periMICA Container

PKI4mfg

User Guide

Perinet
Seamless IoT Connectivity

Abstract

This document outlines the functionality of the PKI4mfg container. The PKI4mfg is designed for use in the manufacturing of *periCORE* based devices, managing security apparatus to establish security protocols during production.

Doc-No.: PRN.100.809 rev: 2

today

Document Information

Title	periMICA Container
Subtitle	PKI4mfg
Type	User Guide
Status	Release
Version	2
Date	today
Disclosure Restriction	

Contents

1 Overview

The PKI4mfg container is specifically designed to manage security certificates in the manufacturing environment. It leverages *YubiKey* devices, which are depicted in figure 1, to create and store security keys. *YubiKeys* are manufactured by Yubico [15] typically used for two-factor authentication (2FA) due to their ability to safely store cryptographic keys. In the context of PKI4mfg, *YubiKeys* hold the private keys of PKI security entities, such as the root CA and batch CA. The Batch CA is the entity responsible for signing the attestation host certificates, which are subsequently deployed and stored on each manufactured device.

Utilizing an authentic *YubiKey*, the PKI4mfg container configures itself to employ the Batch CA's private key, which is stored on a YubiKey inserted into a periMICA USB slot. This setup facilitates the deployment of attestation certificates to devices.

Figure 1: YubiKey Devices

The container integrates Perinet base services through the API and features its own distinct API, enabling users to configure it effectively for production readiness.

Additionally, the container offers a user-friendly web-based UI, allowing users to effortlessly manage the available features, as shown in figure 2. This document provides a detailed description of the container's functionalities and usage instructions.

