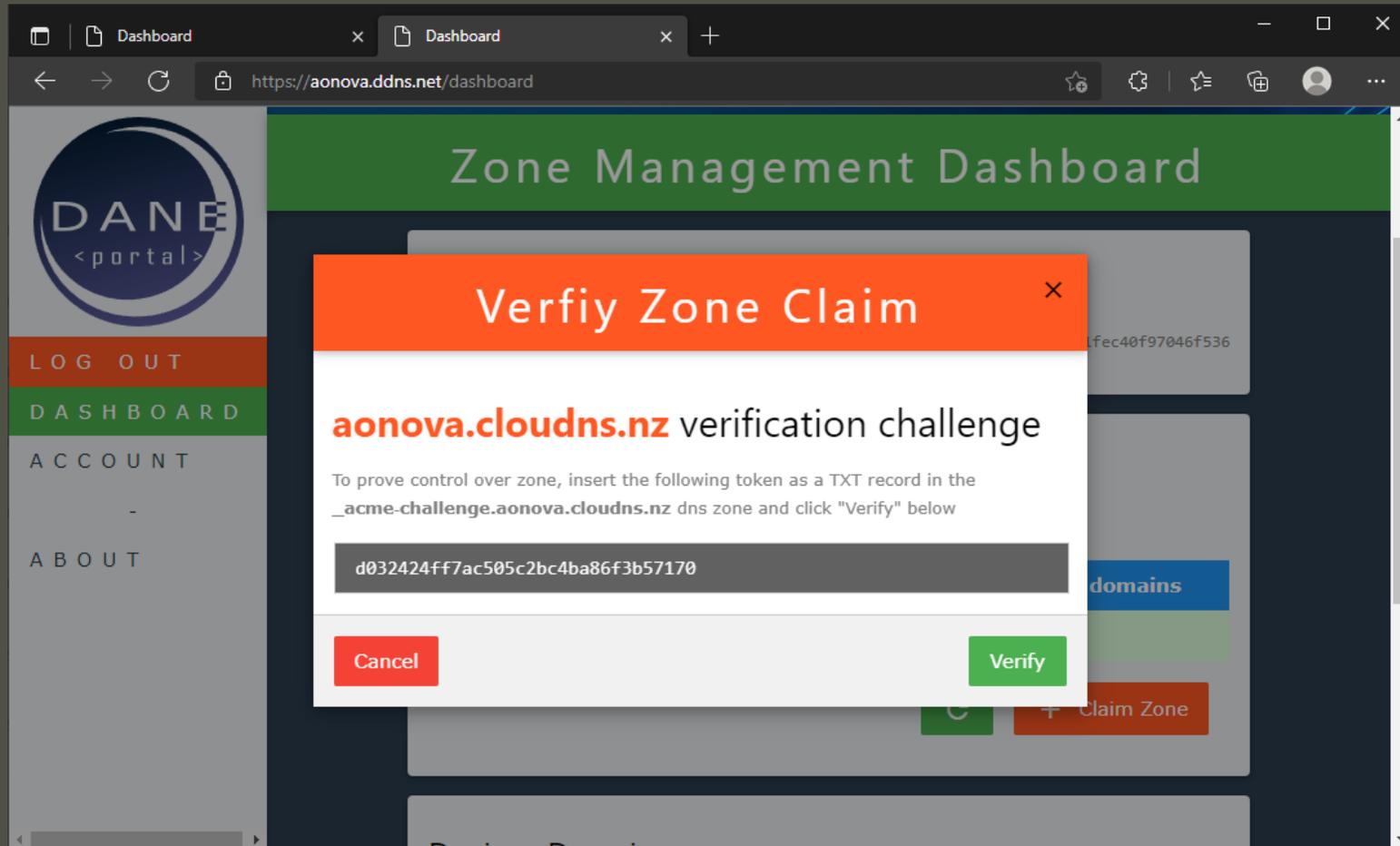
The screenshot shows a web browser window with the URL <https://daneportal.net/dashboard>. The page title is "Zone Management Dashboard". A modal window titled "Verify Zone Claim" is open, displaying a verification challenge for "example.com". The challenge text reads: "To prove control over zone, insert the following token as a TXT record in the `_acme-challenge.example.com` dns zone and click 'Verify' below". The token is `f021ff37f528bde0a7bd7aa77404cee2`. The modal has three buttons: "Close", "Remove", and "Verify". Below the modal, a table titled "Managed Zone Zones" shows a list of zones. The table has columns for "id", "zone", and "# of domains". The table contains one entry: "468", "example.com (unverified)", and "-". There are "Refresh" and "Claim Zone" buttons below the table.

