

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.

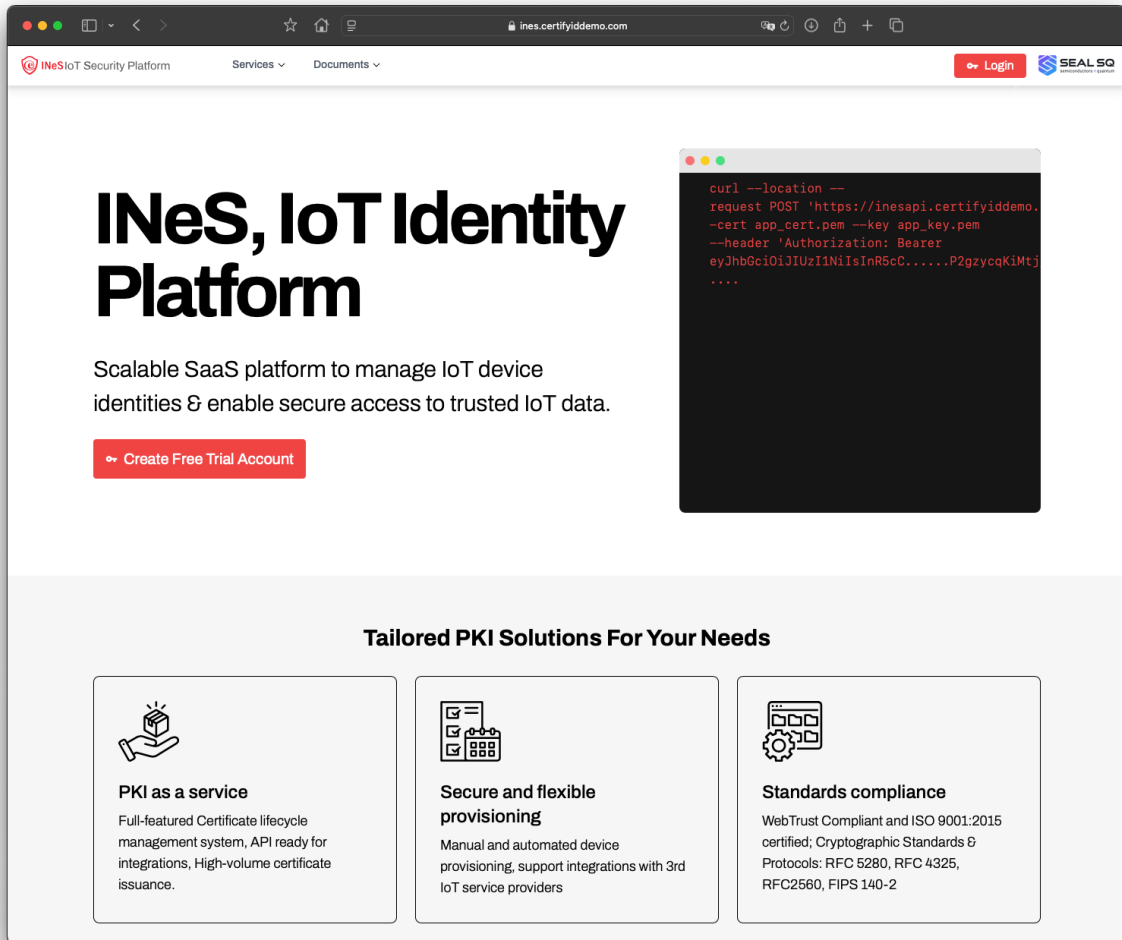
Ingredients:

- A computer
- A web browser

Instructions:

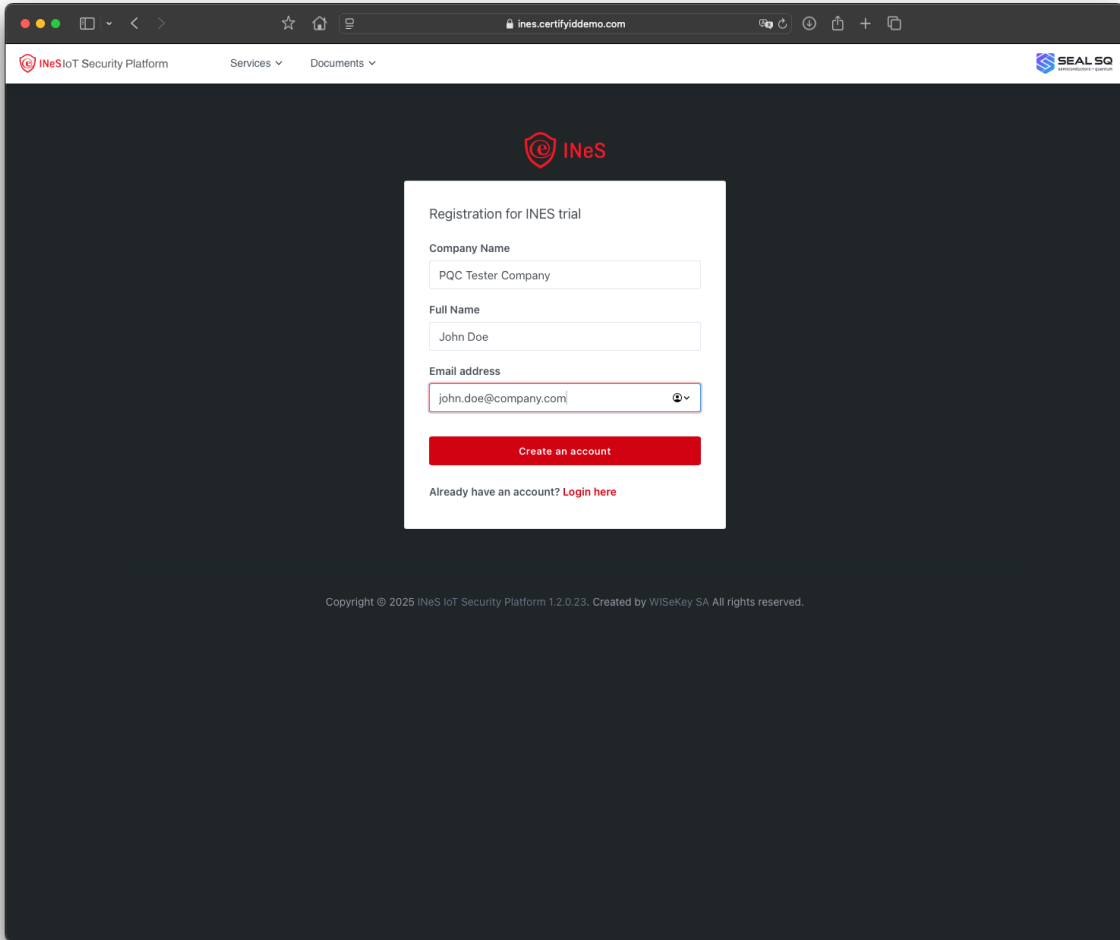
Step 1: Create a Trial Account

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



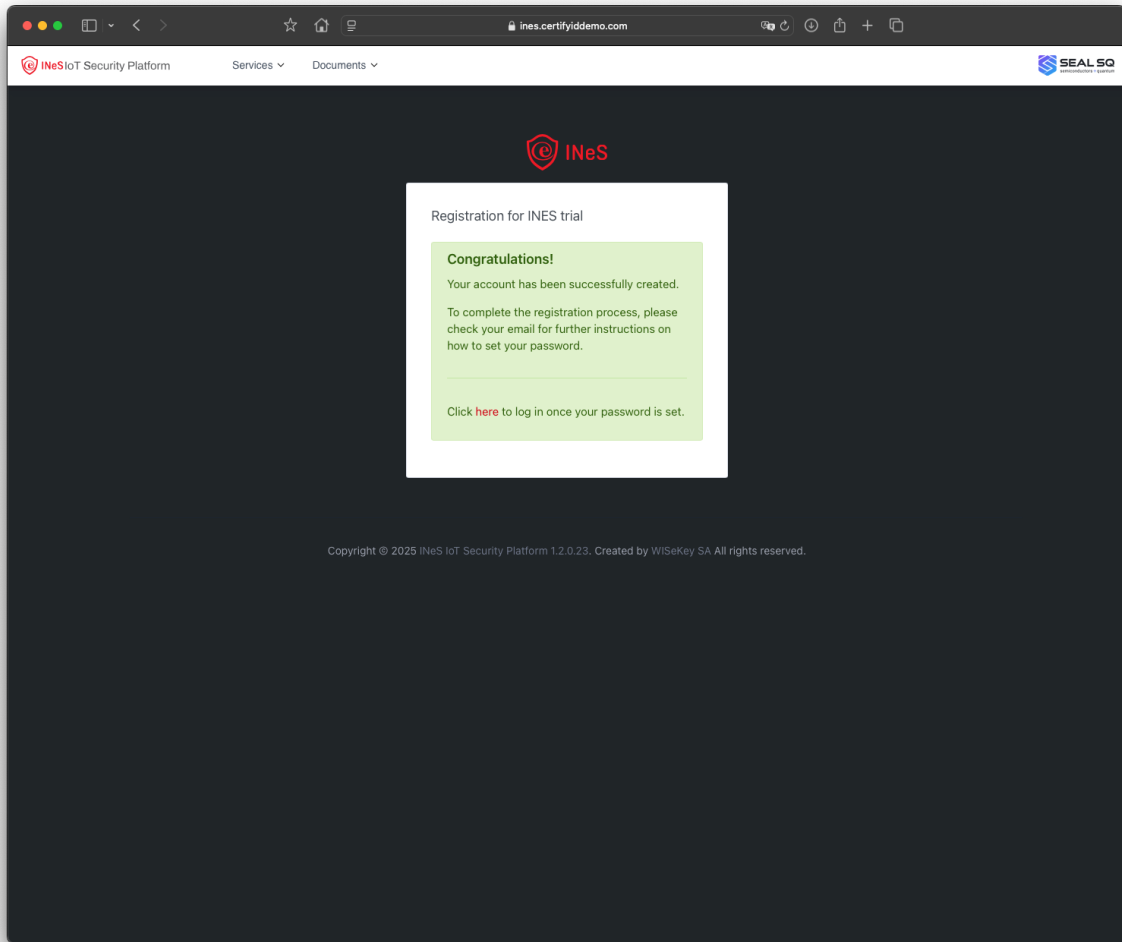
The screenshot shows a web browser window displaying the INeS IoT Security Platform website. The browser's address bar shows 'ines.certifyiddemo.com'. The website header includes the INeS IoT Security Platform logo, navigation menus for 'Services' and 'Documents', a 'Login' button, and the SEAL SQ logo. The main content area features a large heading 'INeS, IoT Identity Platform' and a sub-heading 'Scalable SaaS platform to manage IoT device identities & enable secure access to trusted IoT data.' Below this is a red button labeled 'Create Free Trial Account'. To the right is a terminal window showing a curl command: 'curl --location --request POST 'https://inesapi.certifyiddemo...' --cert app_cert.pem --key app_key.pem --header 'Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cGU6IjY9ImF...''. Below the main content is a section titled 'Tailored PKI Solutions For Your Needs' with three columns: 'PKI as a service' (Full-featured Certificate lifecycle management system, API ready for integrations, High-volume certificate issuance), 'Secure and flexible provisioning' (Manual and automated device provisioning, support integrations with 3rd IoT service providers), and 'Standards compliance' (WebTrust Compliant and ISO 9001:2015 certified; Cryptographic Standards & Protocols: RFC 5280, RFC 4325, RFC2580, FIPS 140-2).