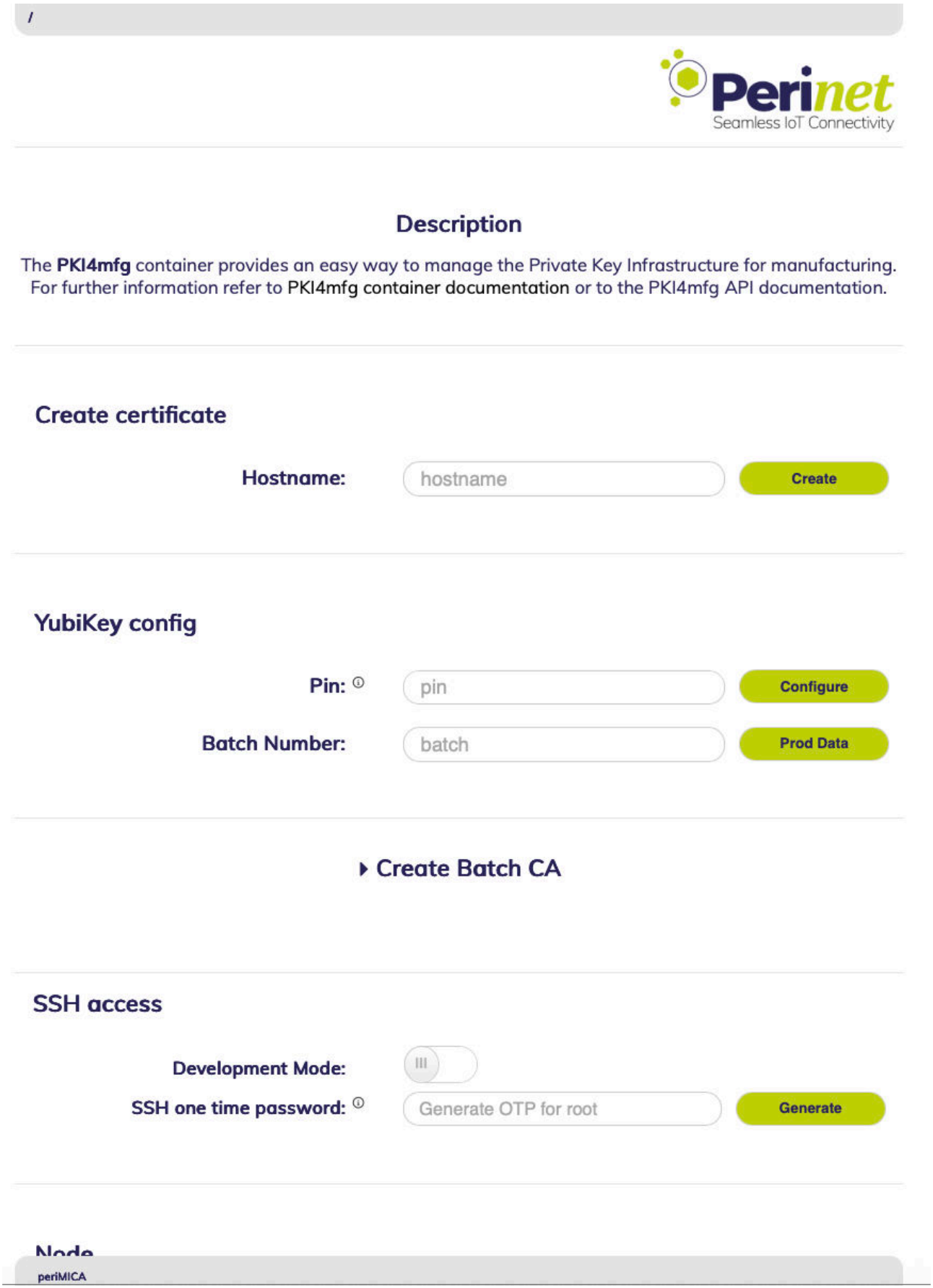

Figure 2: PKI4mfg homepage

2 Features

2.1 YubiKey config

To begin, ensure that the *YubiKey* device is connected to the periMICA USB slot. The initial step into the container involves configuring the Batch CA *YubiKey*. Enter the PIN and click on the **Configure** button, as illustrated in figure 3.

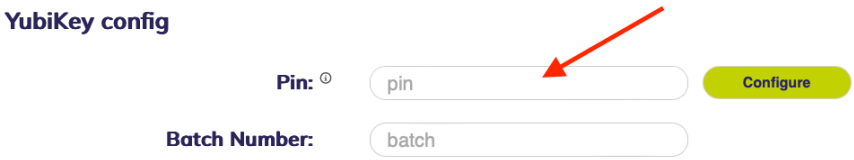

Figure 3: Type the Pin and click on Configure

The Pin will be verified, and the confirmation message is expected:

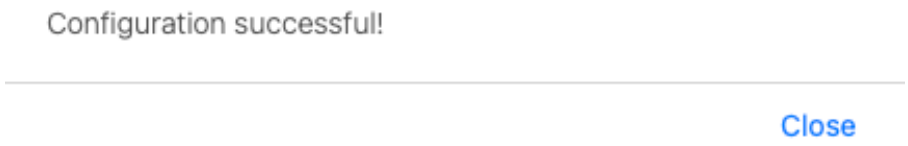

Figure 4: Configured successful

Once the Batch CA *YubiKey* is correctly configured, the Batch Number extracted from the certificate can be viewed in the Batch Number field, as shown in figure 5. The Batch Number is composed of the year and the week number in which the *YubiKey* was created, formatted as YYYY-WW.

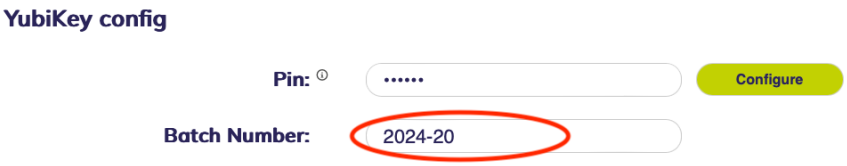

Figure 5: Batch Number Found

If the Pin is not correct one error will pop up (figure 6) and the Batch Number will remain empty.

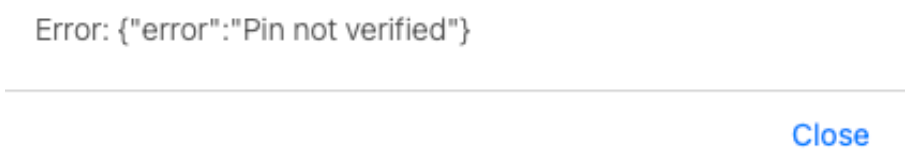

Figure 6: Error in PIN

2.2 Create a host certificate

Once the *YubiKey* is configured, the container is prepared to generate host certificates signed by the *YubiKey* Batch CA. From the homepage, enter the hostname and select the **Create Certificate** button, as depicted in figure 7.

