

PKI2go Container

User Guide

August 31, 2021



Contents

1	Introduction	3
2	Access PKI2go and Create Root CA	4
3	Automatic Host Discovery	7
4	Add Discovered Hosts to the Application	7
5	Add Other Hosts to the Application	8
6	Download the Application Root CA Certificate	9
7	Users & User Roles	10
8	Reset	11
9	Command Line Examples Using Client Certificates	12
10	Known Issues	13
11	Contact & Support	14

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).

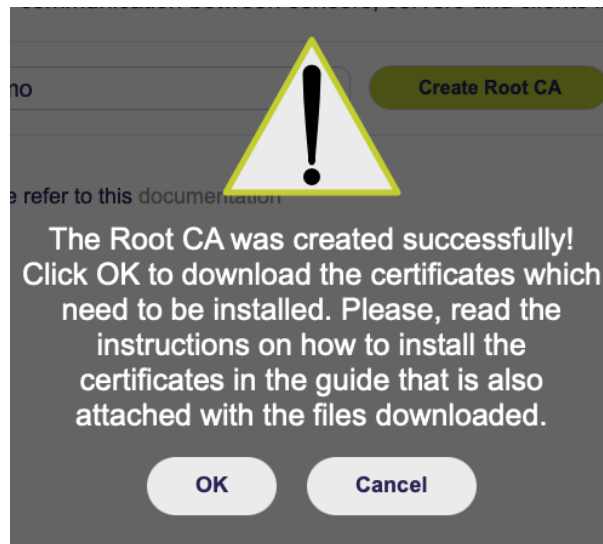


Figure 2: Confirmation dialog upon Root CA creation

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

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 just like the file name (**admin_pki_container**).

Note: *The name of the CA will also be the **application name** configured automatically to peri-NODE 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).

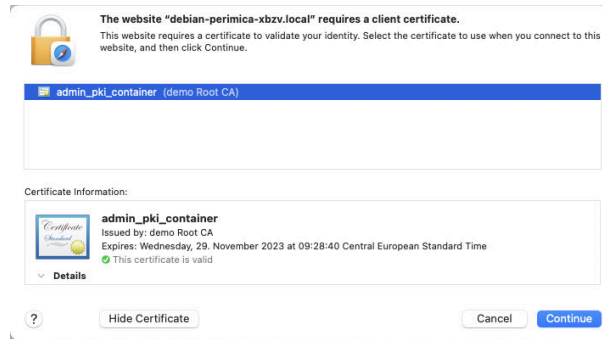


Figure 3: Example: Browser request client certificate

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



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).

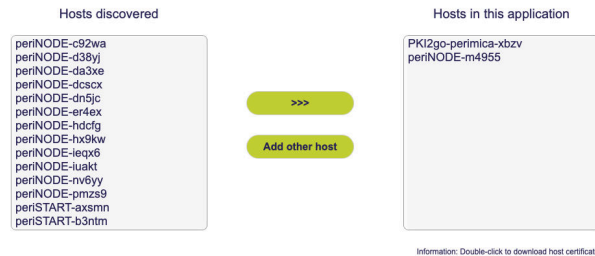


Figure 5: Hosts discovered and hosts in this application

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:

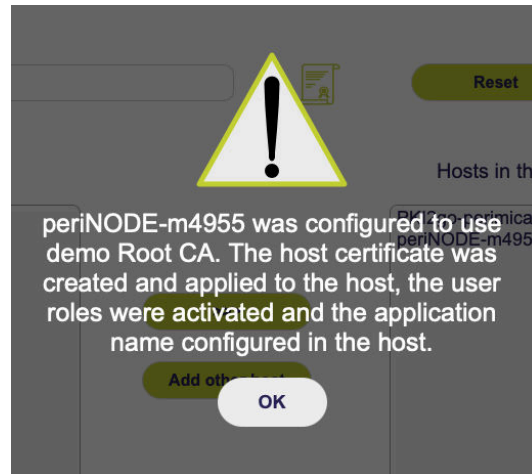


Figure 6: Host successfully added to application

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):

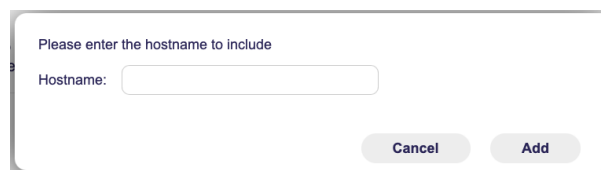


Figure 7: Add other host dialog

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

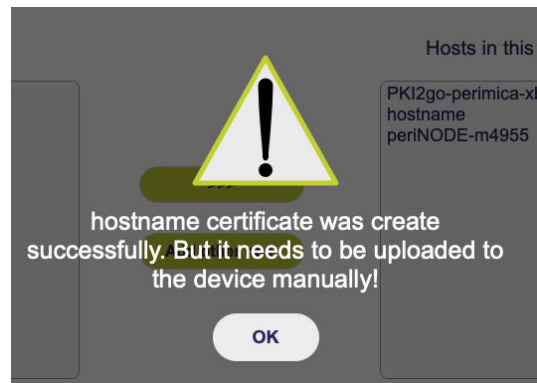


Figure 8: Other host successfully added to application

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

6 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 9: 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** [1].

