PKI2go

periMICA Container

User Guide

Abstract

This guide describes the usage of the PKI2go periMICA Container which provides a PKI management with a user-friendly interface.

Doc-No.: PRN.100.465 rev: 2

2023-08-03

Document Information

Title	PKI2go
Subtitle	periMICA Container
Type	User Guide
Status	Release
Version	2
Date	2023-08-03
Disclosure Restriction	

Contents

1 Introduction

The PKI2go is Perinet's portable Public Key Infrastructure PKI patent-pending security solution for enabling highly secured communication between all entities (services and users) of an IoT application.

PKI2go works locally, is independent of your network setup and is easy to use. The container provides the possibility to create your own application Certificate Authority (***CA***), by creating and signing root, host and client certificates:

- ***root certificate***: certificate that identifies the root CA (*Certificate Authority*) trusted by a host (periNODE or periMICA container) when mTLS (mutual TLS) is enabled
- ***host certificate***: a unique certificate used by the server host (periNODE or periMICA container) to authenticate itself when communicating to a client (e.g. web browser client). It holds the host name and, for consistency purposes, it should be issued by the same root CA. This certificate proves the originality of a device.
- ***client certificate***: certificate used by a client (periNODE, periMICA container, web browser client) to authenticate itself when communicating to a server (e.g. MQTT broker).

Furthermore, users can register with specific user roles and corresponding client certificates and administrators can use this mechanism to grant different levels of authorization to specific users.

mTLS

When every local network participant has successfully authenticated itself, a mutual TLS connection can be established, based on the local PKI. Each network participant is authorized to do the operations dictated by the capabilities of its client certificate.

For further information on security concepts, please refer to https://docs.perinet.io.

2 Access PKI2go and Create Root CA

The first access to the PKI2go is open to users that can access periMICA with their password. The PKI2go container Web UI can be reached by clicking on the PKI2go icon from the periMICA home page (Figure 1).

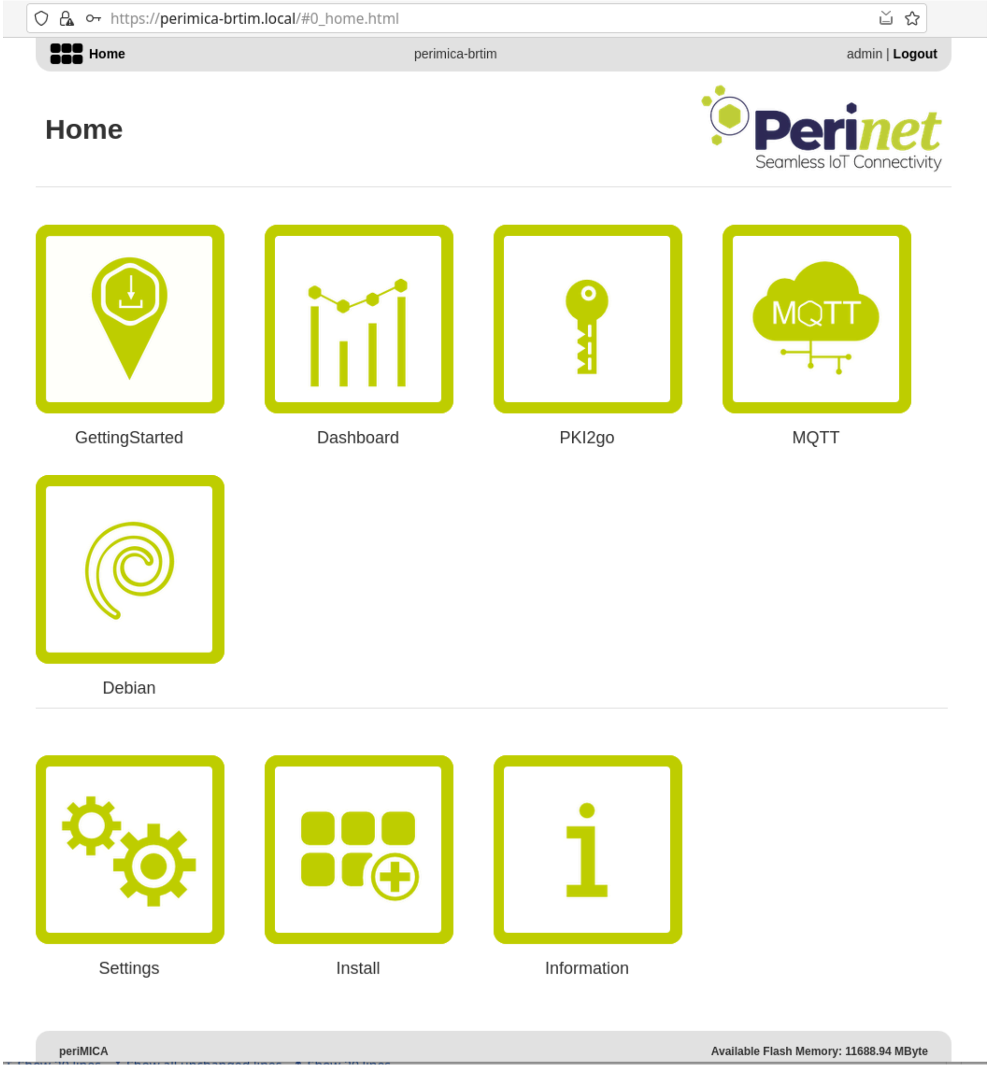
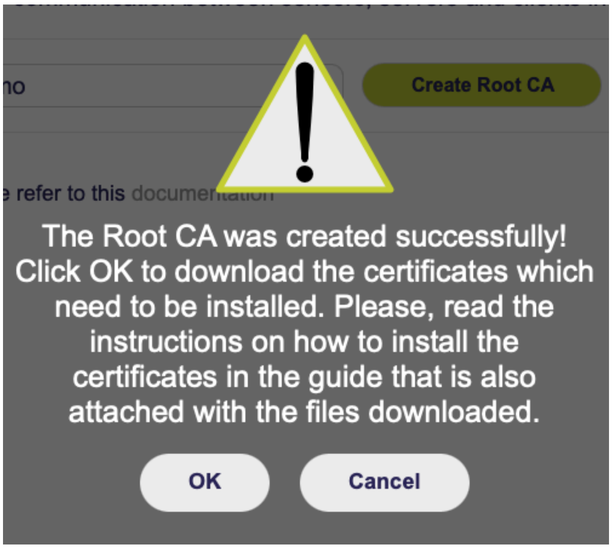


Figure 1: periMICA Home page

On the first setup of the PKI2go container, the Root CA has to be created by inserting the name of the ***CA*** and by clicking on the ***Create Root CA*** button. After that, a confirmation dialog will be prompted, which has to be accepted by clicking ***OK*** (Figure 2).



The Root CA was created successfully! Click OK to download the certificates which need to be installed. Please, read the instructions on how to install the certificates in the guide that is also attached with the files downloaded.