id	zone	# of domains
468	example.com (unverified)	-



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`

The screenshot shows a web browser window with the URL `https://www.cloudns.net/records/domain/3423060/`. The page title is "CloudDNS: Domain settings (aonova)". A modal dialog titled "Add new record" is open, showing the process of adding a TXT record for a verification challenge. The dialog has the following fields and content:

- Title:** `aonova.cloudns.nz` verification challenge
- Type:** `TXT`
- Host:** `_acme-challenge`.aonova.cloudns.nz (The text `_acme-challenge` is highlighted with a red box and an arrow pointing left.)
- Value:** `d032424...ac505c2bc4ba86f3b57170` (The value is partially obscured by a red arrow pointing up from the host field.)
- Points to:** (Empty field)
- Buttons:** `SAVE` (orange), `Change the owner`, `Delete the zone`, `Deactivate`, `Okay`, `Online - Live Chat`



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

The screenshot shows the CloudDNS interface with a modal dialog titled "Add new record" for a verification challenge. The dialog contains the following fields and instructions:

- Title:** aonova.cloudns.nz verification challenge
- Type:** TXT
- Host:** `_acme-challenge` (with a dropdown menu showing `.aonova.cloudns.nz`)
- Points to:** `d032424ff7ac505c2bc4ba86f3b57170` (highlighted with a red box)
- Instructions:** "To prove control over zone, insert the following token as a TXT record in the `_acme-challenge.aonova.cloudns.nz` dns zone and click 'Verify' below"
- Token:** `d032424ff7ac505c2bc4ba86f3b57170` (displayed in a grey box)
- Buttons:** "SAVE" (orange), "Change the owner", "Delete the zone", "Deactivate", "Okay", "Online - Live Chat"

Red arrows indicate the flow of information: one arrow points from the token box in the instructions to the token input field, and another points from the token input field to the "Points to" field.



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

The screenshot shows the CloudDNS website dashboard. The browser address bar displays `https://www.cloudns.net/records/domain/3423060/`. The dashboard header includes the CloudDNS logo, navigation links for Dashboard, Billing, Tools, Services, and Support, and a Logout button. Below the header, there are three promotional banners for domain registration: REGISTER AONOVA.CO FOR ONLY \$32.49, REGISTER AONOVA.IO FOR ONLY \$70.00, and REGISTER AONOVA.BLOG FOR ONLY \$9.39. A row of icons represents various DNS management tools: DNS Records, SOA settings, Records Templates, Cloud domains, Mail forwards, DNS statistics, Zone transfers, Updated (highlighted with a red arrow and a tooltip that says 'Update this zone'), Export zone file, Zone import, Zone shares, Change the owner, and Delete the zone. Below the icons is a search bar containing the text 'aonova.cloudns.nz' and buttons for 'Check on dns.computer' and 'Deactivate'. At the bottom, there is a cookie consent banner and an 'Online - Live Chat' button.



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

The screenshot shows a web browser window with the URL `https://aonova.ddns.net/dashboard`. The page title is "Zone Management Dashboard". A modal dialog box titled "Verfiy Zone Claim" is open, displaying the following content:

aonova.cloudns.nz verification challenge

To prove control over zone, insert the following token as a TXT record in the `_acme-challenge.aonova.cloudns.nz` dns zone and click "Verify" below

`d032424ff7ac505c2bc4ba86f3b57170`

Buttons: Cancel, Verify

A red arrow points to the "Verify" button. The background dashboard shows a sidebar with "DANE <portal>" logo and navigation links: LOG OUT, DASHBOARD, ACCOUNT, ABOUT. The main content area has a "domains" section and a "Claim Zone" button.



