



# 取扱説明書

製品名称

SMC Certificate Generator

型式 / シリーズ / 品番

EXA1-※※-EN

EXA1-※※-PN

EXW1-BENAC1

EXW1-BPNAC1

SMC株式会社

## 目次

<b>本ソフトウェアについて</b> .....	<b>3</b>
概要.....	3
システム構成.....	3
<b>本ソフトウェアの使用方法</b> .....	<b>4</b>
インストール.....	4
CA 証明書の作成.....	7
デバイス証明書の作成およびセットアップ.....	9
デバイス証明書の確認方法.....	13
その他.....	14

# 本ソフトウェアについて

## 概要

本ソフトウェアは OPC UA™対応製品に対して、デバイス証明書を設定するためのソフトウェアツールです。OPC UA™対応製品と OPC UA™クライアントツールを接続する際に、デバイス証明書が必要になる事があります。その場合、本ソフトウェアを用いてデバイス証明書の作成とセットアップが可能です。

本ソフトウェアは、PC上で動作するアプリケーションソフトウェアです。対応 OS は、下記の通りです。

Windows®11(64bit)

Windows®10(32bit/64bit)

本ソフトウェアが対象とする OPC UA™対応製品は、下記の通りです。

EXA1-\*\*-PN-\*\*

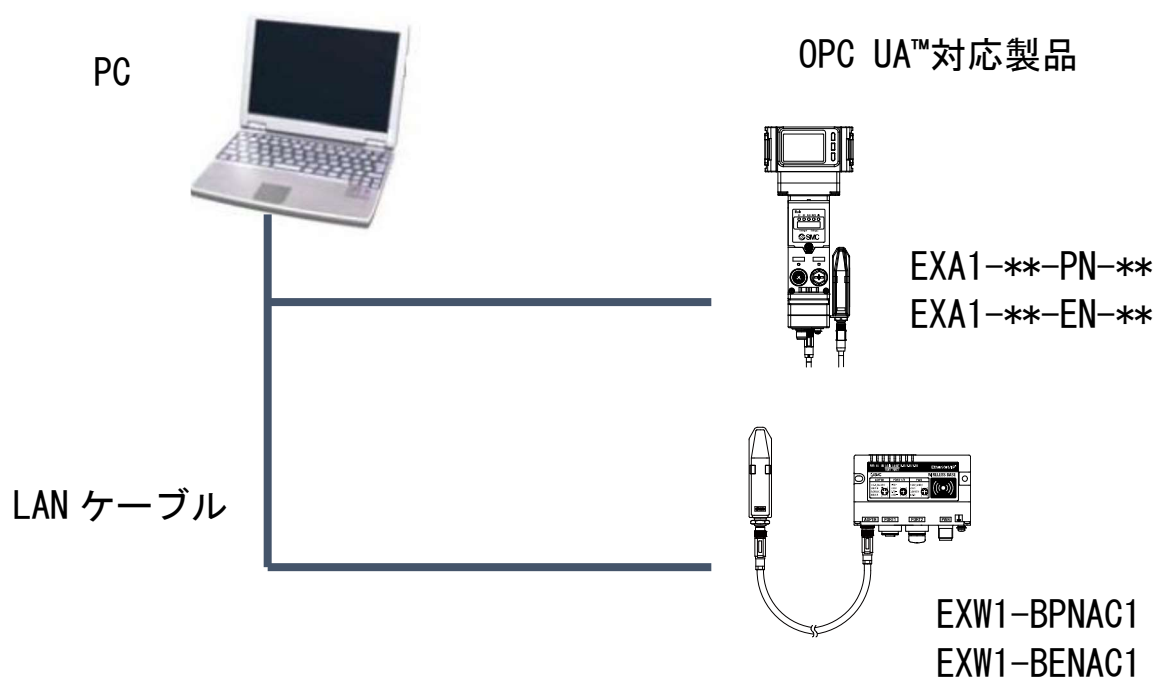
EXA1-\*\*-EN-\*\*

EXW1-BPNAC1

EXW1-BENAC1

## システム構成

本ソフトウェアは、本ソフトウェアをインストールした PC と OPC UA™対応製品を、LAN ケーブルで接続して使用します。LAN ケーブルは、ご使用になる OPC UA™対応製品に適したケーブルをご使用ください。使用可能な LAN ケーブルの詳細については、ご使用になる OPC UA™対応製品の取扱説明書をご参照ください。