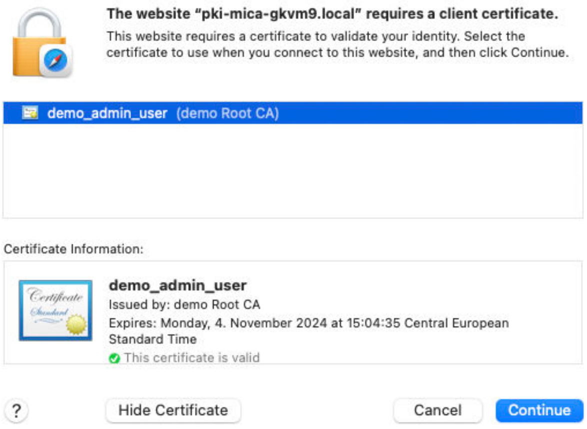
Figure 2: Confirmation dialog upon Root CA creation

A zip file (***PKI2go.zip***) will then be downloaded containing the root certificate, a client certificate (***application_admin_user.p12***), as well as a pdf document, the ***Security Certificates Installation Guide*** [18].

The client certificate must be installed into the web browser, as the PKI2go container will automatically setup mTLS (mutual TLS), including all certificates for its own web services after the Root CA was created. The password needed to include the client certificate is by default (***admin_pki_container***).

Note: *The name of the* ***CA*** *will also be the* ***application name*** *configured automatically to periNODE devices or periMICA containers that are added to the PKI2go* ***CA****.*

With the client certificates imported, the PKI2go container Web UI can be accessed again. The browser will then prompt a dialog requesting the selection of the client certificate to be included (Figure 3).



The website "pki-mica-gkvm9.local" requires a client certificate.

This website requires a certificate to validate your identity. Select the certificate to use when you connect to this website, and then click Continue.

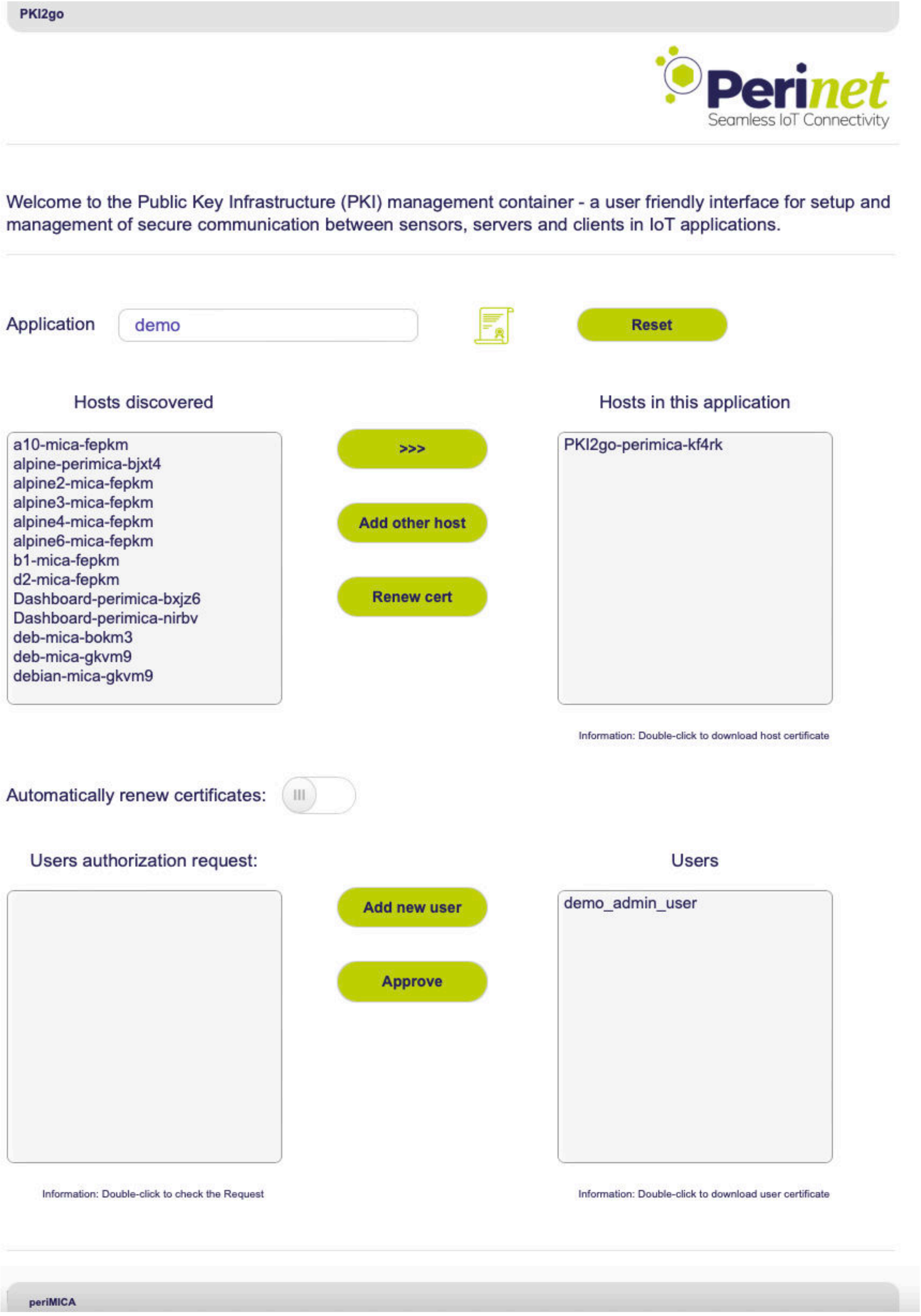
demo_admin_user (demo Root CA)

Certificate Information:

demo_admin_user
Issued by: demo Root CA
Expires: Monday, 4. November 2024 at 15:04:35 Central European Standard Time
This certificate is valid

Figure 3: Example: Browser request client certificate

After confirming, the PKI2go container Web UI should show up like in Figure 4:



Welcome to the Public Key Infrastructure (PKI) management container - a user friendly interface for setup and management of secure communication between sensors, servers and clients in IoT applications.

Application: demo

Hosts discovered

a10-mica-fepkm
alpine-perimica-bjxt4
alpine2-mica-fepkm
alpine3-mica-fepkm
alpine4-mica-fepkm
alpine6-mica-fepkm
b1-mica-fepkm
d2-mica-fepkm
Dashboard-perimica-bxjz6
Dashboard-perimica-nirbv
deb-mica-bokm3
deb-mica-gkvm9
debian-mica-gkvm9

Hosts in this application

PKI2go-perimica-kf4rk

Information: Double-click to download host certificate

Automatically renew certificates: ○

Users authorization request:

Information: Double-click to check the Request

Users

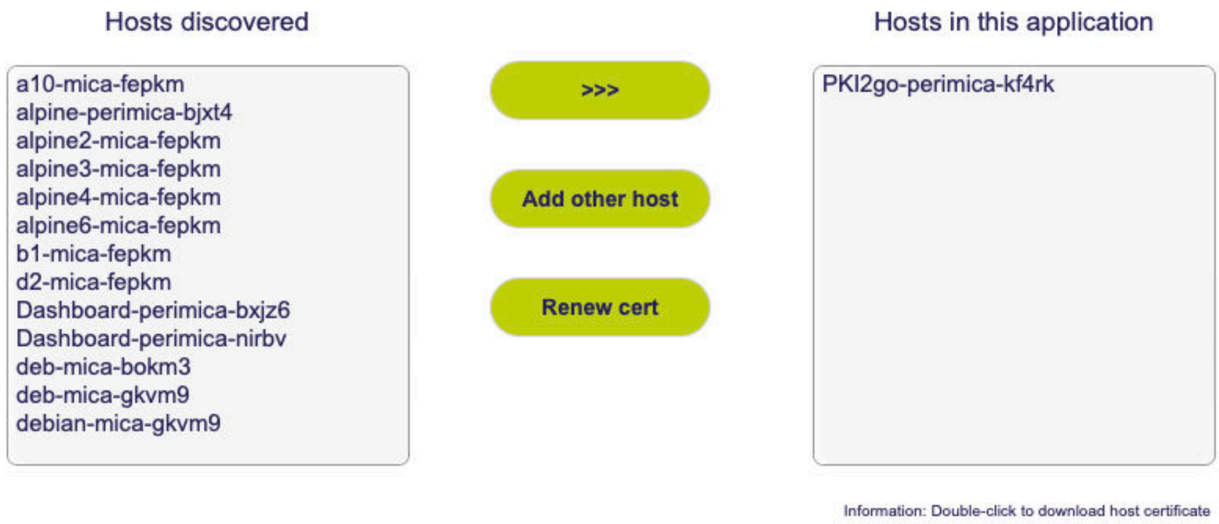
demo_admin_user

Information: Double-click to download user certificate

Figure 4: PKI2go container with a demo Root CA setup

3 Automatic Host Discovery

The PKI2go container is capable of discovering all devices that publish under the ***service_-type*** `_https._tcp`. Discovered devices will be displayed in the ***Hosts discovered*** selection box (Figure 5).


Hosts discovered
>>>
Add other host
Renew cert
Hosts in this application
Information: Double-click to download host certificate

a10-mica-fepkm
alpine-perimica-bjxt4
alpine2-mica-fepkm
alpine3-mica-fepkm
alpine4-mica-fepkm
alpine6-mica-fepkm
b1-mica-fepkm
d2-mica-fepkm
Dashboard-perimica-bxjz6
Dashboard-perimica-nirbv
deb-mica-bokm3
deb-mica-gkvm9
debian-mica-gkvm9

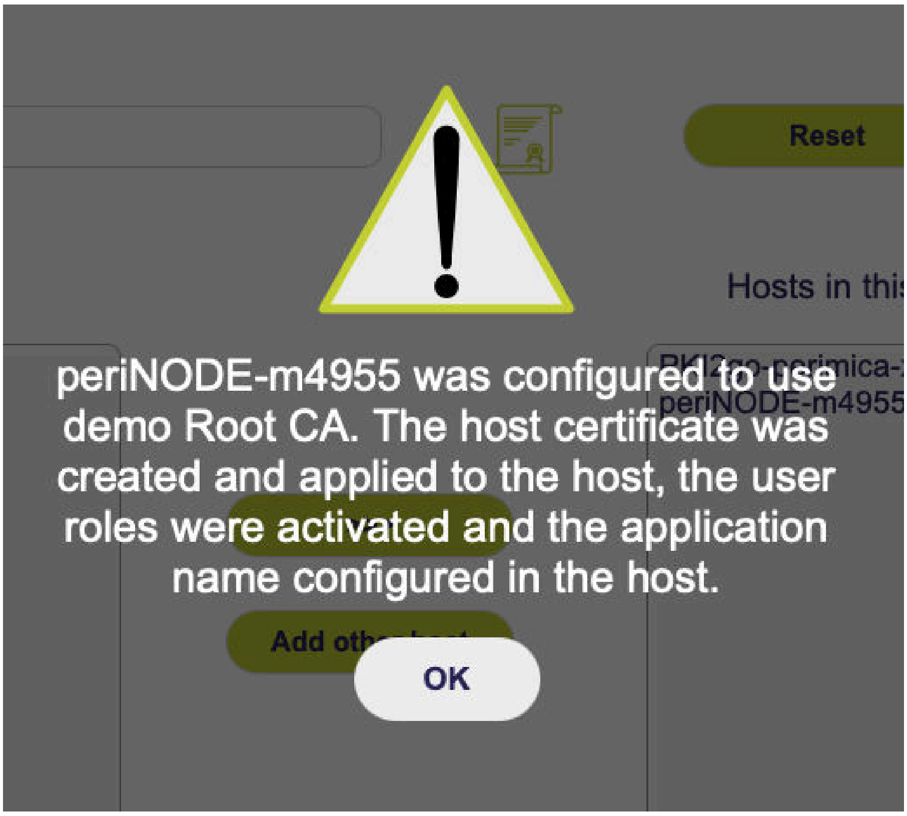
PKI2go-perimica-kf4rk

Figure 5: Hosts discovered and hosts in this application

4 Add Discovered Hosts to the Application

From the discovered hosts list, select the desired host to add to your application. If the host is one of the Perinet Smart Components or periMICA containers, the secure configuration will be done automatically from PKI2go, by pressing the **> > >** button.

The security certificates will then be generated and sent via REST http interface of the corresponding device. Also, via http requests, the application name will be set, as well as mTLS, which means that the device or container can then also only be accessed with the previously imported client certificates. If the configuration was done successfully, a pop-up like in Figure 6 will be displayed:



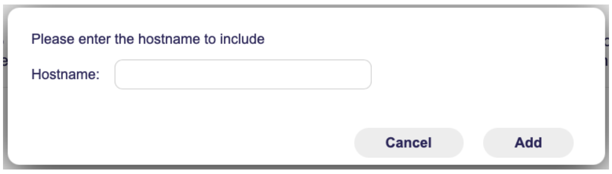
periNODE-m4955 was configured to use demo Root CA. The host certificate was created and applied to the host, the user roles were activated and the application name configured in the host.

Figure 6: Host successfully added to application

5 Add Other Hosts to the Application

If the desired host is not a Perinet Smart Component or periMICA container, it is still possible to generate a dedicated certificate for this host, signed by ***application Root CA***.

To generate the host certificate, click on ***Add other host*** button and type the host name in the displayed dialog (Figure 7):

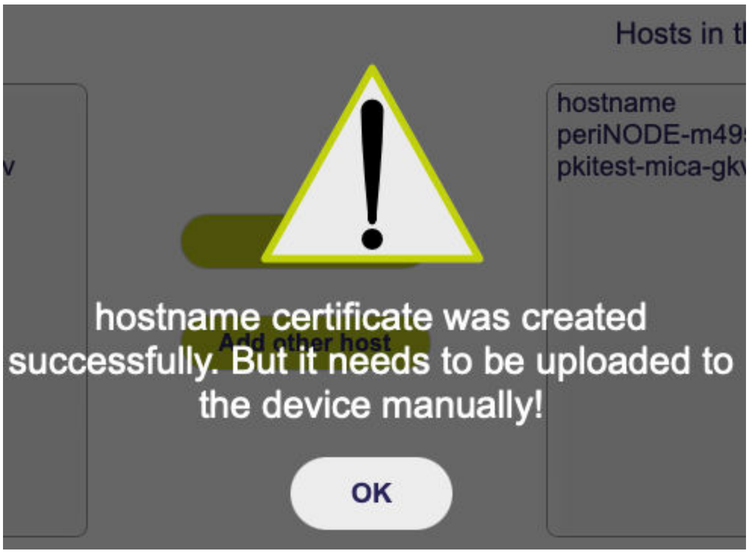


Please enter the hostname to include

Hostname:

Figure 7: Add other host dialog

The host certificate will be downloaded automatically and needs to be manually uploaded to the host (Figure 8).



hostname certificate was created successfully. But it needs to be uploaded to the device manually!