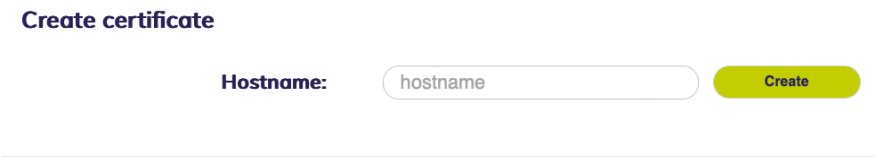

Figure 7: Create Certificate

The chain certificates are automatically extracted from the slots in the Batch CA *YubiKey*, ensuring a seamless integration process. The chain certificate will be presented, figure 8.

Note: The certificate chain does not include the Root CA. The generated chain certificate is designed for storage directly on the device and should not be concatenated with the Root CA.

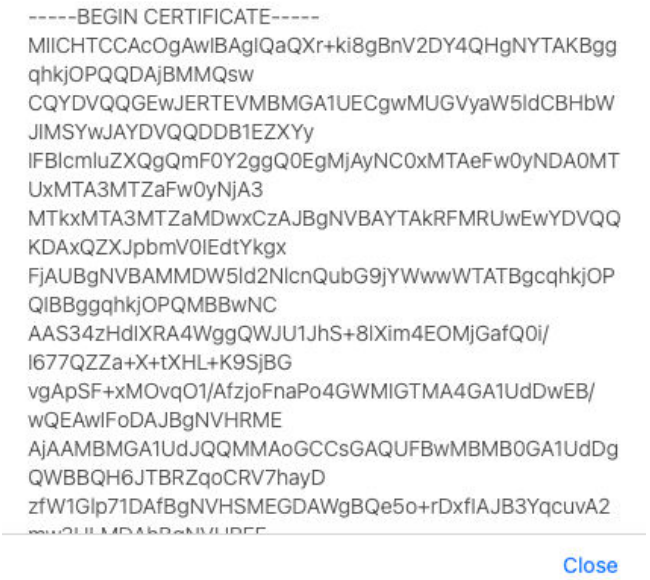

Figure 8: Example Certificate

2.3 Create Batch CA

The functionality to create a Batch CA is available in the webUI. To access it, click on the side arrow labelled *Create*, as illustrated in Figure 9, to expand the section, which is hidden by default.

This feature is designed to prepare a YubiKey for use in a specific production batch. In this context, it is required to provide complete and accurate production data.

Figure 9: Expand the Create Batch CA Session

The Batch Order CA YubiKey is typically created by the responsible for initiating the production batch. This YubiKey is used to generate the production certificates for all devices within the specified batch. The *Batch CA* will be labelled according to the *Batch Number* in the format *YYYY-WW*.

The production data form, as shown in Figure 10, must be completed in full before proceeding. Enter the necessary production certificate data and the YubiKey credentials, then click on *Create*. The PIN for the Batch Order CA YubiKey is required in order to sign the new Batch CA certificate. Additionally, the PIN of the *Batch CA* is used to sign the CSR. The associated Management Key is used to generate the private key and to store the certificates in the appropriate slots of the YubiKey.