7 Users & User Roles

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

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

The PKI2go container comes by default with an initial user called **admin_pki_container**. To create a new user, click on the **Add new user** button. In the dialog displayed (Fig. 10), type the user name and select the desired capabilities (role) to be applied to the new user.

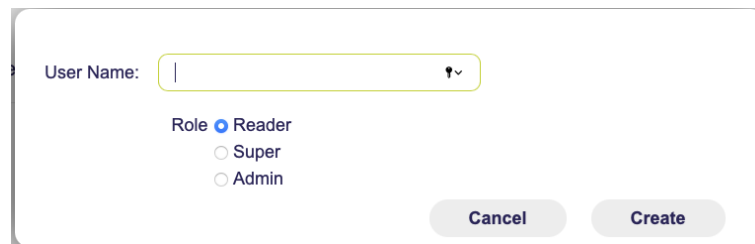


Figure 10: Add new user

After this step, the client certificates will be downloaded automatically. The password needed for the installation is the same as the provided user name, similarly as for the **admin_pki_container**.

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.

8 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 11) will be displayed:

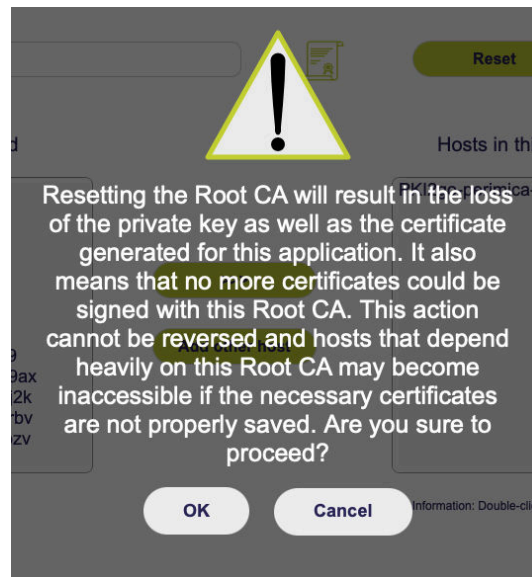


Figure 11: Reset Root CA confirmation

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

9 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
```

10 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 12). This behavior 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.

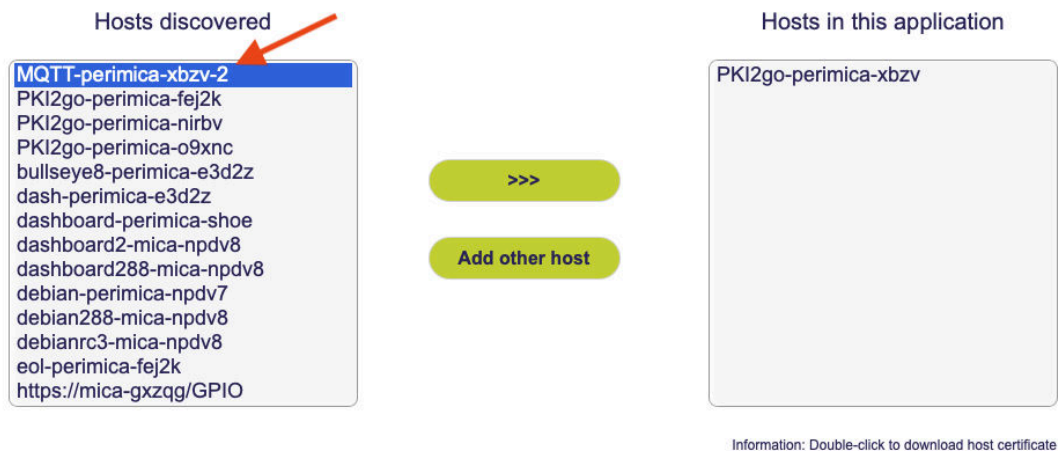


Figure 12: PKI2go wrong hostname with suffix

11 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

References

- [1] *Security Certificates Installation Guide*

Revision History

Revision	Date	Author(s)	Description
1.0	August 31, 2021	Dilmari Seidel Heuer	Initial release