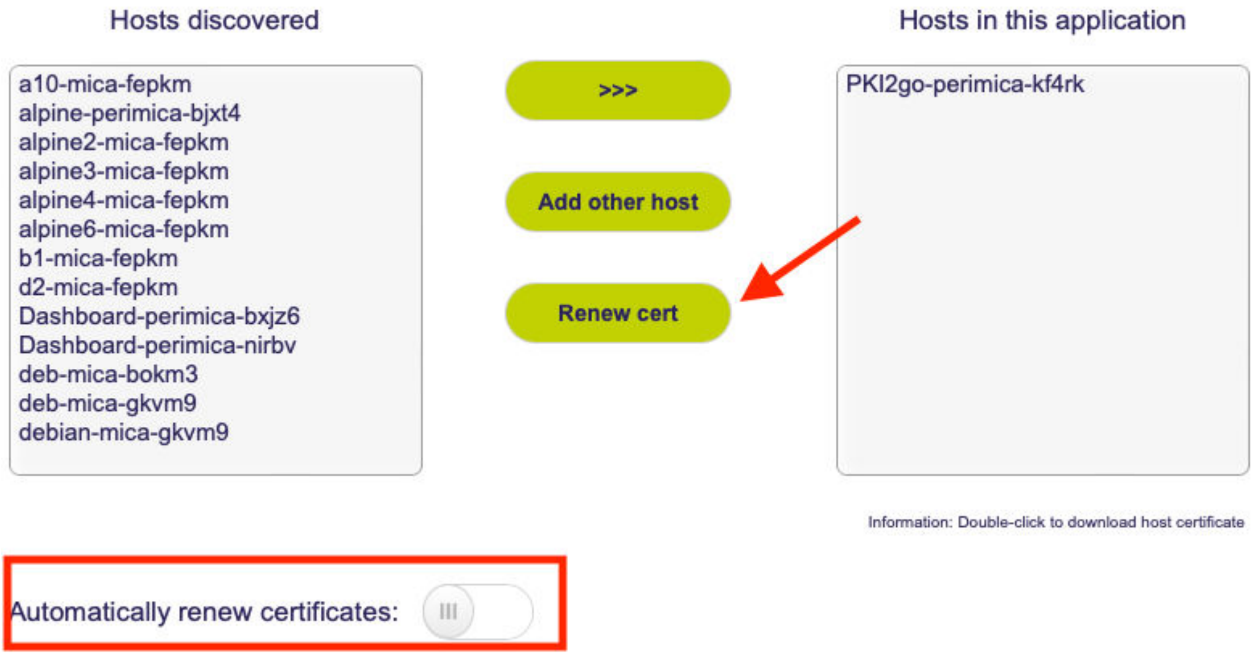
Figure 8: Other host successfully added to application

Note: *Host certificates can also be downloaded afterwards by double-clicking on the desired host present in the* ***Hosts in this application*** *list.*

6 Renew Certificate and Automatically renew certificates

The certificates have a certain validity time. The clients accessing the application will receive security warnings if the certificates has an expired datetime. The intent is keeping the certificates always up-to-dated to avoid this kind of warnings. In order to improve security of the systems some manufactors and/or platforms are going accept only short validity time for security certiticates. It means they need to be renewed after a short period of time and it can make the task to keep the certitificates valid a bit more hard, specially when the number of hosts to manage increases.

With the *PKI2go* the user can do the renew of the certificates manually through the button ***Renew cert***. For this, it just need to select the host that needs to be renewed and press the button ***Renew cert***.



Hosts discovered

a10-mica-fepkm
alpine-perimica-bjxt4
alpine2-mica-fepkm
alpine3-mica-fepkm
alpine4-mica-fepkm
alpine6-mica-fepkm
b1-mica-fepkm
d2-mica-fepkm
Dashboard-perimica-bxjz6
Dashboard-perimica-nirbv
deb-mica-bokm3
deb-mica-gkvm9
debian-mica-gkvm9

Hosts in this application

PKI2go-perimica-kf4rk

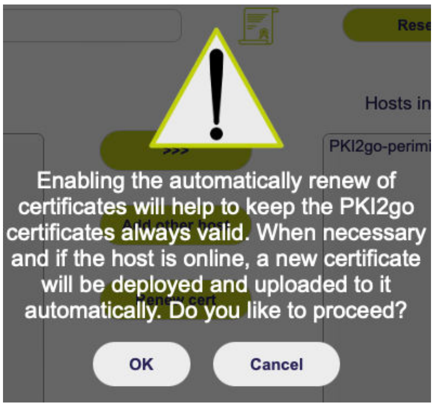
Information: Double-click to download host certificate

Automatically renew certificates:

Figure 9: Renew certificate options

The *PKI2go* is also able to check the validity and generate automatically new certificates to the hosts that have already been added into the application. *30 days* before the date expiration, a process running in the background will check the validity and generate new certificates to the hosts. The new certificates will also be automatically sent to the hosts using the *security API*.

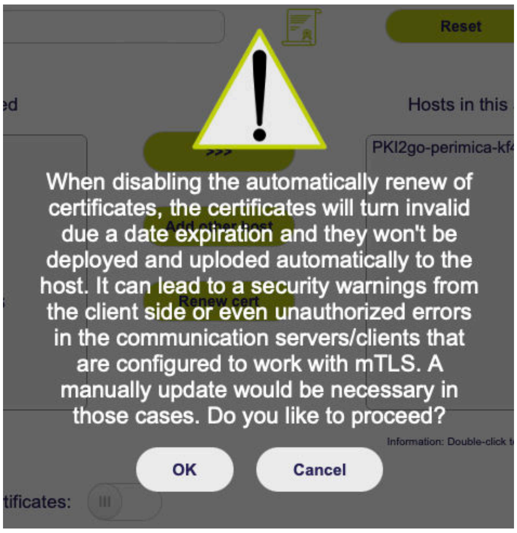
The switch ***Automatically renew certificates*** bring the option in the PKI2go webUI. Click on the switch and confirm the message that will pop-up like in 10 clicking on ***OK***.



Enabling the automatically renew of certificates will help to keep the PKI2go certificates always valid. When necessary and if the host is online, a new certificate will be deployed and uploaded to it automatically. Do you like to proceed?