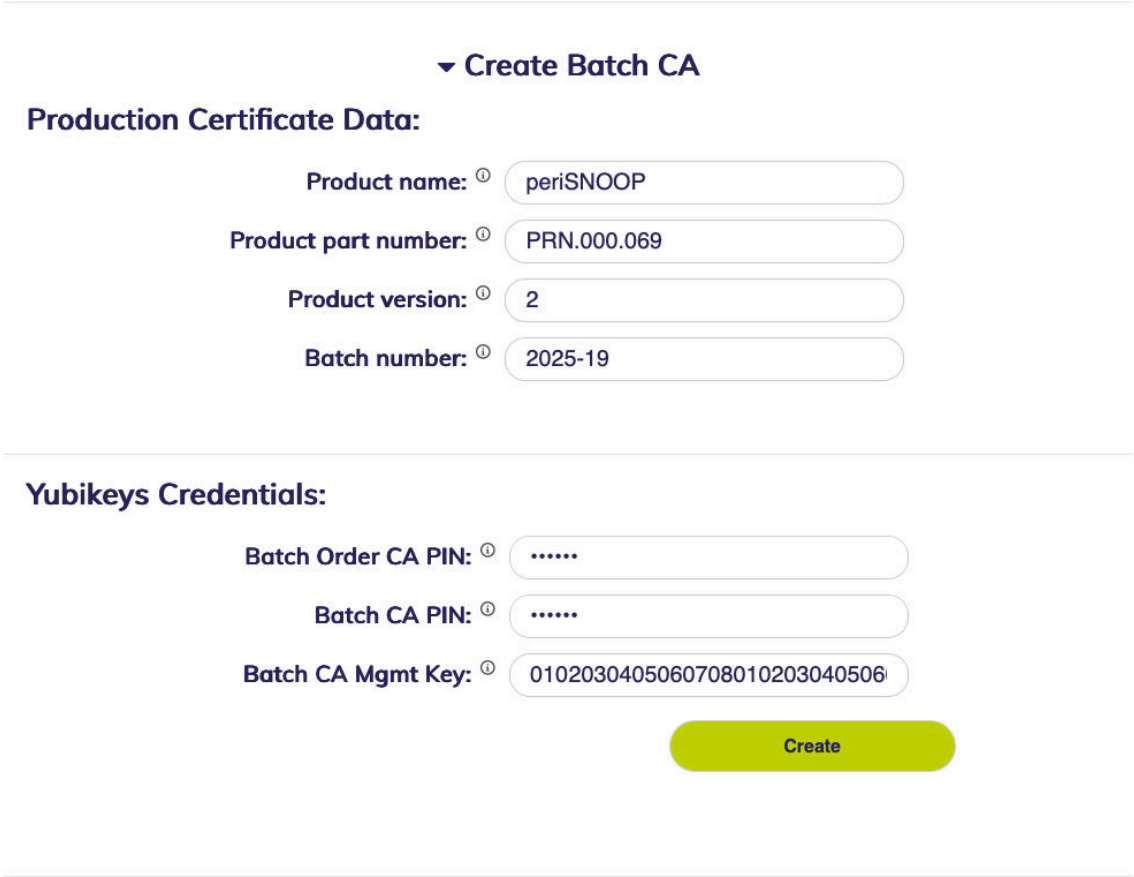

Figure 10: Production data

Upon successful creation, a confirmation message will be displayed, as shown in Figure 11.

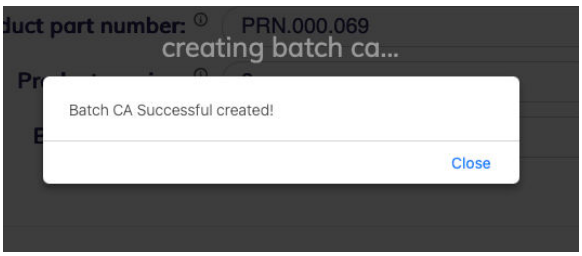

Figure 11: Confirmation Message

2.4 SSH access

The container can be also accessed via SSH using a OTP, which can be generated through the *webUI*, as illustrated in figure 12. The SSH access is particularly important in order to establishment the Production PKI, for further instructions please refer to the *Production Public Key Infrastructure Establishment document*[13].

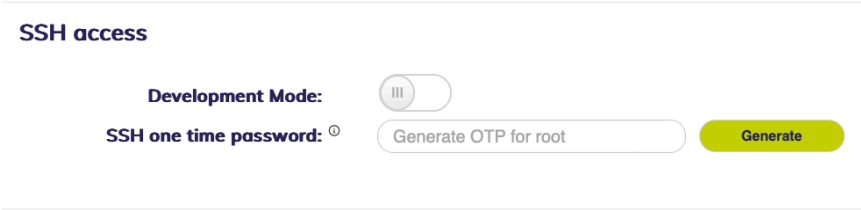

Figure 12: SSH access

Switch to *Development mode* (figure 13) to open port 22, enabling SSH access and allowing the generation of a one-time password.