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

The screenshot shows a web browser window with the URL `https://aonova.ddns.net/dashboard`. The page title is "Zone Management Dashboard". A modal dialog box titled "Verfiy Zone Claim" is open, displaying the following content:

aonova.cloudns.nz verification challenge

To prove control over zone, insert the following token as a TXT record in the `_acme-challenge.aonova.cloudns.nz` dns zone and click "Verify" below

`d032424ff7ac505c2bc4ba86f3b57170`

Below the dialog, a green notification bar with a checkmark icon says "Zone successfully verified". At the bottom right of the dialog, a red arrow points to a green "OK" button.

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**

id	zone	# of domains
182	aonova.net	1
465	example.com (unverified)	-

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.

The screenshot shows a web browser window with the URL `https://daneportal.net/zone?id=182`. The page title is "Zone aonova.net". On the left is a navigation menu with the following items: LOG OUT, DASHBOARD, ZONE (highlighted in green), ACCOUNT, and ABOUT. The main content area displays "aonova.net info". Under "current admins", there is a table with two columns: "Access ID (debug)" and "Admin Username". The table contains one row with the values "184" and "minar". Below this, under "available protocols", there is a note: "Each protocol is served as its own DANE zone" and a green button labeled "S/MIME". At the bottom, under "actions", there are two buttons: "Add admin account" and "Delete zone".

Access ID (debug)	Admin Username
184	minar

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

The screenshot shows a web browser window with the URL `https://daneportal.net/zone?id=182`. The page title is "Zone aonova.net". On the left is a navigation menu with the following items: LOG OUT, DASHBOARD, ZONE, ACCOUNT, and ABOUT. The main content area is titled "aonova.net info" and contains the following sections:

- current admins**: A table with two columns: "Access ID (debug)" and "Admin Username".

Access ID (debug)	Admin Username
184	minar
- available protocols**: A section with an information icon and the text "Each protocol is served as its own DANE zone". Below this is a green button labeled "S/MIME" with a lock icon. A red arrow points to this button.
- actions**: Two buttons at the bottom: "Add admin account" (orange) and "Delete zone" (red).

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

The screenshot shows a web browser window with the URL `https://daneportal.net/zone?id=182`. The page title is "Zone aonova.net". The left sidebar contains navigation links: LOG OUT, DASHBOARD, ZONE (highlighted), ACCOUNT, and ABOUT. The main content area displays the configuration for the "aonova.net - s/mime" zone, which is currently "Active".

delegation records

- Info: Serve these records with your delegating name server to close the loop
- ns record**: `_smimecert.aonova.net. IN NS dane-dns.care.gmu.edu.`
- ds record**: `_smimecert.aonova.net. IN DS 61774 13 2 CA8DFF7E913F1B2DC008E64BCDE8EB517B0A4CE`

template

- Info: Baseline record served for the DANE zone

```
$ORIGIN _smimecert.aonova.net.  
$TTL 3600  
@ IN SOA dane-dns.care.gmu.edu. mail.daneportal.ddns.net. ( 2022012800 7200 3600  
@ IN NS dane-dns.care.gmu.edu.
```

actions

- + Add domain
- + Add domain bulk
- Set Inactive

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

Zone aonova.net

aonova.net - s/mime zone

status - **Active**

delegation records

i Serve these records with your delegating name server to close the loop

ns record

```
_smimecert.aonova.net. IN NS dane-dns.care.gmu.edu.
```

ds record

```
_smimecert.aonova.net. IN DS 61774 13 2 CA8DFF7E913F1B2DC008E64BCDE8E8517B0A4CE
```

template

i Baseline record served for the DANE zone

```
$ORIGIN _smimecert.aonova.net.  
$TTL 3600  
@ IN SOA dane-dns.care.gmu.edu. mail.daneportal.ddns.net. ( 2022012800 7200 3600  
@ IN NS dane-dns.care.gmu.edu.
```

actions

+ Add domain + Add domain bulk Set Inactive

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.