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

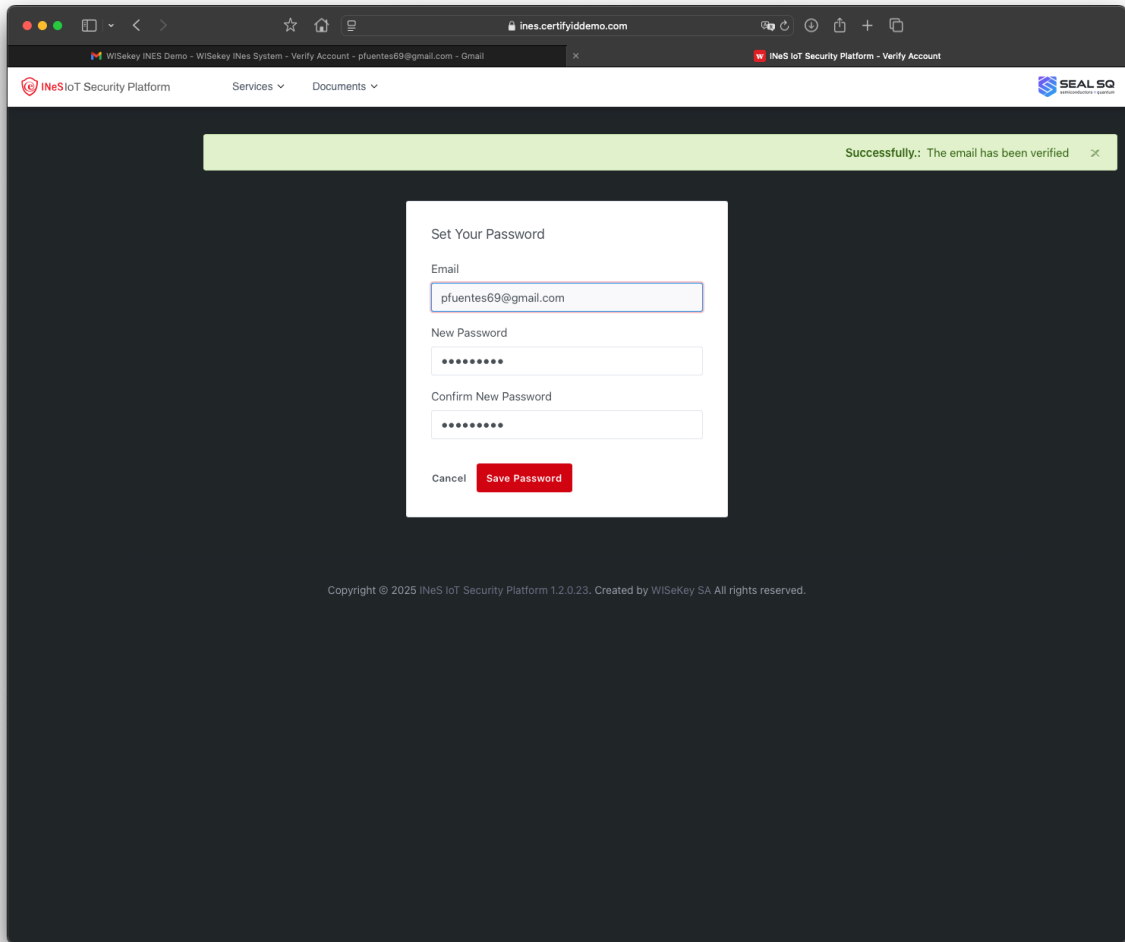


The screenshot shows a web browser window with the URL `ines.certifyiddemo.com`. The page header includes "INeS IoT Security Platform", "Services", "Documents", and the "SEAL SQ" logo. The main content area features the "INeS" logo and a registration form titled "Registration for INES trial". The form contains three input fields: "Company Name" with the value "PQC Tester Company", "Full Name" with the value "John Doe", and "Email address" with the value "john.doe@company.com". A red "Create an account" button is positioned below the email field. At the bottom of the form, there is a link: "Already have an account? [Login here](#)". A copyright notice at the bottom of the page reads: "Copyright © 2025 INeS IoT Security Platform 1.2.0.23. Created by WiSeKey SA All rights reserved."

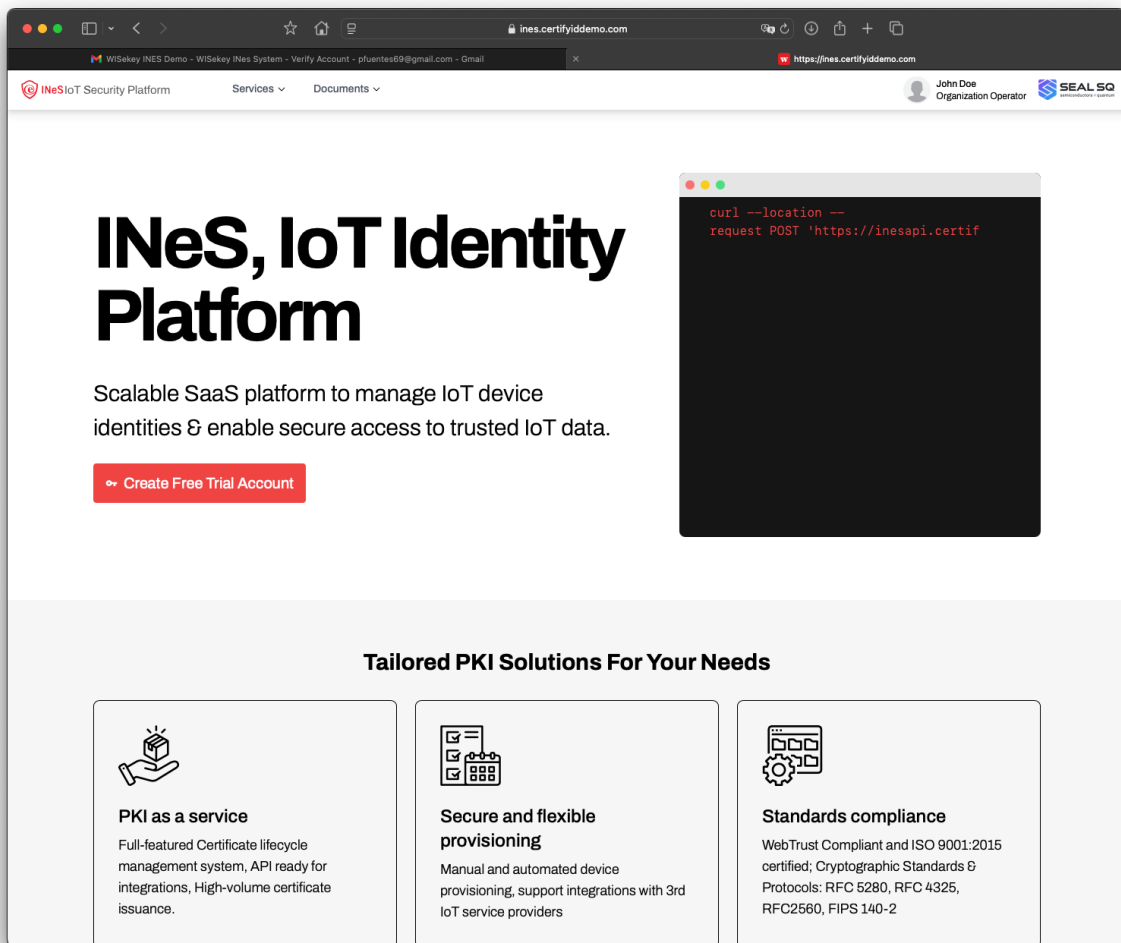
3. Fill in the required details (e.g., name, email address, and company name). You will get a confirmation message, and a mail will be sent to your mailbox to activate your account and define your password



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.