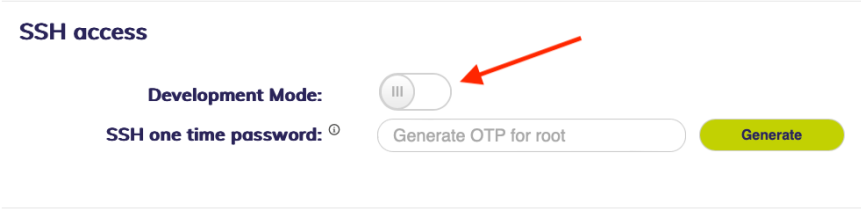

Figure 13: SSH enable development mode

Once SSH access is enabled it is possible to generate the one time password, to do it, click on *Generate* and confirm the message like the figure in 14 to proceed.

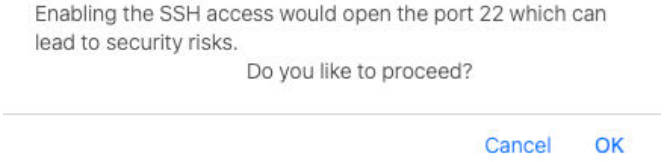

Figure 14: Development node confirmation message

After clicking on *Generate* the SSH password is presented and can be used to access the container.

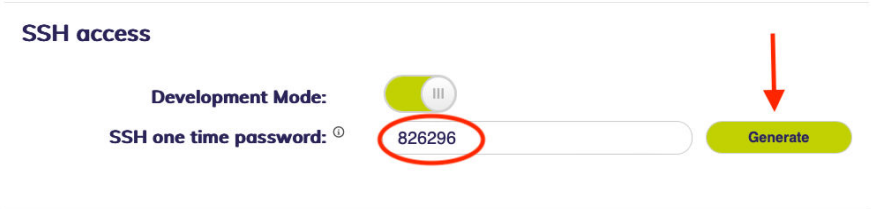

Figure 15: SSH one time password generated

Note: It is recommended to keep the SSH access disable to avoid unauthorized attempts of access. Remember, the certificate generation process is a security measure and need to be kept as secure as possible.

2.5 Node

As a component of the *Perinet* Containers Portfolio, the PKI4mfg container can be seamlessly integrated into the application and collaborate with other components. Being part of a production chain it can be used to generate the OEM or production certificate for new devices or containers.

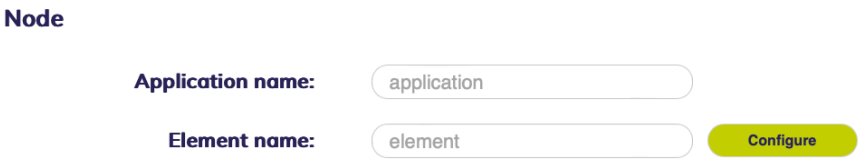

Figure 16: Node config

2.6 Security

As a key element of the Perinet Security solutions, the PKI4mfg container facilitates the configuration of security settings via the webUI, as shown in figure 17.