Zone aonova.net

aonova.net - s/mime zone

status - **Active**

delegation records

i Serve these records with your delegating name server to close the loop

ns record

```
_smimecert.aonova.net. IN NS dane-dns.care.gmu.edu.
```

ds record

```
_smimecert.aonova.net. IN DS 61774 13 2 CA8DFF7E913F1B2DC008E64BCDE8EB517B0A4CE
```

template

i Baseline record served for the DANE zone

```
$ORIGIN _smimecert.aonova.net.  
$TTL 3600  
@ IN SOA dane-dns.care.gmu.edu. mail.daneportal.ddns.net. ( 2022012800 7200 3600  
@ IN NS dane-dns.care.gmu.edu.
```

actions

+ Add domain + Add domain bulk 🌐 Set Inactive



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 DANEzone domain name is dependent on the protocol

The screenshot shows the CloudDNS interface with a modal window for adding a new record. The modal has the following fields:

- Type:** NS
- Host:** .aonova.cloudns.nz
- Points to:**
- SAVE** button

A popup window titled "delegation records" is overlaid on the right side of the modal. It contains the following text:

Serve these records with your delegating name server to close the loop

- ns record
_smimecert.aonova.net. IN NS dane-dns.care.gmu.edu.
- ds record
_smimecert.aonova.net. IN DS 61774 13 2 CA8DFF7E913F1B2DC008E64BCDE8E8517B0A4CE

Red arrows point from the "Add new record" button to the "Type" field, and from the "Host" field to the "delegation records" popup.



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

delegation records

Serve these records with your delegating name server to close the loop

ns record

_smimecert.aonova.net. IN NS dane-dns.care.gmu.edu.

ds record

_smimecert.aonova.net. IN DS 61774 13 2 CA8DFF7E913F1B2DC008E64BCDE8E8517B0A4CE

Add new record

Type:

NS

Host:

_smimecert .aonova.cloudns.nz

Leave empty for aonova.cloudns.nz

Points to:

aonova.ddns.net

SAVE

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.

Zone aonova.net

aonova.net - s/mime zone

status - **Active**

delegation records

i Serve these records with your delegating name server to close the loop

ns record

```
_smimecert.aonova.net. IN NS dane-dns.care.gmu.edu.
```

ds record

```
_smimecert.aonova.net. IN DS 61774 13 2 CA8DFF7E913F1B2DC008E64BCDE8E8517B0A4CE
```

template

i Baseline record served for the DANE zone

```
$ORIGIN _smimecert.aonova.net.  
$TTL 3600  
@ IN SOA dane-dns.care.gmu.edu. mail.daneportal.ddns.net. ( 2022012800 7200 3600 1800 1800 )  
@ IN NS dane-dns.care.gmu.edu.
```

actions

+ Add domain + Add domain bulk Set Inactive



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.

Dashboard Billing

ds records

Serve these records with your delegating name server to complete DNSSEC chain-of-trust

Type: `_smimecert.aonova.cloudns.nz. IN DS 63705 13 2 4C49B1033B78D3158A`

Type: DS

Host: `_smimecert`.aonova.cloudns.nz

Key Tag:

Algorithm: (2) Diffie-Hellman

Digest Type: (1) SHA-1

Points to:

SAVE



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.

The screenshot shows the CloudDNS interface with a modal window titled "Add new record" for a "ds record". The form contains the following fields:

- Type: DS
- Host: `_smimecert.aonova.cloudns.nz`
- Key Tag: `63705`
- Algorithm: (2) Diffie-Hellman
- Digest Type: (1) SHA-1
- Points to: (empty field)

A "SAVE" button is located at the bottom of the modal. The background shows the CloudDNS dashboard with a search bar for "aonova.cl" and a "Cookies help us" notice.



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 won't appear immediately after the zone is made if the system is under load – if so, try refreshing the page until it does.

Dashboard Billing

ds records

Serve these records with your delegating name server to complete DNSSEC chain-of-trust

`_smimecert.aonova.cloudns.nz. IN DS 63705 13 2 4C49B1033B78D3158A`

Add new record

Type: DS 1 Hour

Host: _smimecert .aonova.cloudns.nz

Key Tag: 63705 Algorithm: (13) ECDSA Curve Digest Type: (1) SHA-1

Points to:

SAVE



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 won't appear immediately after the zone is made if the system is under load – if so, try refreshing the page until it does.

Dashboard Billing

ds records

Serve these records with your delegating name server to complete DNSSEC chain-of-trust

`_smimecert.aonova.cloudns.nz. IN DS 63705 13 2 4C49B1033B78D3158A`

Type: DS 1 Hour

Host: `_smimecert`.aonova.cloudns.nz

Key Tag: 63705 Algorithm: (13) ECDSA Curve Digest Type: (2) SHA-256

Points to:

SAVE

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.

