Recipe for Generating Digital Certificates with Post-Quantum Cryptography Using INeS

Introduction:

In today's digital landscape, secure communication and data protection are paramount, this also applies to the interactions of IoT devices that transmit confidential information. Post-Quantum Cryptography (PQC) is a game-changing technology designed to safeguard against future quantum threats. This recipe will guide you through the straightforward process of generating a digital certificate using PQC algorithms on the INeS platform. No special equipment is needed — just a computer and a web browser.

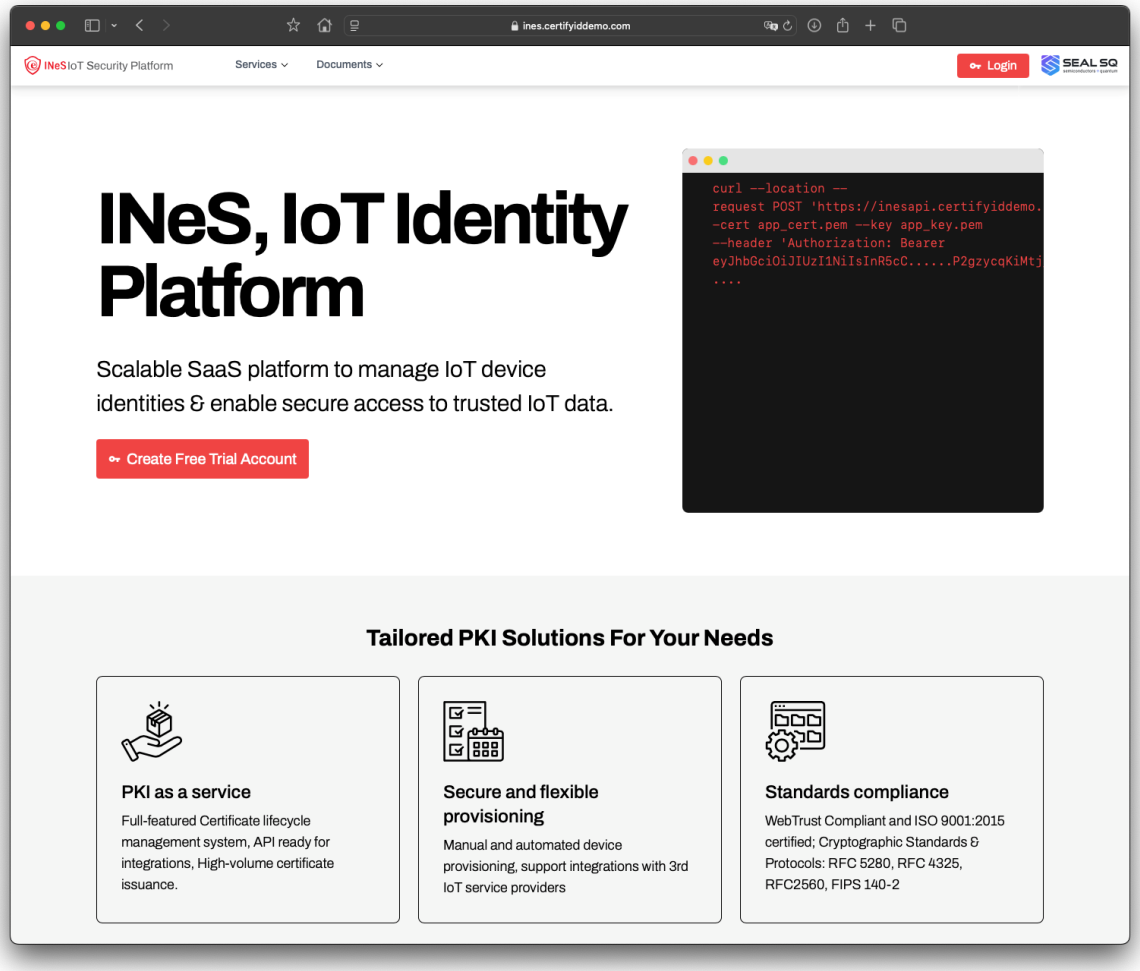
Ingredients:

- A computer
- A web browser

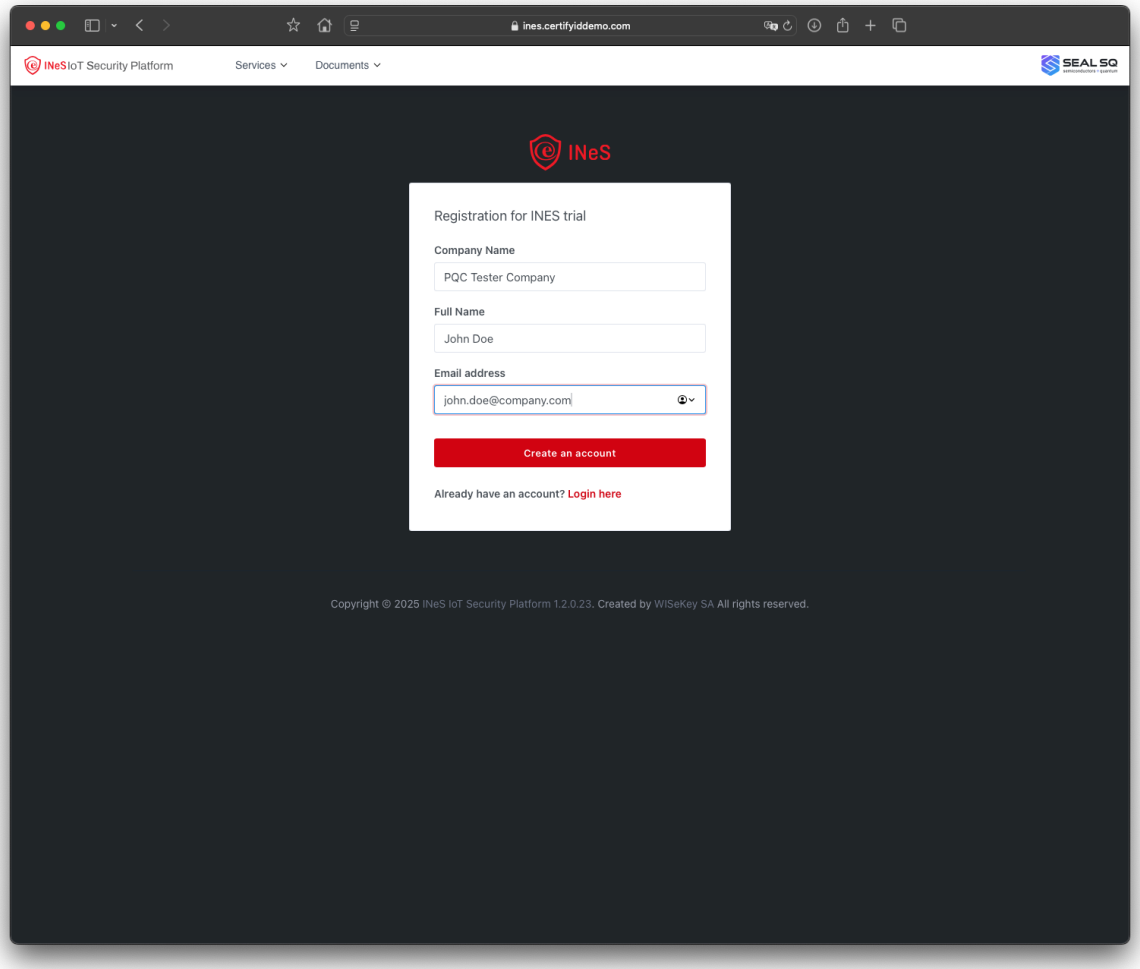
Instructions:

Step 1: Create a Trial Account

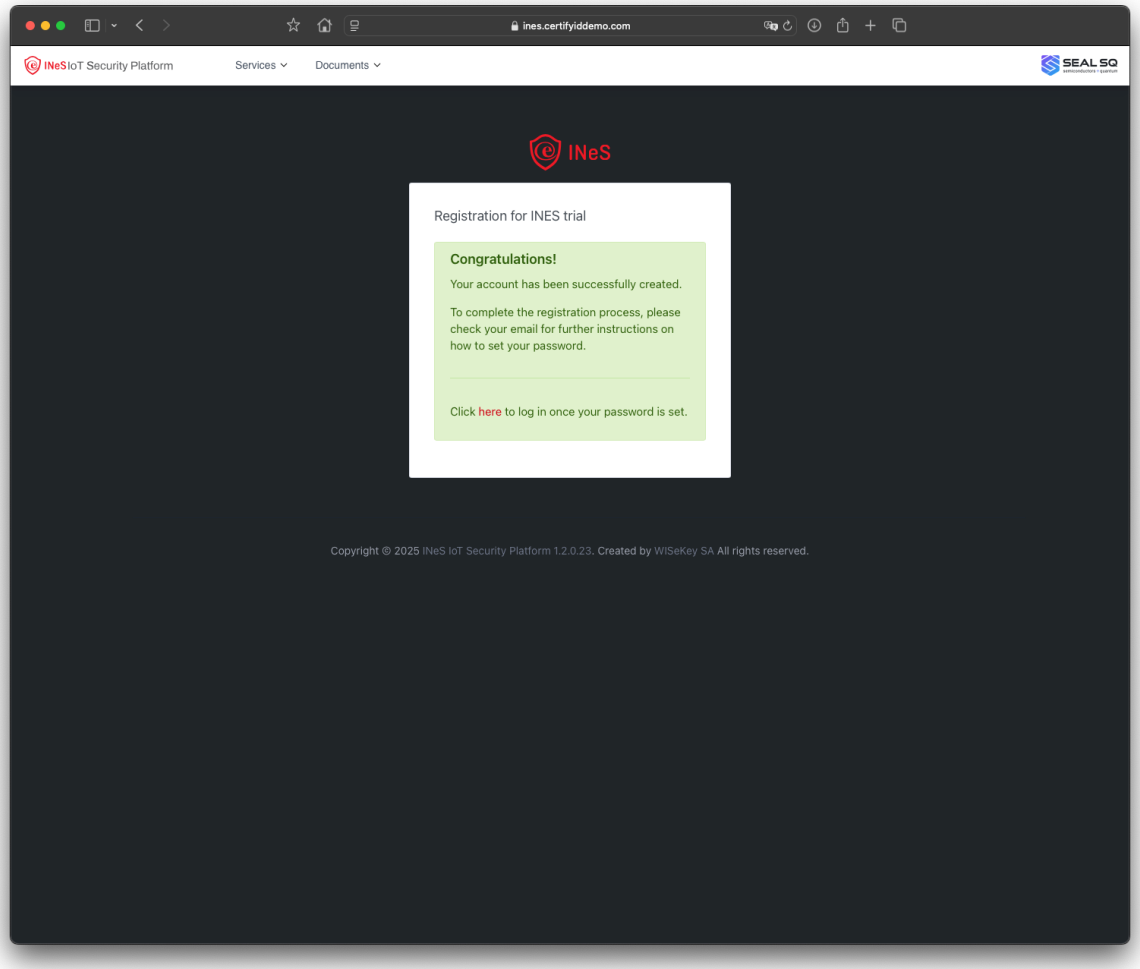
1. Open your web browser and navigate to the INeS DEMO platform's homepage at the URL https://ines.certifyiddemo.com



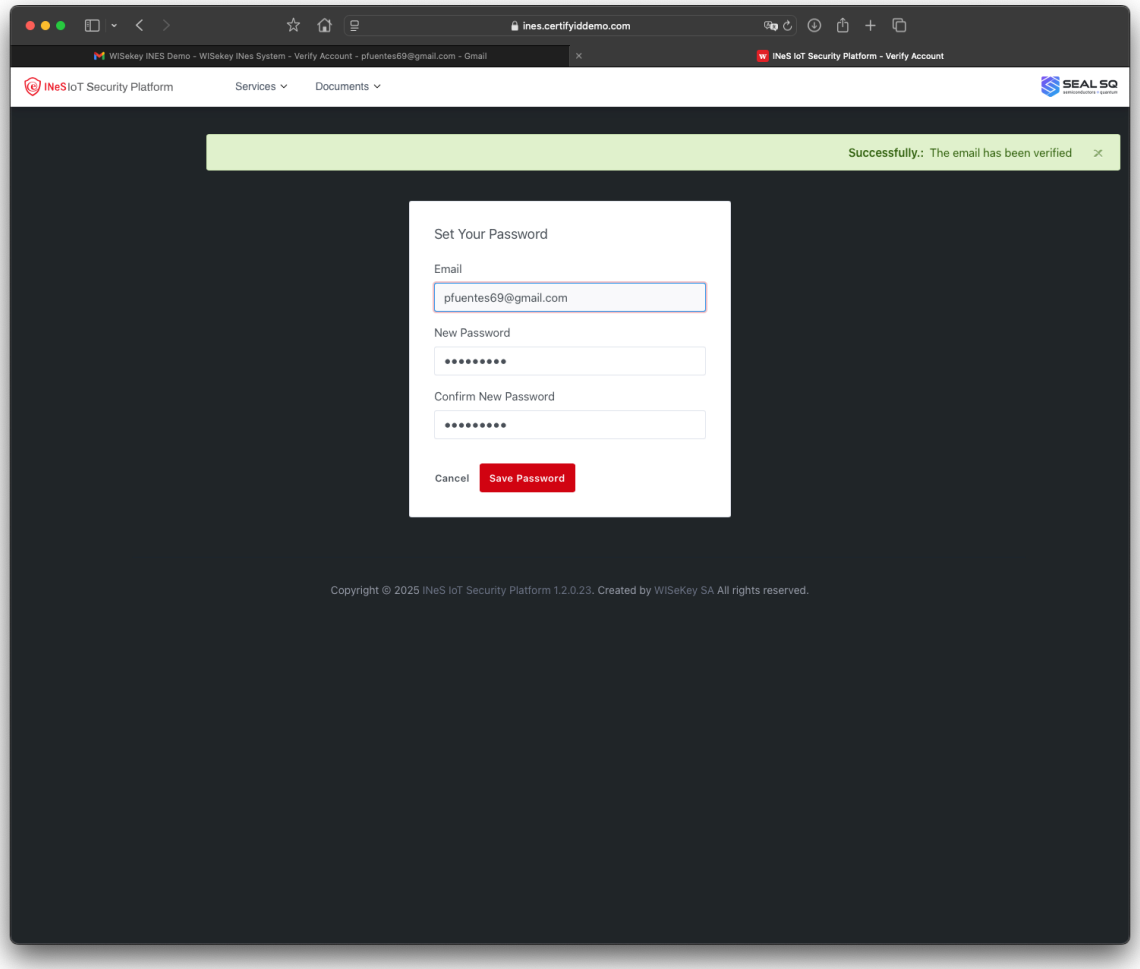
2. Click on the “Create Free Trial Account” button.