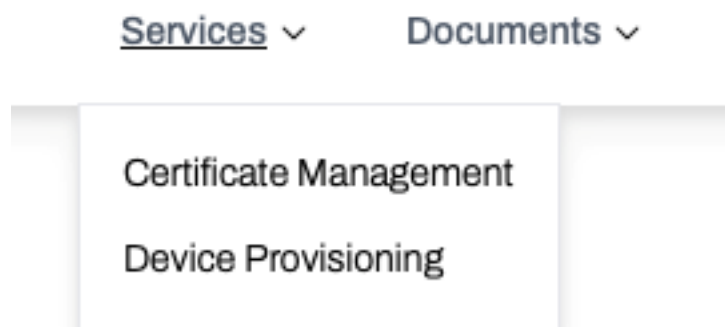


The screenshot shows the INeS IoT Security Platform website. The main heading is "INeS, IoT Identity Platform". Below it, the text reads: "Scalable SaaS platform to manage IoT device identities & enable secure access to trusted IoT data." A red button says "Create Free Trial Account". To the right, there is a terminal window showing a curl command: `curl --location --request POST 'https://inesapi.certif'`. Below the main content, there is a section titled "Tailored PKI Solutions For Your Needs" with three columns:

- PKI as a service**: Full-featured Certificate lifecycle management system, API ready for integrations, High-volume certificate issuance.
- Secure and flexible provisioning**: Manual and automated device provisioning, support integrations with 3rd IoT service providers.
- Standards compliance**: WebTrust Compliant and ISO 9001:2015 certified; Cryptographic Standards & Protocols: RFC 5280, RFC 4325, RFC2560, FIPS 140-2.

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.