Dashboard Billing

ds records

Serve these records with your delegating name server to complete DNSSEC chain-of-trust

`_smimecert.aonova.cloudns.nz. IN DS 63705 13 2 4C49B1033B78D3158A`

Add new record

Type: DS 1 Hour

Host: `_smimecert`.aonova.cloudns.nz

Key Tag: 63705 Algorithm: (13) ECDSA Curve Digest Type: (2) SHA-256

Points to: `4C49B1033B78D3158ABFA464561B7D636F41AFAE7537B67931581`

SAVE

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

Zone aonova.net

status - **Inactive**

delegation records

i Serve these records with your delegating name server to close the loop

ns record

```
_smimecert.aonova.net. IN NS dane-dns.care.gmu.edu.
```

ds record

```
_smimecert.aonova.net. IN DS 61774 13 2 CA8DFF7E913F1B2DC008E64BCDE8EB517B0A4CE
```

template

i Baseline record served for the DANE zone

```
$ORIGIN _smimecert.aonova.net.  
$TTL 3600  
@ IN SOA dane-dns.care.gmu.edu. mail.daneportal.ddns.net. ( 2022012800 7200 3600  
@ IN NS dane-dns.care.gmu.edu.
```

actions

+ Add domain + Add domain bulk **Set Active**



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](#)

Zone aonova.net

status - **Active - pending**

delegation records

i Serve these records with your delegating name server to close the loop

ns record

```
_smimecert.aonova.net. IN NS dane-dns.care.gmu.edu.
```

ds record

```
_smimecert.aonova.net. IN DS 61774 13 2 CA8DFF7E913F1B2DC008E64BCDE8EB517B0A4CE
```

template

i Baseline record served for the DANE zone

```
$ORIGIN _smimecert.aonova.net.  
$TTL 3600  
@ IN SOA dane-dns.care.gmu.edu. mail.daneportal1.ddns.net. ( 2022012800 7200 3600  
@ IN NS dane-dns.care.gmu.edu.
```

actions

[+ Add domain](#) [+ Add domain bulk](#) [Set Inactive](#)

DANE zone toggled successfully [x](#)



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.

The screenshot shows a web browser window with the URL `https://aonova.ddns.net/zone?id=2`. The page title is "Zone aonova.cloudns.nz". The main content area displays the following information:

- Zone:** aonova.cloudns.nz - s/mime zone
- status:** Active
- ds records:** Serve these records with your delegating name server to complete DNSSEC chain-of-trust. The record is: `_smimecert.aonova.cloudns.nz. IN DS 63705 13 2 4C49B1033B78D3158ABFA464`
- template:** Baseline records used for zone when serving. The template is:

```
$ORIGIN _smimecert.aonova.cloudns.nz.  
$TTL 3600  
@ IN SOA aonova.ddns.net. mail.aonova.ddns.net. ( 2021100500 7200 3600  
@ IN NS aonova.ddns.net.
```
- actions:** + Add domain, + Add domain bulk, Set Inactive
- domains:** (partially visible)



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

The screenshot shows two browser windows. The top window is the DANE portal at <https://aonova.ddns.net/zone?id=2>. It displays the 'Zone aonova.cloudns.nz' configuration for the 'aonova.cloudns.nz - s/mime' zone. The status is 'Active' and it shows 'ds records' with a note to 'Serve these records with your delegating name server to complete DNSSEC chain-of-trust'. The bottom window is the SecSpider website at <https://secspider.net>. It features the SecSpider logo and the text 'Global DNSSEC deployment tracking'. There are navigation buttons for 'Status', 'Deployment Stats', 'Deployment Growth', and 'Hierarchy'. A search bar is visible with the text 'Lookup zone: _smimecert.aonova.net' and a 'Search' button.



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

A screenshot of a web browser showing the 'Zone aonova.cloudns.nz' page. The browser's address bar shows 'https://aonova.ddns.net/zone?id=2'. The page has a green header with the zone name. On the left is a sidebar with the DANE portal logo and navigation links: LOG OUT, DASHBOARD, ZONE, ACCOUNT, and ABOUT. The main content area shows a 'template' section with baseline records for the zone, including SOA and NS records. Below this is an 'actions' section with three buttons: '+ Add domain' (highlighted with a red arrow), 'Add domain bulk', and 'Set Inactive'. At the bottom is a 'domains' section with a table header containing columns for ID (debug), Domain, User, and Records (active/total).