Figure 10: Enabling the Automatically renew certificates message

In case of disabling the ***Automatically renew certificates***, a message like presented in 11 will be shown, click on ***Ok*** to confirm.



When disabling the automatically renew of certificates, the certificates will turn invalid due a date expiration and they won't be deployed and uploded automatically to the host. It can lead to a security warnings from the client side or even unauthorized errors in the communication servers/clients that are configured to work with mTLS. A manually update would be necessary in those cases. Do you like to proceed?

Figure 11: Disabling the Automatically renew certificates message

7 Download the Application Root CA Certificate

In case the root certificate of the application ***CA*** was lost somehow, it can be downloaded again by clicking on the certificate icon:

Figure 12: Certificate icon

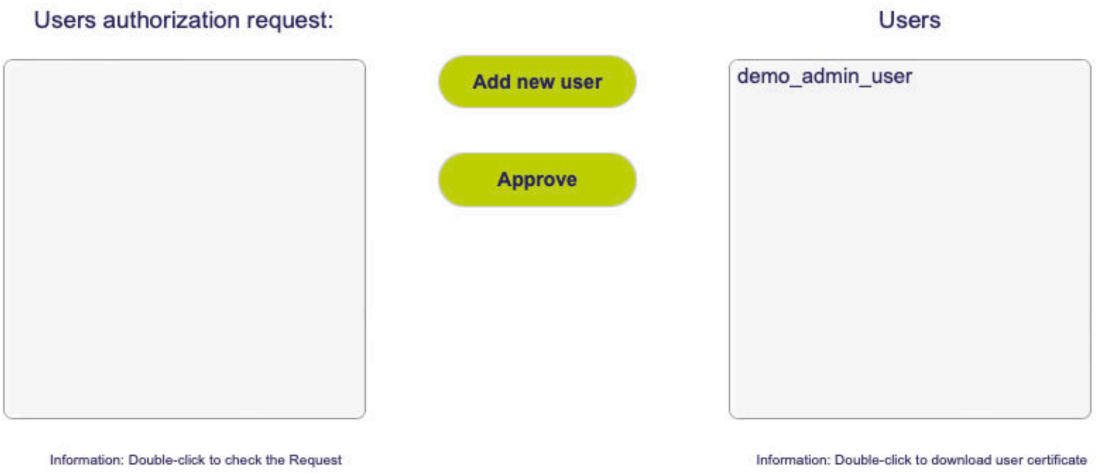
***Note:** Like mentioned above, the installation of the Root CA certificate in user systems is strongly recommended, in order to avoid security warnings during the usage. For a more detailed explanation on how to install certificates in different operating systems and browsers, please read our **Security Certificates Installation Guide** [18].*

8 Users & User Roles

In order to have access control through client certificates, periNODE devices and periMICA containers currently support the following user roles:

- ***User***: Read-only access.
- ***Super***: Permits only periNODE or specific container configurations. Firmware update and security settings are not possible.
- ***Admin***: Permits all operations, including firmware update, security settings and periNODE/container configurations.

The section of *Users* on the PKI2go web interface is shown below:



Users authorization request:

Users

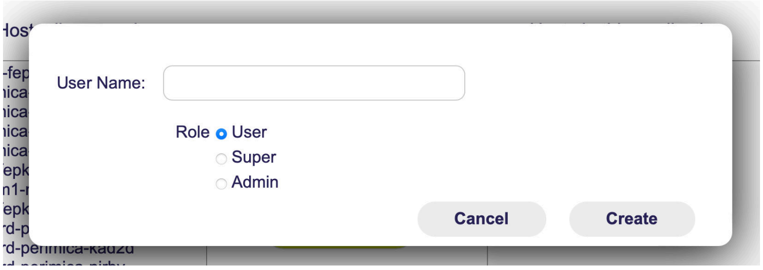
demo_admin_user

Information: Double-click to check the Request

Information: Double-click to download user certificate

Figure 13: User section in PKI2go interface

The PKI2go container comes by default with an initial user called ***application_admin_user***. To create a new user, click on the ***Add new user*** button. In the dialog displayed (Figure 14), type the user name and select the desired capabilities (role) to be applied to the new user.



User Name:

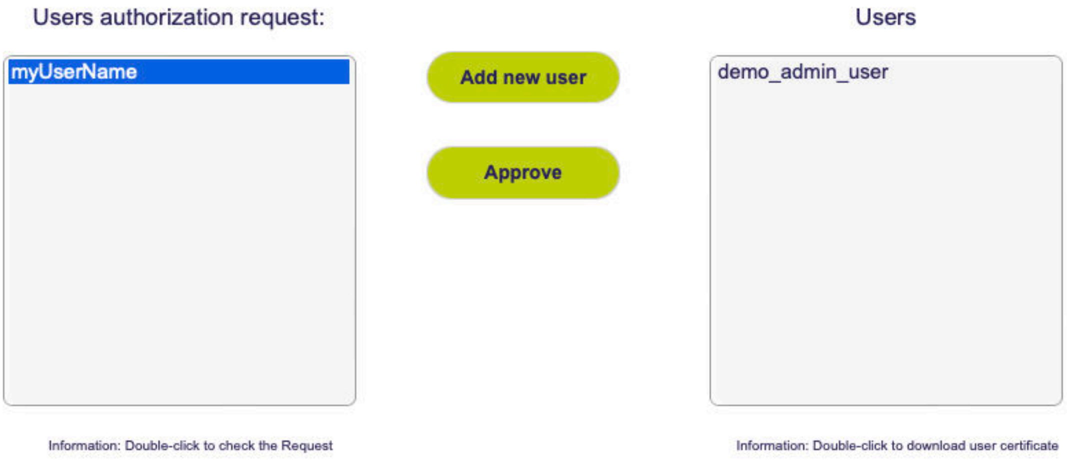
Role ● User ○ Super ○ Admin

Figure 14: Add new user

After this step, the client certificates will be downloaded automatically. The password to access the bundle *.p12* defined by default is "**password**" for all users created from this button. The admin user is responsible to transfer the certificate to the new user added.

Warning: *Avoid attaching the client certificate to an e-mail which is not properly protected, don't send it through chatting tools, neither store it in a public folder in the company network, ensure that it is protected during the shipping. With this certificate, the client or anyone else who has this certificate installed could access the components and in case of* ***admin*** *users, the access to PKI2go would be compromised as well.*

Other way to add an user into the application is approving their requests. The users can request certificate for the *application CA* from the form present in the *Unauthorized Page* as described in section 10. When a new user submit the request, it will be displayed in the box *User authorization request* (see figure 15).