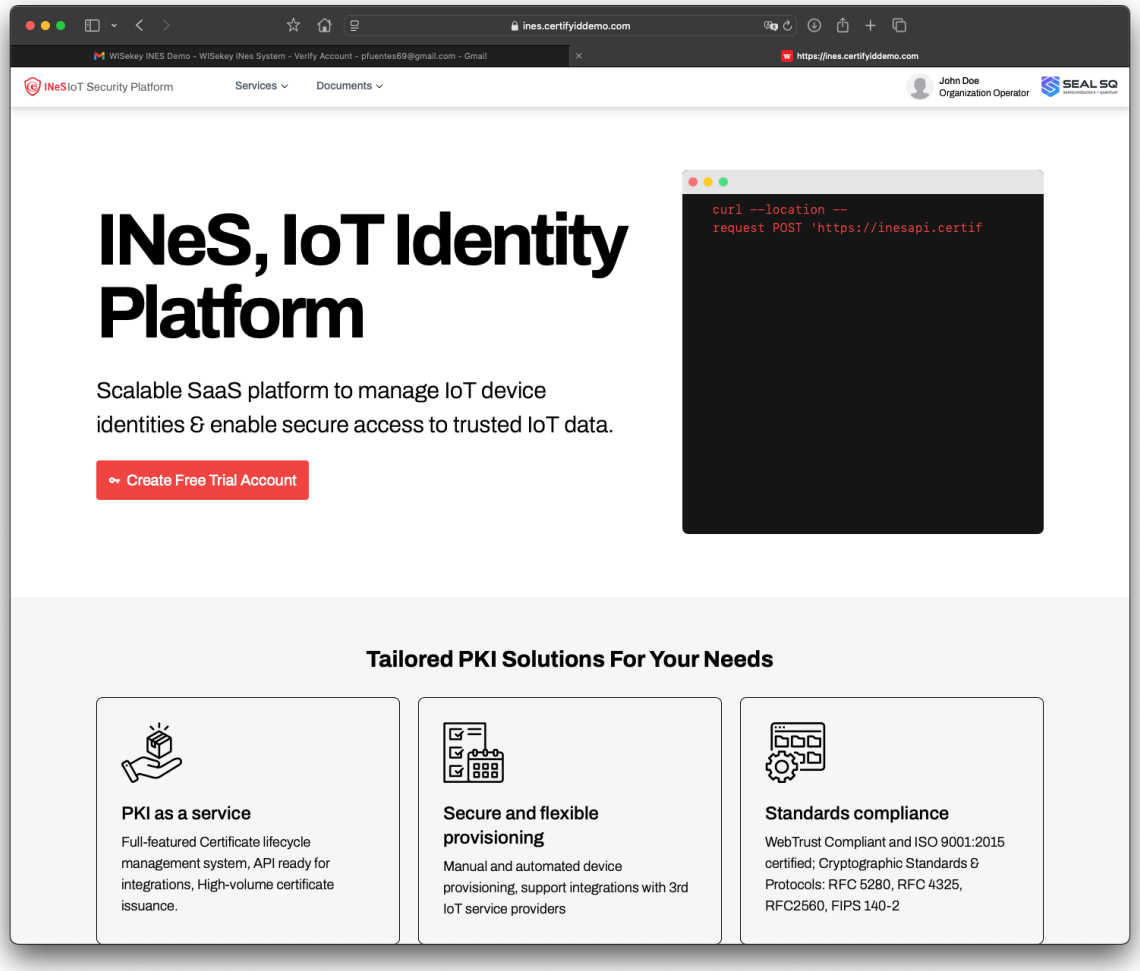
3. Fill in the required details (e.g., name, email address, and company name). You will get a confirmation message, and a mail will be sent to your mailbox to activate your account and define your password



4. Confirm your email address by clicking on the verification link sent to your inbox and define your password to access INeS.