Services ▾

Documents ▾

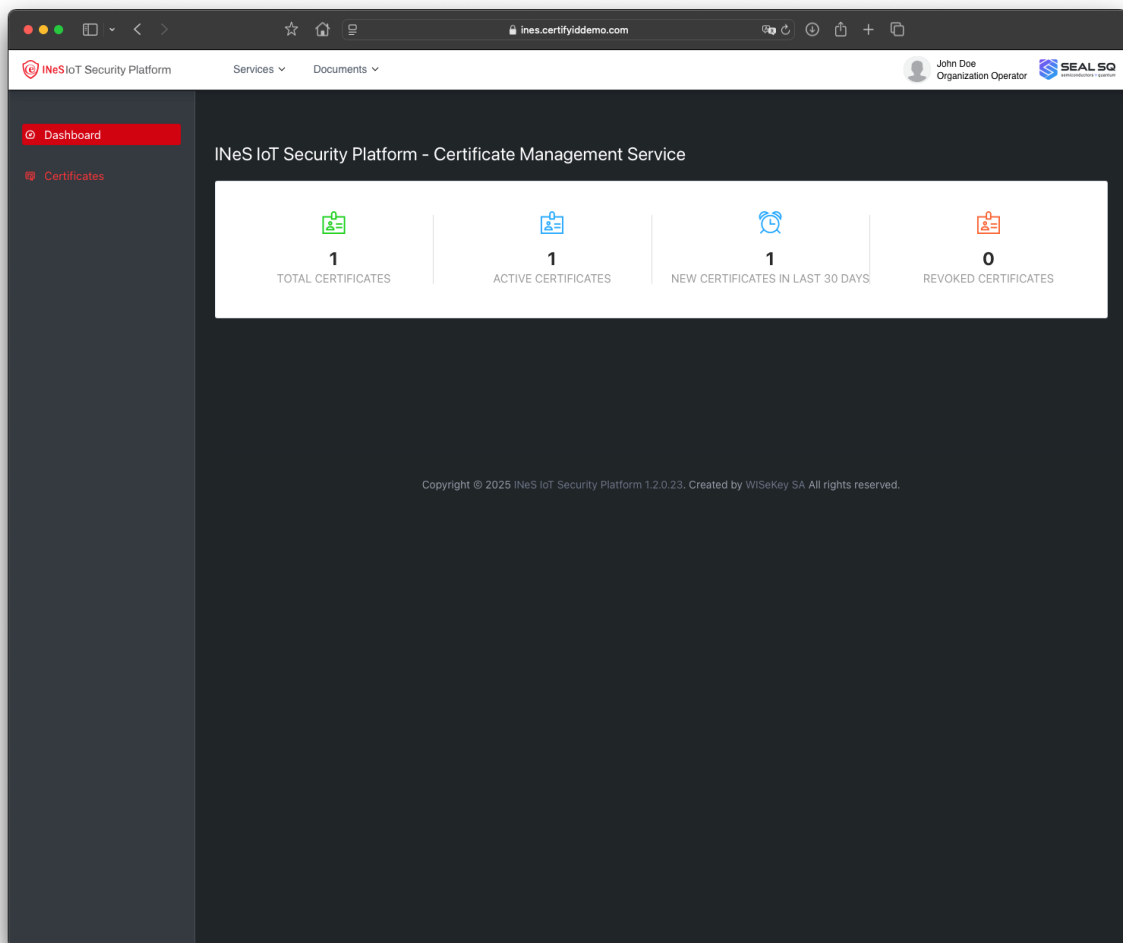
Developers Guide

CMS User Guide

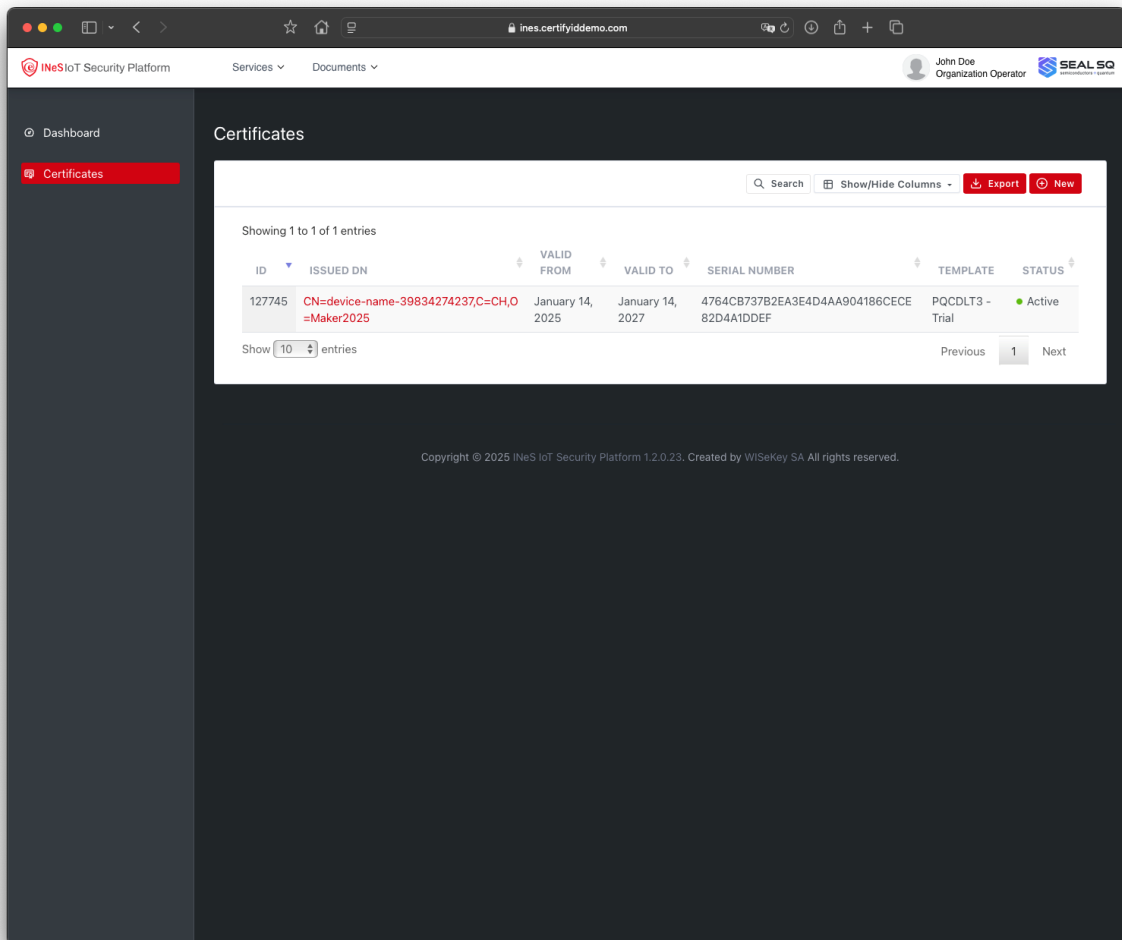
DPS User Guide

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.