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.

Dashboard

Zone

ClouDNS: Domain settings (aonc x | +)

https://aonova.ddns.net/zone?id=2

DANE
<portal>

LOG OUT

DASHBOARD

ZONE

ACCOUNT

ABOUT

Zone aonova.cloudns.nz

s/mime zone - new denizen domain

Add new denizen domain to [aonova.cloudns.nz](#) and grant its access to an existing DANEportal user

john.doe
Domain Name (only local part)

JohnDoe123
DANEportal Username

Select Protocol
Domain Protocol

Cancel

Reset Form

Submit

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

A screenshot of a web browser showing the 'Zone aonova.cloudns.nz' settings page. The page has a green header with the zone name. On the left is a navigation menu with 'DANE <portal>' logo, 'LOG OUT', 'DASHBOARD', 'ZONE', 'ACCOUNT', and 'ABOUT'. The main content area is titled 's/mime zone - new denizen domain' and contains a form with the following fields: 'Domain Name (only local part)' with the value 'janedoe', 'DANEportal Username' with the value 'jane_doe_123', and a dropdown menu for 'S/MIME' with 'Domain Protocol' below it. At the bottom of the form are three buttons: 'Cancel', 'Reset Form', and 'Submit'. A large red arrow points down to the 'Submit' button.



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

Zone aonova.cloudns.nz

```
_smimecert.aonova.cloudns.nz. IN DS 63705 13 2 4C49B1033B78D3158ABFA46456
```

template

Baseline records used for zone when serving

```
$ORIGIN _smimecert.aonova.cloudns.nz.  
$TTL 3600  
@ IN SOA aonova.ddns.net. mail.aonova.ddns.net. ( 2021100500 7200 3600 12  
@ IN NS aonova.ddns.net.
```

actions

+ Add domain + Add domain bulk Set Inactive

domains

Denizen accessed domains under aonova.cloudns.nz S/MIME

ID (debug)	Domain	User	Records (active/total)
5	janedoe@aonova.cloudns.nz	jane_doe_123	0/0



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**

Dashboard

https://daneportal.net/dashboard

Zone Management Dashboard

user **minar**

dane-enabled email addresses

i These your email addresses which were added by zone admins
Click one to manage its public crypto keys

email	protocol	# of records (active/total)
minar@osterweil.net	SMIME	1/1
minar@aonova.net	SMIME	1/3
tislam20@aonova.net	SMIME	1/1
john.doe@aonova.net	SMIME	0/0

managed **dane zones**

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

The screenshot shows a web browser window with the URL <https://daneportal.net/domain?id=315>. The page features a sidebar with navigation links: LOG OUT, DASHBOARD, EMAIL, ACCOUNT, ABOUT, and DOCS. The main content area is titled "Email Associated Data" and displays the following information:

- user **minar**
- email **john.doe@aonova.net**
- Information: This page lets you manage the public data associated with your DANE email identity **john.doe@aonova.net**
- protocol **s/mime**
- Information: Below are the **smime certificates** associated with this email. You can **authorize/deauthorize** or **delete** added certificates with the toggle switches on the right. Be sure to click [[apply](#)] to confirm any changes.
- Buttons: [+ New Cert](#) and [Apply](#)

A red arrow points to the [+ New Cert](#) button.



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

[← New Cert](#) [✓ Apply](#)

Add new cert to [john.doe@aonova.net](#)

Upload certificate file

No file chosen

Unnamed
Nickname to remember this by (optional)

Domain-issued certificate (DANE-EE) ▾
Usage

Full certificate (Cert) ▾
Selector

No hash used (Full) ▾
Matching

Both (default) ▾
Signing or encrypting



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

Be sure to click [[apply](#)] to confirm any changes

[New Cert](#)

Add new cert to john.doe@aonova.net

S/MIME PEM Certificate File

74:f3:95:18:44:2f:a0:44:3e:cc:02:fa:69:42:ae:52
Signature Algorithm: sha256WithRSAEncryption
Issuer: Actalis Client Authentication CA G3, Actalis S.p.A. - Ponte San Pietro Bergamo, IT
Validity
Not Before: Jun 6 02:46:39 2022 GMT
Not After : Jun 6 02:46:39 2023 GMT
minar@aonova.net,
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public-Key: (2048 bit)