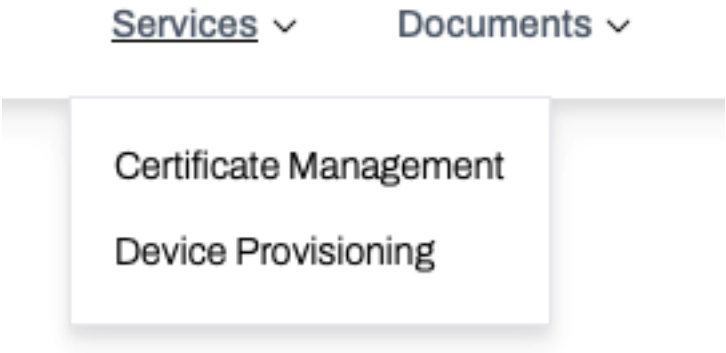


5. Log in to your newly created trial account.

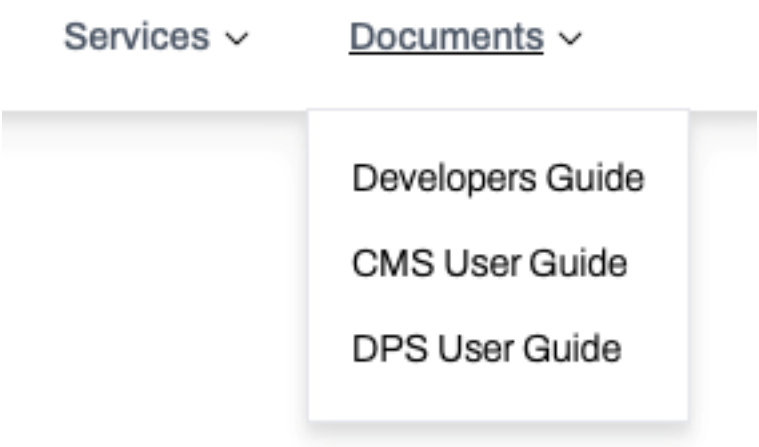


Step 2: Navigate the Menu

1. The menu “Services” gives you access to the two main modules of INeS: Certificate Management and Device Provisioning. We will focus in this recipe in Certificate Management.