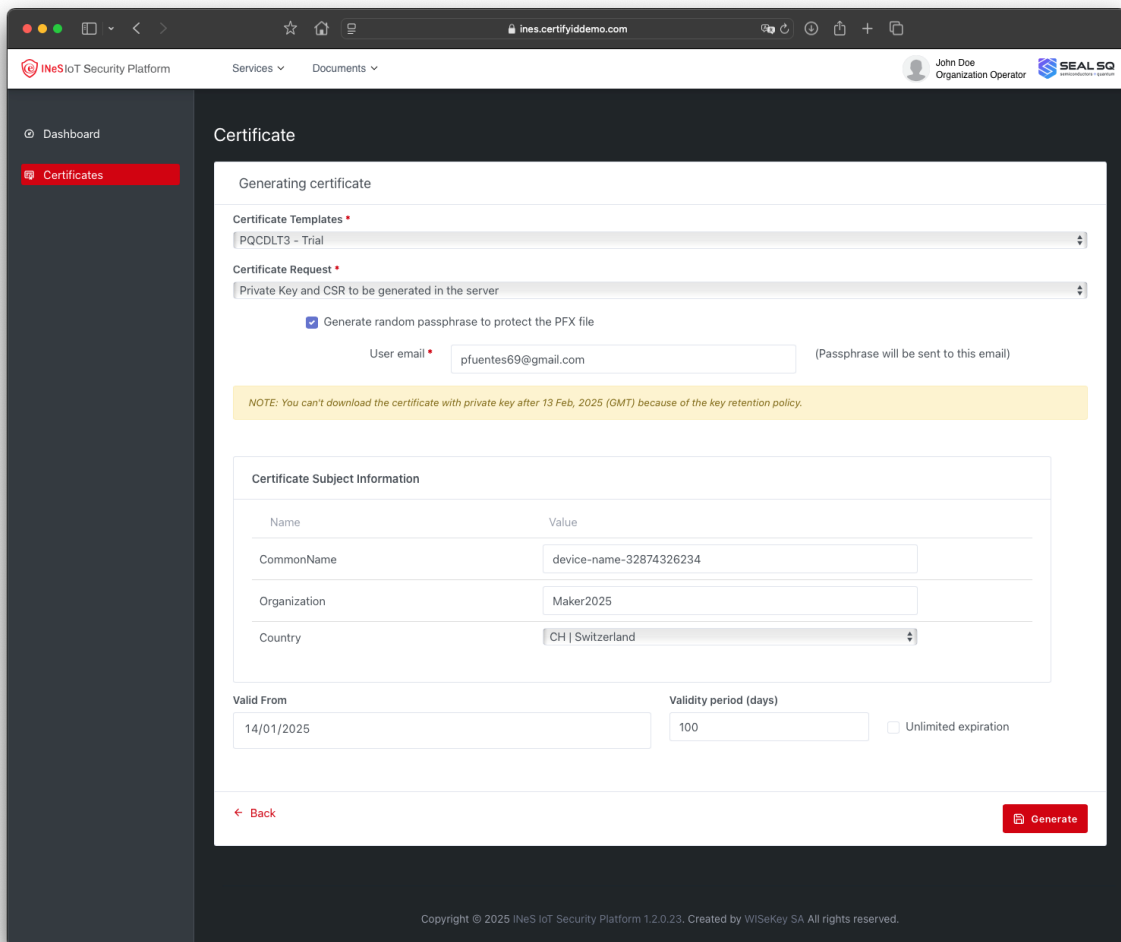


The screenshot shows the IneS IoT Security Platform interface. The left sidebar contains a navigation menu with 'Dashboard' and 'Certificates' (highlighted in red). The main content area is titled 'Certificates' and displays a table with one entry. The table has columns for ID, ISSUED DN, VALID FROM, VALID TO, SERIAL NUMBER, TEMPLATE, and STATUS. The entry has ID 127745, ISSUED DN CN=device-name-39834274237,C=CH,O=Maker2025, VALID FROM January 14, 2025, VALID TO January 14, 2027, SERIAL NUMBER 4764CB737B2EA3E4D4AA904186CECE82D4A1DDEF, TEMPLATE PQCDLT3 - Trial, and STATUS Active. Below the table, there is a 'Show 10 entries' dropdown and 'Previous 1 Next' navigation links. The top right of the interface shows the user 'John Doe, Organization Operator' and the SEAL SQ logo. The bottom of the page has a copyright notice: 'Copyright © 2025 IneS IoT Security Platform 1.2.0.23. Created by WiSeKey SA. All rights reserved.'

ID	ISSUED DN	VALID FROM	VALID TO	SERIAL NUMBER	TEMPLATE	STATUS
127745	CN=device-name-39834274237,C=CH,O=Maker2025	January 14, 2025	January 14, 2027	4764CB737B2EA3E4D4AA904186CECE82D4A1DDEF	PQCDLT3 - Trial	Active