Basic Constraints: critical
CA:FALSE
X509v3 Authority Key Identifier:
keyid:BE:97:A9:AA:84:BF:80:BF:10:53:7D:09:32:F9:E1:2E:32:1B:CF:77

Authority Information Access:
CA Issuers - URI:http://cacert.actalis.it/certs/actalis-autclig3
OCSP - URI:http://ocsp09.actalis.it/VA/AUTHCL-G3

X509v3 Subject Alternative Name:
email:minar@aonova.net
X509v3 Certificate Policies:
Policy: 1.3.159.1.24.1
CPS: https://www.actalis.it/area-download

X509v3 Extended Key Usage:
TLS Web Client Authentication, E-mail Protection
X509v3 CRL Distribution Points:
Full Name:
URI:http://cr09.actalis.it/Repository/AUTHCL-G3/getLastCRL

X509v3 Key Usage: critical
Digital Signature, Key Encipherment

minar@aonova.net.crt.pem

My first DANE record!

Nickname to remember this by (optional)

Selector

Matching

Signing or encrypting



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

Be sure to click [[apply](#)] to confirm any changes

[New Cert](#)

Add new cert to [john.doe@aonova.net](#)

S/MIME PEM Certificate File

74:f3:95:18:44:2f:a0:44:3e:cc:02:fa:69:42:ae:52
Signature Algorithm: sha256WithRSAEncryption
Issuer: Actalis Client Authentication CA G3, Actalis S.p.A. - Ponte S
Pietro Bergamo, IT
Validity
Not Before: Jun 6 02:46:39 2022 GMT
Not After : Jun 6 02:46:39 2023 GMT
minar@aonova.net,
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public-Key: (2048 bit)

Basic Constraints: critical
CA:FALSE
X509v3 Authority Key Identifier:
keyid:BE:97:A9:AA:84:BF:80:BF:10:53:7D:09:32:F9:E1:2E:32:1B:CF:
Authority Information Access:
CA Issuers - URI:http://cacert.actalis.it/certs/actalis-autclig3
OCSP - URI:http://ocsp09.actalis.it/VA/AUTHCL-G3

X509v3 Subject Alternative Name:
email:minar@aonova.net
X509v3 Certificate Policies:
Policy: 1.3.159.1.24.1
CPS: https://www.actalis.it/area-download

X509v3 Extended Key Usage:
TLS Web Client Authentication, E-mail Protection
X509v3 CRL Distribution Points:
Full Name:
URI:http://crl09.actalis.it/Repository/AUTHCL-G3/getLastCRL

X509v3 Key Usage: critical
Digital Signature, Key Encipherment

My first DANE record!

Nickname to remember this by (optional)

Domain-issued certificate (DANE-EE) ▾

Usage

Full certificate (Cert) ▾

Selector

No hash used (Full) ▾

Matching

Both (default) ▾

Signing or encrypting

[Defaults](#) [Submit](#)

[Choose File](#) minar@aonova.net.crt.pem



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

Be sure to click [[apply](#)] to confirm any changes

New Cert

Add new cert to john.doe@aonova.net

S/MIME PEM Certificate File

```
74:f3:95:18:44:2f:a0:44:3e:cc:02:fa:69:42:ae:52
Signature Algorithm: sha256WithRSAEncryption
Issuer: Actalis Client Authentication CA G3, Actalis S.p.A. - Ponte San
Pietro Bergamo, IT
Validity
Not Before: Jun 6 02:46:39 2022 GMT
Not After : Jun 6 02:46:39 2023 GMT
minar@aonova.net
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public-Key: (2048 bit)

Basic Constraints: critical
CA:FALSE
X509v3 Authority Key Identifier:
keyid:BE:97:A9:AA:84:BF:80:BF:10:53:7D:09:32:F9:E1:2E:32:1B:CF:77

Authority Information Access:
CA Issuers - URI:http://cacert.actalis.it/certs/actalis-autclig3
OCSP - URI:http://ocsp09.actalis.it/VA/AUTHCL-G3

X509v3 Subject Alternative Name:
email:minar@aonova.net
X509v3 Certificate Policies:
Policy: 1.3.159.1.24.1
CPS: https://www.actalis.it/area-download

X509v3 Extended Key Usage:
TLS Web Client Authentication, E-mail Protection
X509v3 CRL Distribution Points:

Full Name:
URI:http://crl09.actalis.it/Repository/AUTHCL-G3/getLastCRL

X509v3 Key Usage: critical
Digital Signature, Key Encipherment
```

My first DANE record!