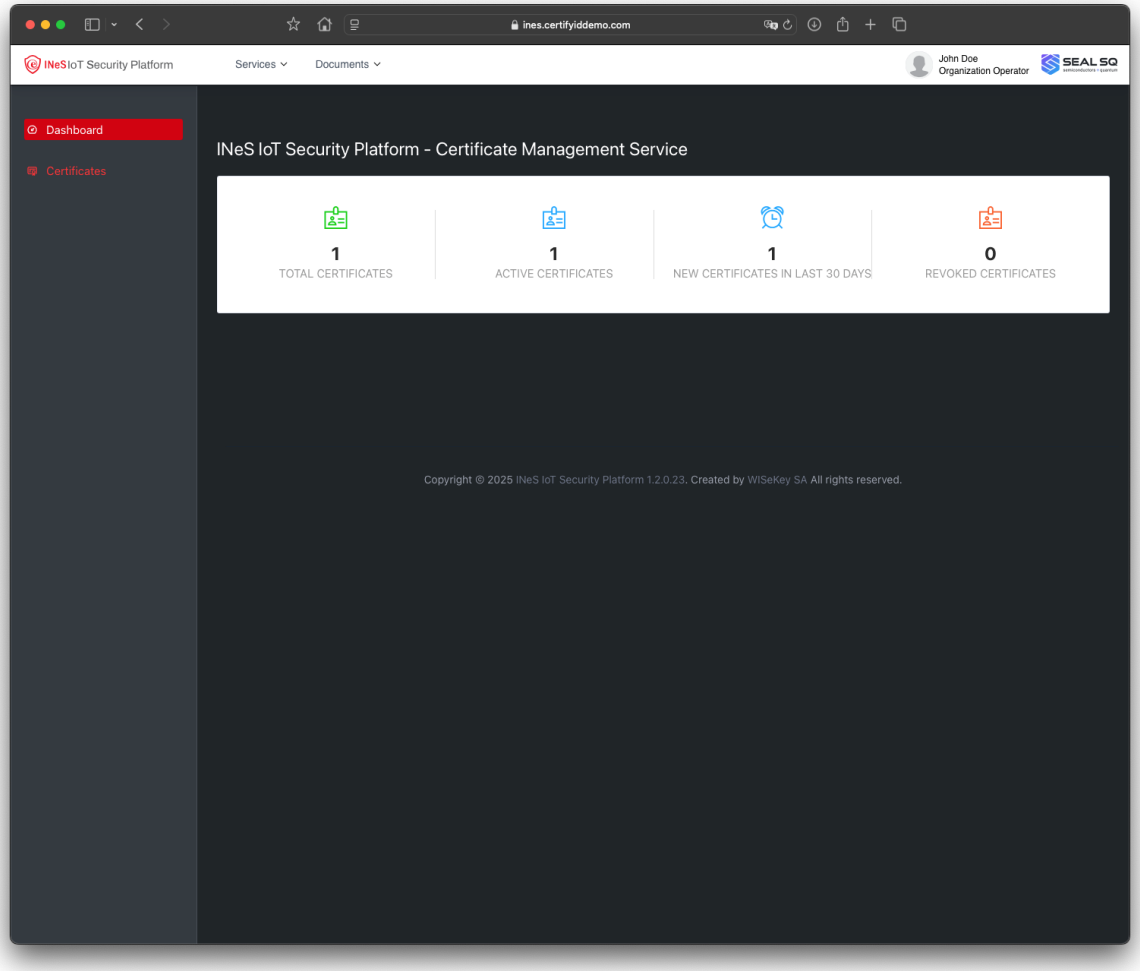


2. You can also access the user manuals and API documentation in the “Documents” menu.

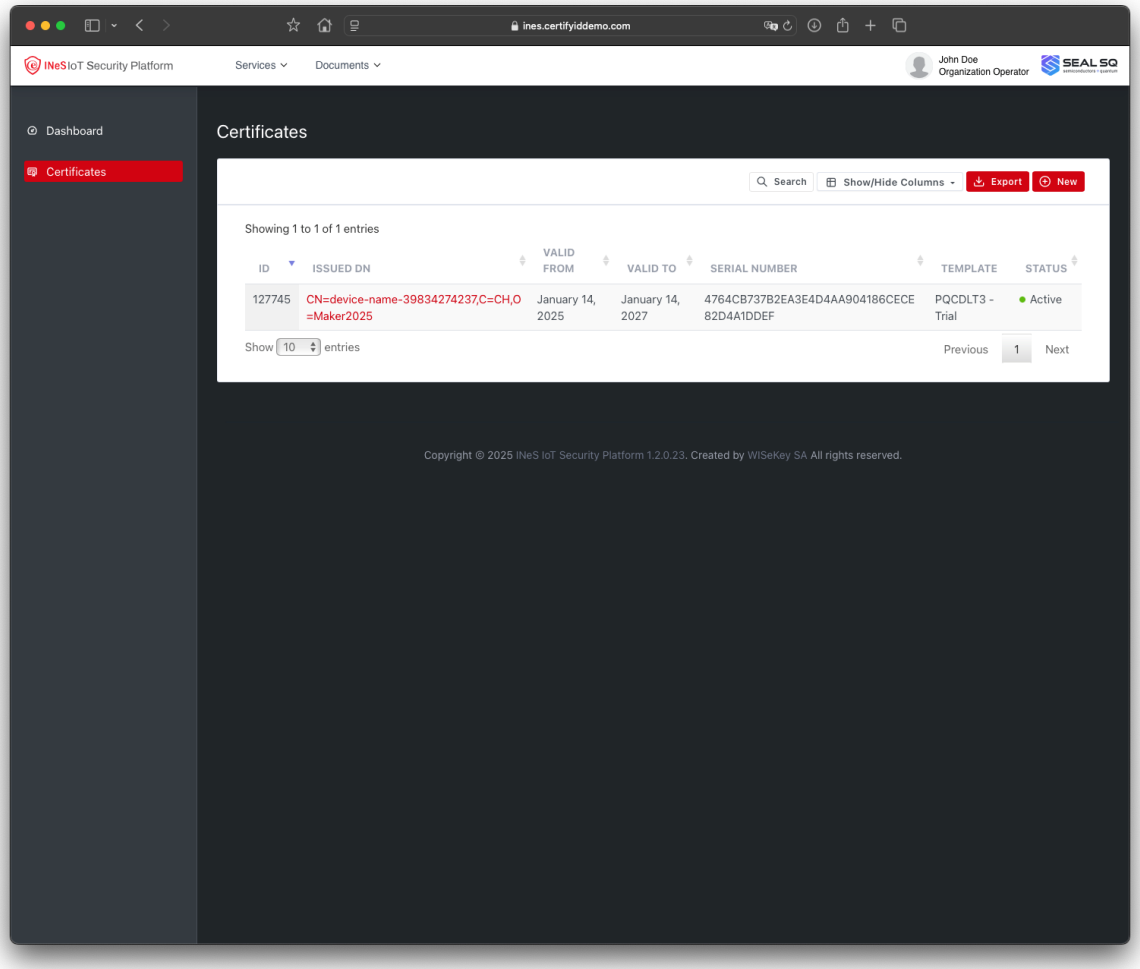


Step 3: Generate a New Certificate

1. Open the “Certificate Management” Menu option. The CMS Dashboard will open.

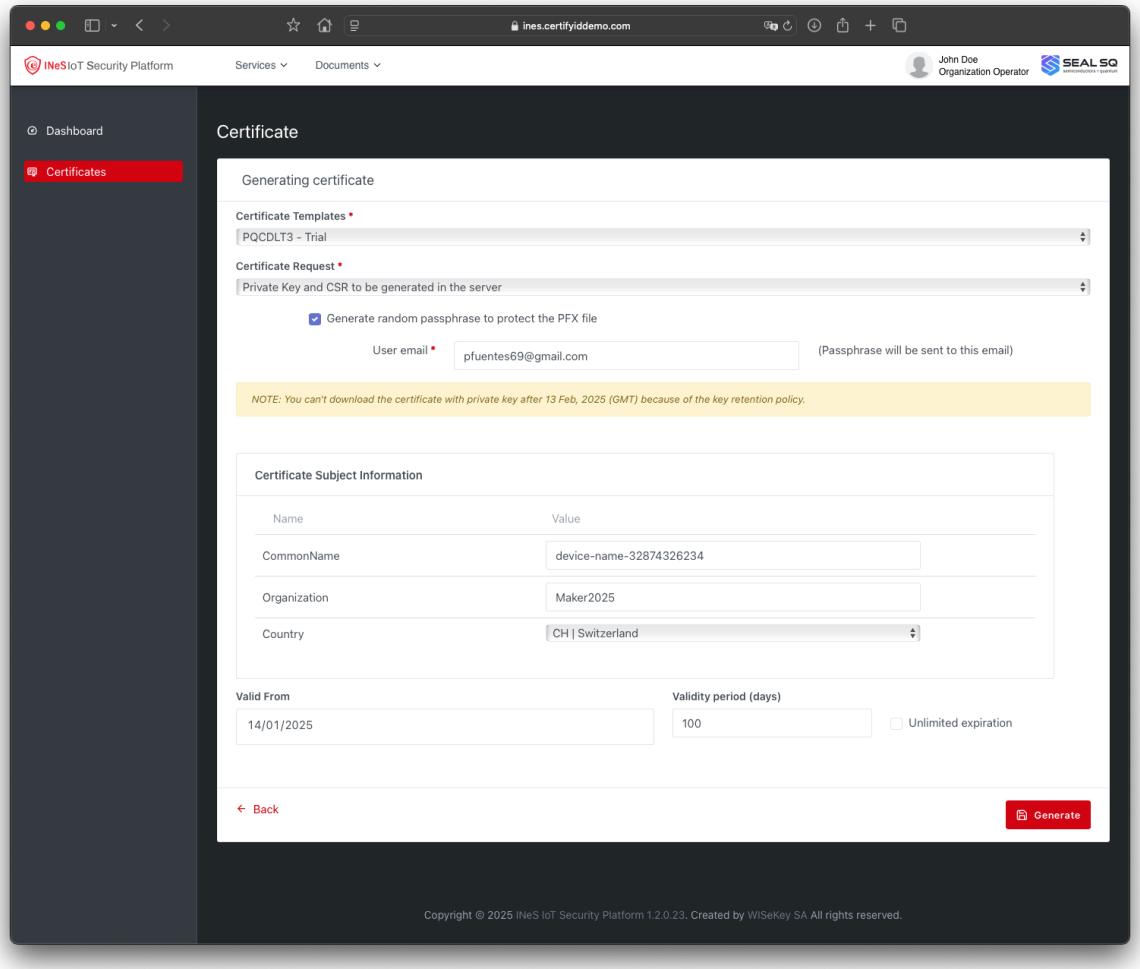


2. Click on “Certificates” to see and manage the list of certificates.

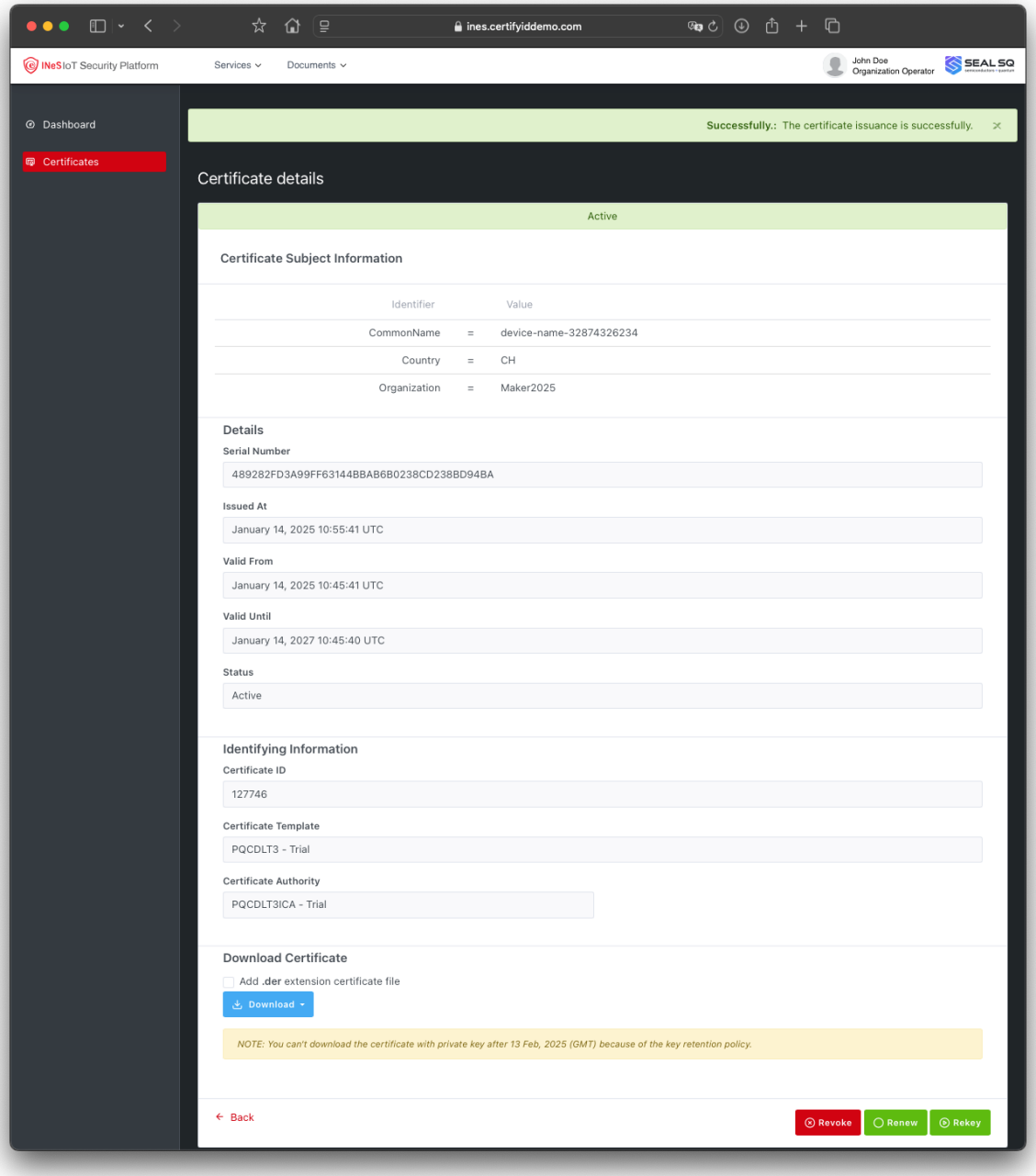


3. Click on “New” and select the type of certificate you want to generate. In this case select “PQCDLT3 – Trial”. Select how the keys will be generated (you will provide a CSR or you want the keys generated in the server fill in the required certificate details:

- Common Name (CN): The primary identifier for the certificate (e.g., the device name).
- Organization Name (O): The name of your company or entity (device manufacturer).
- Country Code)C): Select the desired country in the list.



4. Confirm the details and click on “Generate” to obtain the certificate. A page with the certificate details will open.



5. Click the **Download** button to save the certificate file to your computer.
6. If you selected to generate the keys in the server and receive a random passphrase by email, check the message sent by the platform with the PFX password and be able to download and install it.

Conclusion:

Congratulations! You've successfully generated a digital certificate using PQC algorithms on the INeS platform. With just a few simple steps, you've taken a significant stride toward securing your digital communications against quantum threats. Start exploring how these certificates can enhance your systems' security today!