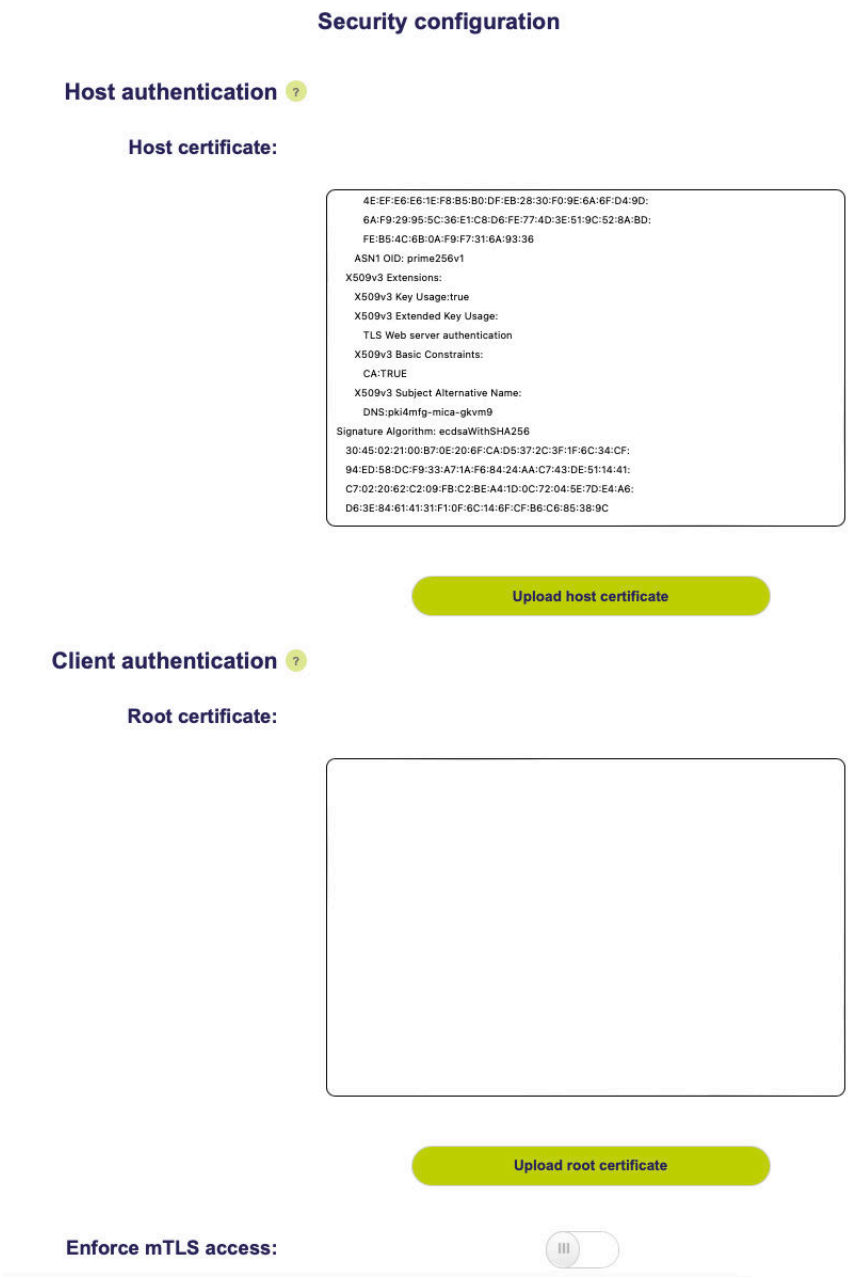

Figure 17: Security Session

3 Further Documentation

3.1 periCORE

Document Name	Description
periCORE Product Summary [5]	A product features summary documentation for the product *periCORE*.
periCORE Datasheet [1]	A detailed reference documentation of the product *periCORE*.
periCORE Development Kit Product Summary [2]	A product features summary documentation for the product *periCORE Development Kit*.
periCORE Development Kit Setup Application Note [3]	A setup guide for the product *periCORE Development Kit*. The starting point when you are new to the product which describes how to quickly set up a development environment for firmware development for a periCORE based product.
periCORE Development Kit User Guide [4]	A guide and reference documentation for the product *periCORE Development Kit*.

3.2 periMICA

Document Name	Description
periMICA Product Summary [8]	A product features summary documentation for the *periMICA*.
periMICA Quick Start Guide [9]	A setup guide for the product *periMICA*. The starting point when you are new to the product.
periMICA User Guide [10]	A detailed description and reference documentation of the product *periMICA*.
PKI2go Container User Guide [11]	A detailed description of the public key infrastructure (PKI) periMICA container 'PKI2go'.
Security Certificates Installation Guide [14]	A guide on how to install prerequisites certificates on various platforms (MAC, Windows and Linux).
periMICA Debian Container User Guide [6]	A detailed description of the base container of a periMICA lxc-based container. It's the starting point for container development.
periMICA Product ReBranding Application Note [7]	A detailed description for development to rebrand the product periMICA to a dedicated customer corporate design.