Nickname to remember this by (optional)

Domain-issued certificate (DANE-EE) ▾

Usage

Full certificate (Cert) ▾

Selector

No hash used (Full) ▾

Matching

Both (default) ▾

Signing or encrypting

Defaults **Submit**

Choose File minar@aonova.net.crt.pem



View record



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

The screenshot shows a web browser window at <https://daneportal.net/domain?id=315>. The page title is "Email Associated Data". The user is logged in as "minar" with the email "john.doe@aonova.net".

The main content area includes:

- An information box: "This page lets you manage the public data associated with your DANE email identity john.doe@aonova.net".
- A section for "protocol s/mime" with an information box: "Below are the smime certificates associated with this email. You can authorize/deauthorize or delete added certificates with the toggle switches on the right. Be sure to click [apply] to confirm any changes".
- A "New Cert" button and an "Apply" button.
- A green success message: "Certificate added successfully" with an "OK" button.
- A record card titled "my first dane record!" with a status of "not authorized". It shows "Added just now" and "Last updated just now". There are toggle switches and a "Signatures and Encryption" button.

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**]

The screenshot shows a web browser window with the URL <https://daneportal.net/domain?id=315>. The page title is "Email Associated Data". On the left, there is a navigation menu with options: LOG OUT, DASHBOARD, EMAIL, ACCOUNT, ABOUT, and DOCS. The main content area displays the following information:

- User: **minar**
- Email: **john.doe@aonova.net**
- Information: This page lets you manage the public data associated with your DANE email identity **john.doe@aonova.net**.
- Protocol: **s/mime**
- Message: Below are the **smime certificates** associated with this email. You can **authorize/deauthorize** or **delete** added certificates with the toggle switches on the right. Be sure to click [**apply**] to confirm any changes.
- Buttons: **+ New Cert** and **✓ Apply**.
- Record Card: **my first dane record!** with status **- not authorized** (modified). It includes fields for "Added just now" and "Last updated just now". The card has a control panel with a blue "authorize" switch (indicated by a red arrow), a red trash icon, and a grey "deauthorize" switch. A "Signatures and Encryption" button is also visible.

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

A screenshot of a web browser showing the 'Email Associated Data' page on the DANE Portal. The browser address bar shows 'https://daneportal.net/domain?id=315'. The page has a dark blue header with the DANE Portal logo and a green navigation bar with 'EMAIL' selected. The main content area shows the user 'minar' and email 'john.doe@aonova.net'. An information box states: 'This page lets you manage the public data associated with your DANE email identity john.doe@aonova.net'. Below this, the 'protocol s/mime' section shows instructions for managing SMIME certificates, with a '+ New Cert' button and an 'Apply' button. At the bottom, a record titled 'my first dane record!' is shown with a status of 'authorized', added 2 minutes ago, and last updated just now. To the right of the record are toggle switches and a 'Signatures and Encryption' button.

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](#)]

The screenshot shows the 'Email Associated Data' page in a browser. The URL is <https://daneportal.net/domain?id=315>. The page has a sidebar with navigation links: LOG OUT, DASHBOARD, EMAIL, ACCOUNT, ABOUT, and DOCS. The main content area shows the user 'minar' and email 'john.doe@aonova.net'. Below this, there is an information box stating: 'This page lets you manage the public data associated with your DANE email identity john.doe@aonova.net'. The main section is titled 'protocol s/mime' and contains a list of smime certificates. A green '+ New Cert' button is visible. A blue 'Apply' button with a checkmark is highlighted by a red arrow. Below the certificates, there is a record titled 'my first dane record!' with a status of 'authorized' and a 'modified' timestamp. A red arrow points to a 'delete switch' (a red square) on the right side of this record. A 'Signatures and Encryption' button is also visible at the bottom right.

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>