myUserName

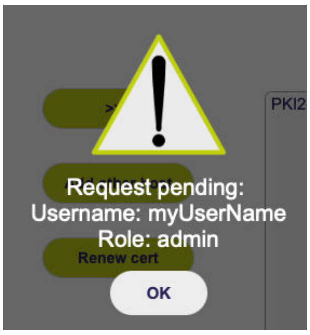
demo_admin_user

Information: Double-click to check the Request

Information: Double-click to download user certificate

Figure 15: New user request

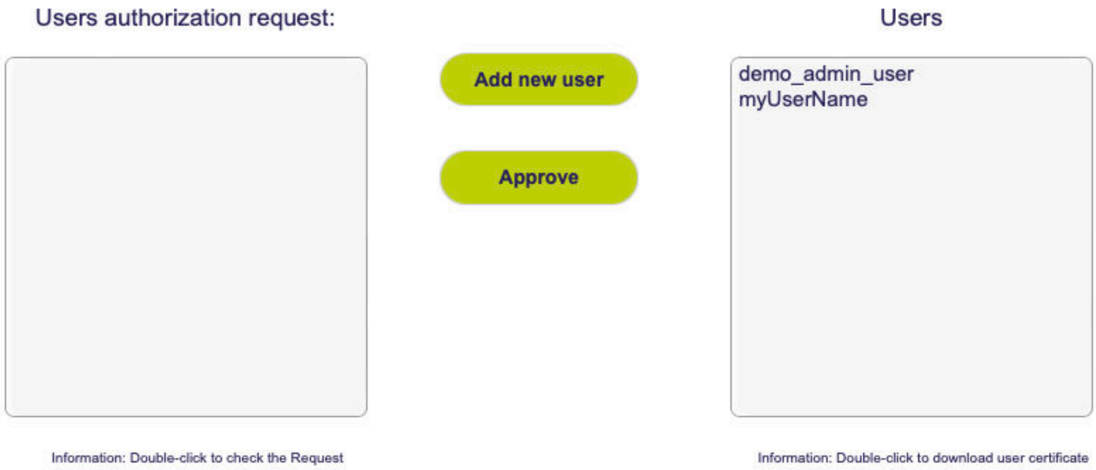
An *admin* user can double-click on the user name and read the request information (see figure 16), regarding the role the user is requering and approve when it is accordingly. In this case the certificate will be sent automatically to the requester user, see 10 for more details.



Request pending:
Username: myUserName
Role: admin

Figure 16: User request information

To approve the request the admin should click on the user name in the selection box and click on the button *Approve*. The user will receive the client certificate automatically. The requests remained are cleaned up *once a day*. After approved the new user can be located in the box *Users* as shown in the figure 17.


Users authorization request:
Add new user
Approve
Users
Information: Double-click to check the Request
Information: Double-click to download user certificate

demo_admin_user
myUserName

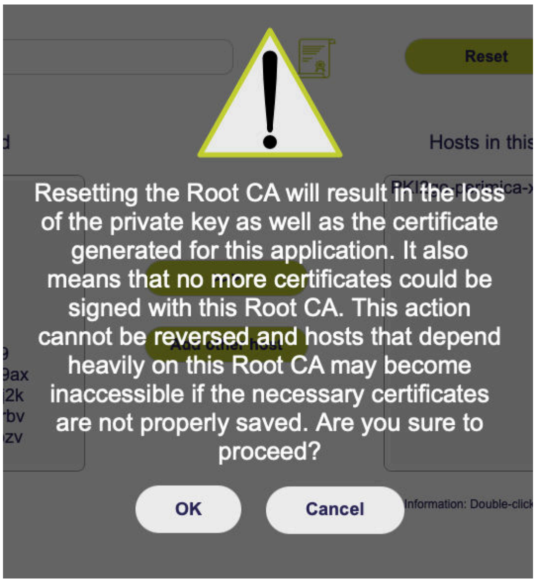
Figure 17: New user added

9 Reset

By resetting the PKI2go configuration, the initial ***application Root CA*** is erased and all host certificates and user certificates will be removed from the container.

Warning: *Make sure that this is the correct intent! Save all certificates needed to access the periNODEs and containers beforehand. Also note that even the PKI2go container is protected by a self-generated security certificate. If a reset of the Root CA is done, the PKI2go will be open to any user with access to periMICA.*

By clicking on the ***Reset*** button, a confirmation message (Figure 18) will be displayed:



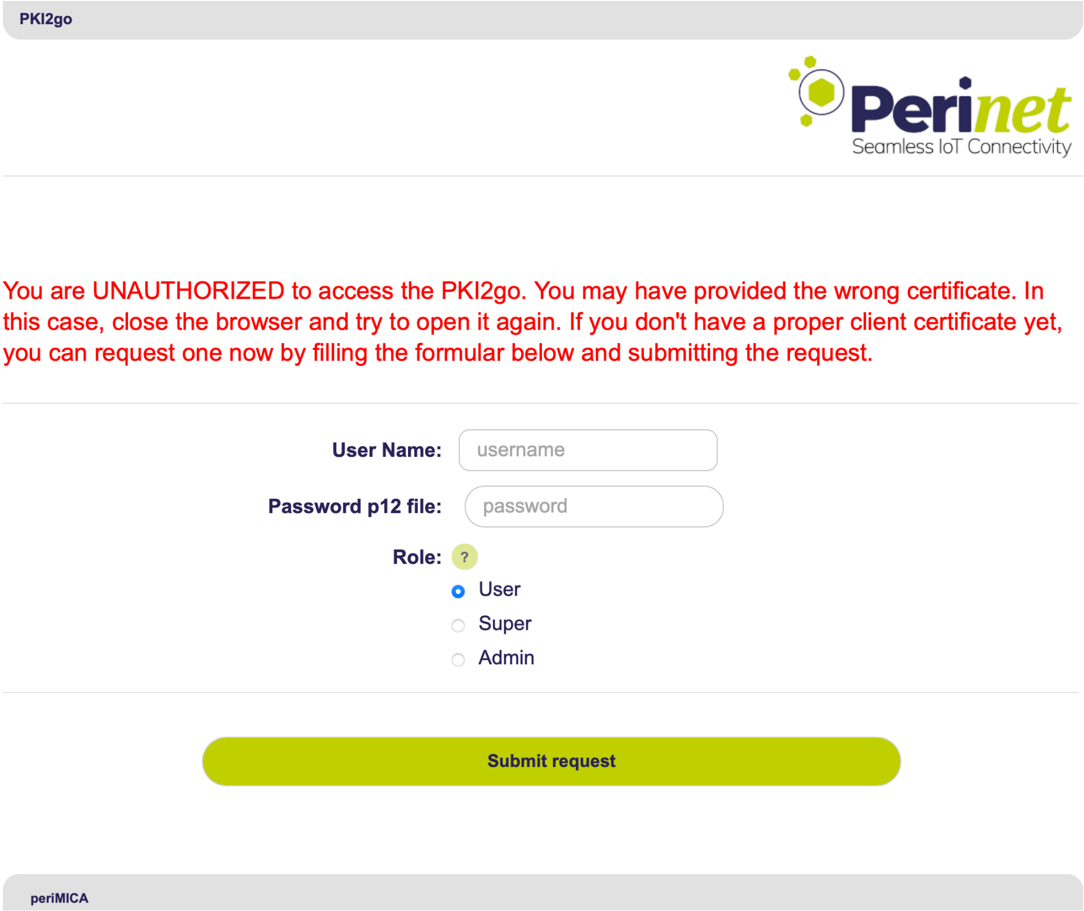
Resetting the Root CA will result in the loss of the private key as well as the certificate generated for this application. It also means that no more certificates could be signed with this Root CA. This action cannot be reversed and hosts that depend heavily on this Root CA may become inaccessible if the necessary certificates are not properly saved. Are you sure to proceed?