3.3 Perinet Security

Document Name	Description
PKI2go Container User Guide [11]	A detailed description of the public key infrastructure (PKI) periMICA container 'PKI2go'.
PKI4mfg Container User Guide [12]	The (PKI) periMICA container 'PKI4mfg' User Guide.
Production Public Key Infrastructure Establishment [13]	Production Public Key Infrastructure Establishment.
Security Certificates Installation Guide [14]	A guide on how to install prerequisites certificates on various platforms (MAC, Windows and Linux).

4 Contact & Support

For customer support, please call us at **+49 30 863 206 701** or send an e-mail to *support@perinet.io*.

For complete contact information visit us at www.perinet.io

A List of Figures

B Glossary

API Application Programming Interface. 4

CA Certification Authority, a trusted entity which is represented by a certificate that is used to verify the signature on a certificate issued by that authority (trust anchor). 4, 6–8

CSR Certificate Sign Request. 8

OEM Original Equipment Manufacturer is generally perceived as a company that produces parts and equipment that may be marketed by another manufacturer. 11

OTP One-Time Programmable memory. 10

PKI Public Key Infrastructure. 4, 13, 14

PKI4mfg PKI4mfg is a security service container to manage security to manufacture. 1, 4, 11

SSH Secure Shell Protocol. 10

UI User Interface. 4

C References

[1] Perinet GmbH. periCORE Datasheet. PRN.100.375. https://docs.perinet.io/PRN100375-periCOREDatasheet.pdf.

[2] Perinet GmbH. periCORE Development Kit Product Summary. PRN.100.546. https://docs.perinet.io/PRN100546-periCOREDevelopmentKitProductSummary.pdf.

[3] Perinet GmbH. periCORE Development Kit Setup Application Note. PRN.100.376. https://docs.perinet.io/PRN100376-periCOREDevelopmentKitSetupApplicationNote.pdf.

[4] Perinet GmbH. periCORE Development Kit User Guide. PRN.100.378. https://docs.perinet.io/PRN100378-periCOREDevelopmentKitUserGuide.pdf.

[5] Perinet GmbH. periCORE Product Summary. PRN.100.301. https://docs.perinet.io/PRN100301-periCOREProductSummary.pdf.

[6] Perinet GmbH. periMICA Debian Container User Guide. PRN.100.462. https://docs.perinet.io/PRN100462-DebianContainerUserGuide.pdf.

[7] Perinet GmbH. *periMICA Product ReBranding Application Note*. PRN.100.583. https://docs.perinet.io/.

[8] Perinet GmbH. periMICA Product Summary. PRN.100.389. https://docs.perinet.io/PRN100389-periMICAProductSummary.pdf.

[9] Perinet GmbH. periMICA Quick Start Guide. PRN.100.391. https://docs.perinet.io/PRN100391-periMICAQuickStartGuide.pdf.

[10] Perinet GmbH. periMICA User Guide. PRN.100.392. https://docs.perinet.io/PRN100392-periMICAUserGuide.pdf.

[11] Perinet GmbH. PKI2go Container User Guide. PRN.100.465. https://docs.perinet.io/PRN100465-PKI2goContainerUserGuide.pdf.

[12] Perinet GmbH. PKI4mfg Container User Guide. PRN.100.809. https://docs.perinet.io/PRN100809-PKI4mfgContainerUserGuide.pdf.

[13] Perinet GmbH. Production Public Key Infrastructure Establishment. PRN.100.811. https://docs.perinet.io/PRN100811-ProductionPublicKeyInfrastructureEstablishment.pdf.

[14] Perinet GmbH. Security Certificates Installation Guide. PRN.100.447. https://docs.perinet.io/PRN100447-SecurityCertificatesInstallationGuide.pdf.

[15] Yubico. *Yubico | YubiKey Strong Two-Factor Authentication*. URL: https://www.yubico.com/products.

D Revision History

Revision	Date	Author(s)	Description
1	2025-01-28	dshe	Initial Release
2	today	dshe	Add feature: API/WebUI Create Batch CA