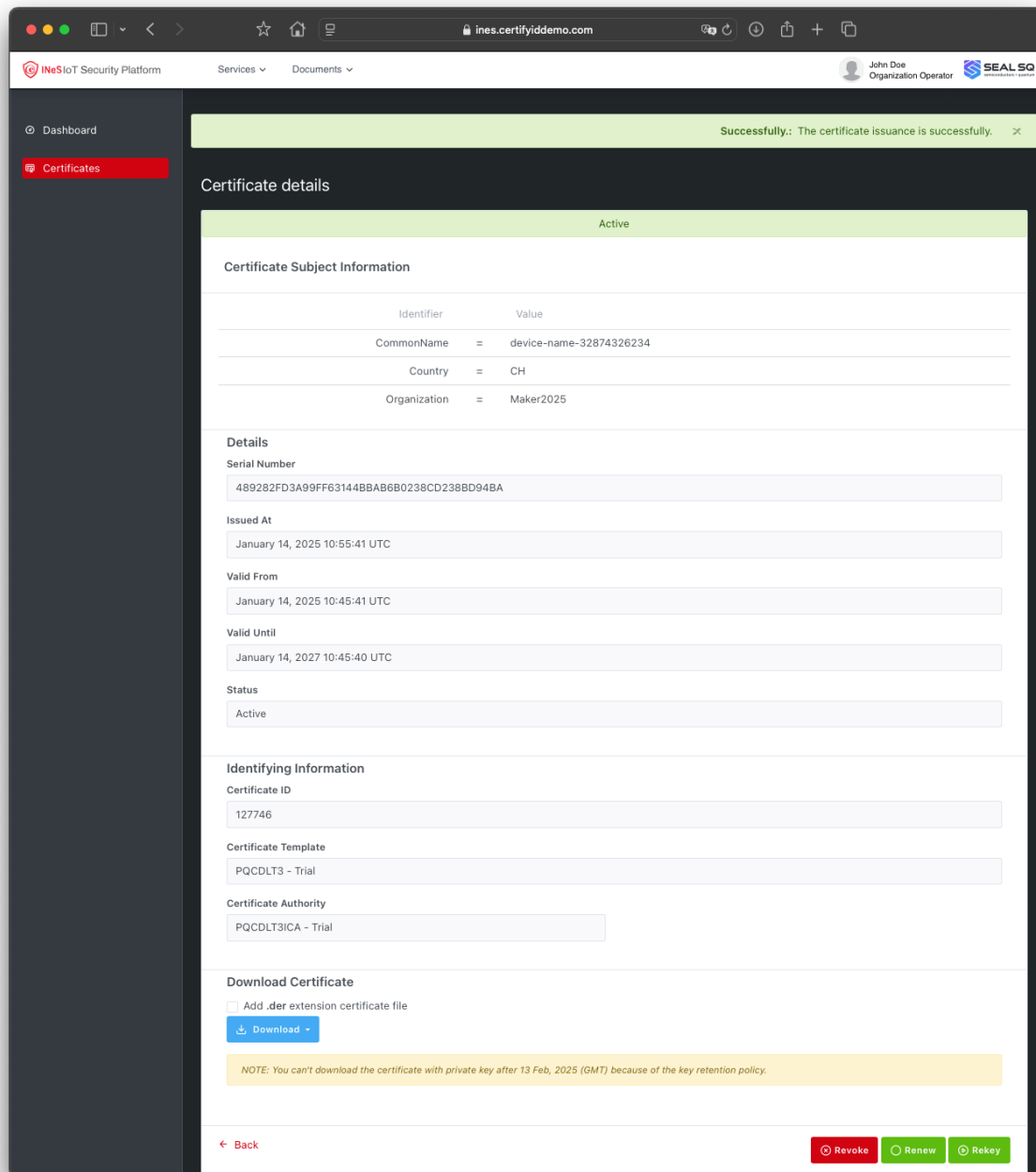
3. Click on “New” and select the type of certificate you want to generate. In this case select “PQCFLT3 – Trial”. Select how the keys will be generated (you will provide a CSR or you want the keys generated in the server fill in the required certificate details:

- 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.



The screenshot shows a web browser window displaying the 'Certificate' page in the iNeS IoT Security Platform. The page title is 'Generating certificate'. The interface includes a sidebar with 'Dashboard' and 'Certificates' (highlighted in red). The main content area has a 'Certificate Templates' dropdown set to 'PQCFLT3 - Trial' and a 'Certificate Request' dropdown set to 'Private Key and CSR to be generated in the server'. A checkbox 'Generate random passphrase to protect the PFX file' is checked. The 'User email' field contains 'pfuentes69@gmail.com'. A yellow note states: 'NOTE: You can't download the certificate with private key after 13 Feb, 2025 (GMT) because of the key retention policy.' Below this is a 'Certificate Subject Information' table with fields for Name, CommonName (device-name-32874326234), Organization (Maker2025), and Country (CH | Switzerland). At the bottom, there are fields for 'Valid From' (14/01/2025) and 'Validity period (days)' (100), with an 'Unlimited expiration' checkbox. A 'Back' button is on the left and a 'Generate' button is on the right. The footer contains the copyright notice: 'Copyright © 2025 iNeS IoT Security Platform 1.2.0.23. Created by WiSeKey SA All rights reserved.'

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



The screenshot shows a web browser window displaying the IneS IoT Security Platform. The page title is "Certificate details" and the status is "Active". A green notification bar at the top right says "Successfully.: The certificate issuance is successfully." The interface is divided into several sections:

- Certificate Subject Information:** A table with two columns: Identifier and Value.

Identifier	Value
CommonName	= device-name-32874326234
Country	= CH
Organization	= Maker2025
- Details:** A list of fields with their values:
 - Serial Number: 489282FD3A99FF63144BBAB6B0238CD238BD94BA
 - Issued At: January 14, 2025 10:55:41 UTC
 - Valid From: January 14, 2025 10:45:41 UTC
 - Valid Until: January 14, 2027 10:45:40 UTC
 - Status: Active
- Identifying Information:** A list of fields with their values:
 - Certificate ID: 127746
 - Certificate Template: PQCDLT3 - Trial
 - Certificate Authority: PQCDLT3ICA - Trial
- Download Certificate:** A section with a checkbox "Add .der extension certificate file" (unchecked) and a "Download" button. Below it is a yellow note: "NOTE: You can't download the certificate with private key after 13 Feb, 2025 (GMT) because of the key retention policy."

At the bottom of the page, there are three buttons: "Back" (with a left arrow), "Revoke" (with a red circle and slash), "Renew" (with a green circle and refresh), and "Rekey" (with a green circle and key).

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!