Figure 18: Reset Root CA confirmation

If a reset was done, it is possible to setup another ***application Root CA***.

10 Unauthorized Page

Users who don't have certificate to access the PKI2go container will be forwarded to an *unauthorized page* like presented in the figura 19.



You are UNAUTHORIZED to access the PKI2go. You may have provided the wrong certificate. In this case, close the browser and try to open it again. If you don't have a proper client certificate yet, you can request one now by filling the formular below and submitting the request.

User Name: username

Password p12 file: password

Role: ?

- ● User
- ○ Super
- ○ Admin

Figure 19: Unauthorized Page

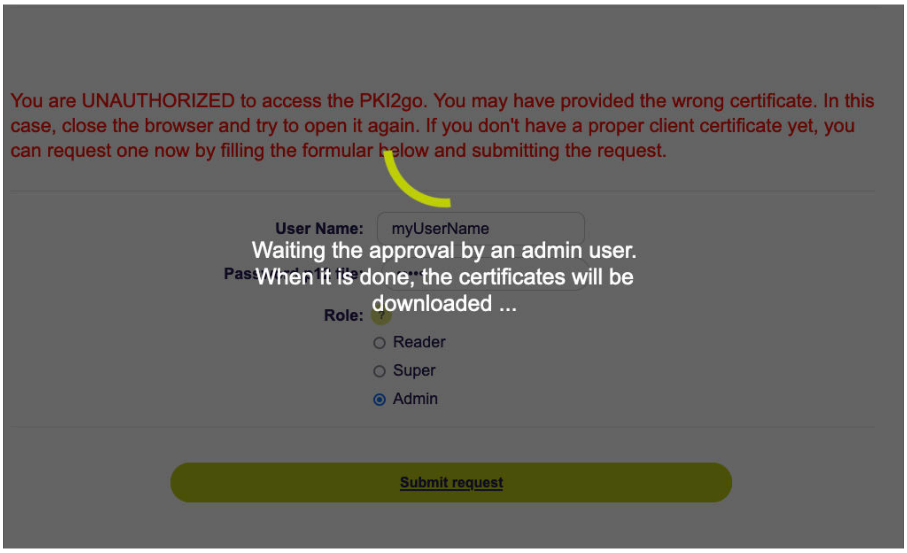
On the top the user can read the message which explains what probably happens:

- The user didn't provide any certificate which is necessary when trying to access a PKI2go that has been already configured for an application.
- The user provides a certificate which was not accepted, which means it has been signed by an unkown CA and not by the Application CA as expected.

Through the *unauthorized page*, it is possible to request a certificate signed by the CA. For that the user should fill the form with the user name, a password to be used to protect the .p12 file when it is created, as well as the role that should be applied in the certificate.

Note: The password should be used when the user will install the certificate in the system.

After the user submit the request, pressing the button *Submit Request*, the request will be displayed for an *admin* user who is the responsible to analyse the request and approve it or not. The page will be temporarilly locked as shown in figure 20).



You are UNAUTHORIZED to access the PKI2go. You may have provided the wrong certificate. In this case, close the browser and try to open it again. If you don't have a proper client certificate yet, you can request one now by filling the formular below and submitting the request.

User Name: myUserName

Password p12 file:

Role:

○ Reader

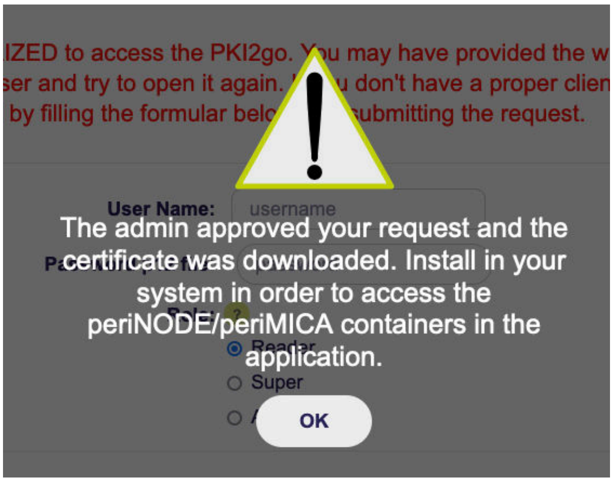
○ Super

● Admin

Waiting the approval by an admin user. When it is done, the certificates will be downloaded ...

Figure 20: Waiting approval from an admin user

As soon the *admin* approve the request, a zip file that contains the certificate will be downloaded in the user machine and the user can follow with the certificate installation. The confirmation message is shown below:



IZED to access the PKI2go. Y u may have provided the w
ser and try to open it again. u don't have a proper clien
by filling the formular belo ubmitting the request.

The admin approved your request and the certificate was downloaded. Install in your system in order to access the periNODE/periMICA containers in the application.

Figure 21: Confirmation message when the request has been approved

11 Command Line Examples Using Client Certificates

For automation purposes, it might be desirable to use the REST API of the periNODE devices or periMICA containers with mTLS enabled, as shown below using ***curl, openssl and httpie***

- Usually, for easier usage, the client certificates are in one single p12 file, but some tools require separate key and crt files, which can be extracted from the p12 file:

```
openssl pkcs12 -in client.p12 -nocerts -out client.key
openssl pkcs12 -in client.p12 -clcerts -nokeys -out client.pem
```

- Simple http GET to /info using ***curl***:

```
http GET https://perinode-abcde.local/info --cert client.pem
--cert-key client.key --CAfile perinet-root-ecc-ca.crt
```

- In newer versions of ***curl***, the p12 file can be passed directly:

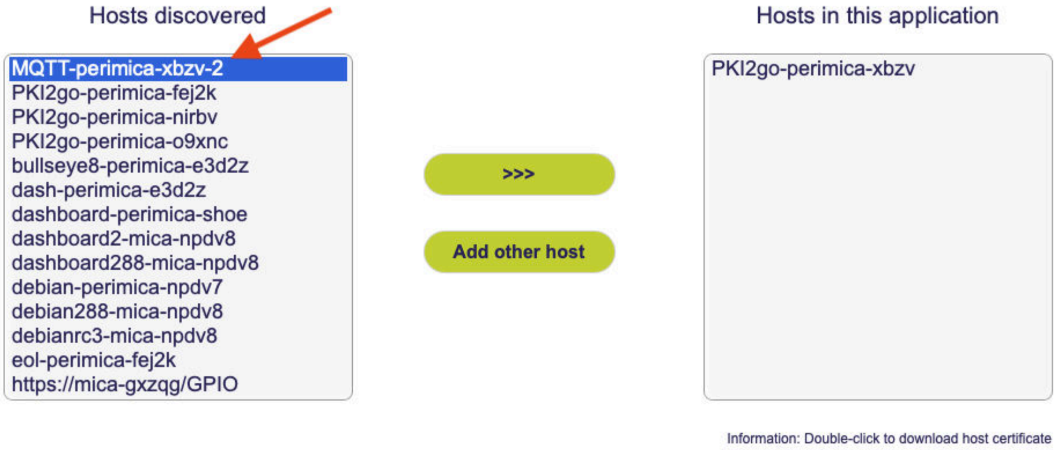
```
curl -6 -g --interface eth0 https://perinode-abcde.local/info --cert-type
P12 --cert client.p12:password
```

- Using ***httpie*** client:

```
http --cert=client.crt --cert-key=client.key
https://perinode-abcde.local/info --verify=root-ca.crt
```

12 Known Issues

- Browsers can cache SSL certificates in order to speed up the access. But caching can cause issues, because a protected server will refuse the connection if the browser sent the incorrect certificate. In that case, refreshing the web page might help. If the problem still occurs, make sure to have the correct client certificates imported and restart the browser.
- Strange host names that look duplicated, with suffixes like “-2”, “-3", appear amongst the ***Hosts discovered*** by PKI2go (like in Figure 22). This behaviour is rare and it happens because of the **avahi-daemon** implementation. The recommended solution is to use the “**Add other host**” button and upload manually the certificate in the host.



Hosts discovered

MQTT-perimica-xbzv-2
PKI2go-perimica-fej2k
PKI2go-perimica-nirbv
PKI2go-perimica-o9xnc
bullseye8-perimica-e3d2z
dash-perimica-e3d2z
dashboard-perimica-shoe
dashboard2-mica-npdv8
dashboard288-mica-npdv8
debian-perimica-npdv7
debian288-mica-npdv8
debianrc3-mica-npdv8
eol-perimica-fej2k
https://mica-gxzqg/GPIO

Hosts in this application

PKI2go-perimica-xbzv

Information: Double-click to download host certificate

Figure 22: PKI2go wrong hostname with suffix

13 Further Documentation

13.1 Starter Kits

Document Name	Description
Starter Kit Plus Product Summary [20]	A product features summary documentation for the *Starter Kit Plus*.
Starter Kit Plus Quick Start Guide [21]	A setup guide for the *Starter Kit Plus* product.
Starter Kit Plus User Guide [23]	A detailed description of the setup *Starter Kit Plus*.
Starter Kit Plus Security Certificates Installation Guide [22]	A small guide on how to install security prerequisites for accessing the various entities of the *Starter Kit Plus* setup.
Starter Kit Product Summary [24]	A product features summary documentation for the available *Starter Kit*s.
Starter Kit Quick Start Guide [25]	A setup guide for the *Starter Kit* products.

13.2 periMICA

Document Name	Description
periMICA Product Summary [9]	A product features summary documentation for the *periMICA*.
periMICA Quick Start Guide [10]	A setup guide for the product *periMICA*. The starting point when you are new to the product.
periMICA User Guide [11]	A detailed description and reference documentation of the product *periMICA*.
PKI2go Container User Guide [17]	A detailed description of the public key infrastructure (PKI) periMICA container 'PKI2go'.
Security Certificates Installation Guide [18]	A guide on how to install prerequisites certificates on various platforms (MAC, Windows and Linux).
periMICA Debian Container User Guide [7]	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 [8]	A detailed description for development to rebrand the product periMICA to a dedicated customer corporate design.

13.3 Smart Components

Document Name	Description
periLINE Product Summary [6]	A product features summary documentation for the product *periLINE*.
periNODE 0-10V Product Summary [12]	A product features summary documentation for the product *periNODE 0-10V*.
periNODE Pt100 Product Summary [14]	A product features summary documentation for the product *periNODE Pt100*.
periNODE GPIO Product Summary [13]	A product features summary documentation for the product *periNODE GPIO*.
periSWITCH 3-port Product Summary [16]	A product features summary documentation for the product *periSWITCH 3-port*.
periSTART Standard Product Summary [15]	A product features summary documentation for the product *periSTART standard*.
Smart Components Datasheet [19]	A detailed reference documentation of the Smart Components products (*periLINE*, *periNODE 0-10V*, *periNODE Pt100*, *periNODE GPIO*, *periSWITCH 3-port*, *periSTART standard*).

13.4 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*.

14 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. 19

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). 3, 4, 17

MQTT Message Queuing Telemetry Transport is a lightweight, publish-subscribe based network protocol that transports messages between devices. 4

mTLS Mutual TLS extends the TLS protocol by requiring clients to pass certificates, allowing to provide authorization mechanisms of Application services. 4, 6, 8, 19

PKI Public Key Infrastructure. 1, 4, 21

PKI2go PKI2go is a patent-pending security service provided by Perinet. 4, 13

REST REpresentational State Transfer, a web API style. 8, 19

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. periLINE Product Summary. PRN.100.386. https://docs.perinet.io/PRN100386-periLINEProductSummary.pdf.

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

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

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

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

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

[12] Perinet GmbH. periNODE 0-10V Product Summary. PRN.100.380. https://docs.perinet.io/PRN100380-periNODE0-10VProductSummary.pdf.

[13] Perinet GmbH. periNODE GPIO Product Summary. PRN.100.382. https://docs.perinet.io/PRN100382-periNODEGPIOProductSummary.pdf.

[14] Perinet GmbH. periNODE Pt100 Product Summary. PRN.100.381. https://docs.perinet.io/PRN100381-periNODEPt100ProductSummary.pdf.

[15] Perinet GmbH. periSTART Standard Product Summary. PRN.100.383. https://docs.perinet.io/PRN100383-periSTARTstandardProductSummary.pdf.

[16] Perinet GmbH. periSWITCH 3-port Product Summary. PRN.100.385. https://docs.perinet.io/PRN100385-periSWITCH3-portProductSummary.pdf.

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

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

[19] Perinet GmbH. Smart Components Datasheet. PRN.100.387. https://docs.perinet.io/PRN100387-SmartComponentsDatasheet.pdf.

[20] Perinet GmbH. Starter Kit Plus Product Summary. PRN.100.568. https://docs.perinet.io/PRN100568-StarterKitPlusProductSummary.pdf.

[21] Perinet GmbH. Starter Kit Plus Quick Start Guide. PRN.100.394. https://docs.perinet.io/PRN100394-StarterKitPlusQuickStartGuide.pdf.

[22] Perinet GmbH. Starter Kit Plus Security Certificates Installation Guide. PRN.100.397. https://docs.perinet.io/PRN100397-StarterKitPlusSecurityCertificatesInstallationGuide.pdf.
[23] Perinet GmbH. Starter Kit Plus User Guide. PRN.100.548. https://docs.perinet.io/PRN100548-StarterKitPlusUserGuide.pdf.
[24] Perinet GmbH. Starter Kit Product Summary. PRN.100.567. https://docs.perinet.io/PRN100567-StarterKitProductSummary.pdf.
[25] Perinet GmbH. Starter Kit Quick Start Guide. PRN.100.569. https://docs.perinet.io/.

D Revision History

Revision	Date	Author(s)	Description
1.0	August 31, 2021	Dilmari Seidel Heuer	Initial release
2	2023-08-03	Dilmari Seidel Heuer	Use application_admin_user client certificate, add unauthorized page, request client certificate and automatically renew certificates