# 本ソフトウェアの使用方法

## インストール

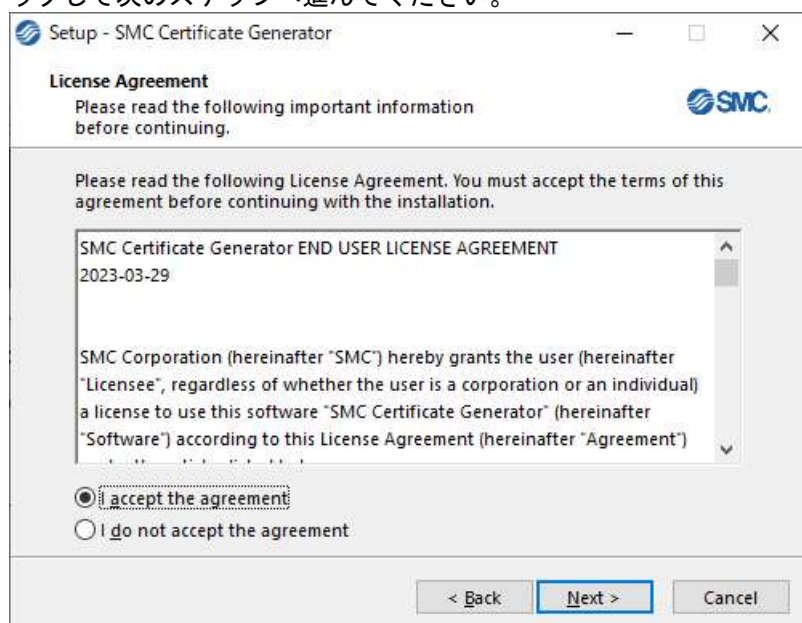
本ソフトウェアは、PC にインストールして使用します。以下のインストーラーファイルをダブルクリックしてインストールを開始してください。

SMC Certificate Generator Setup 2.1.0.0.exe

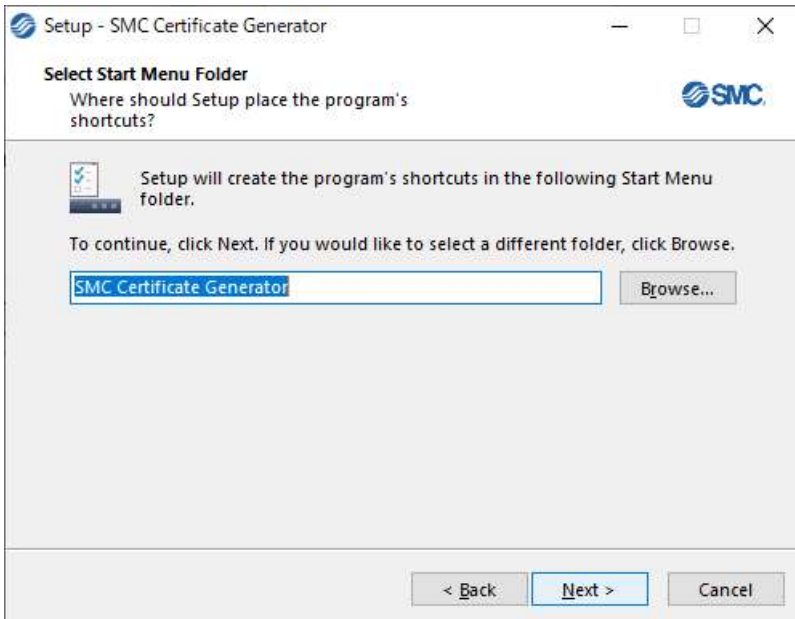
インストールを開始すると以下のウィンドウが表示されます。Next ボタンをクリックして次のステップへ進んでください。



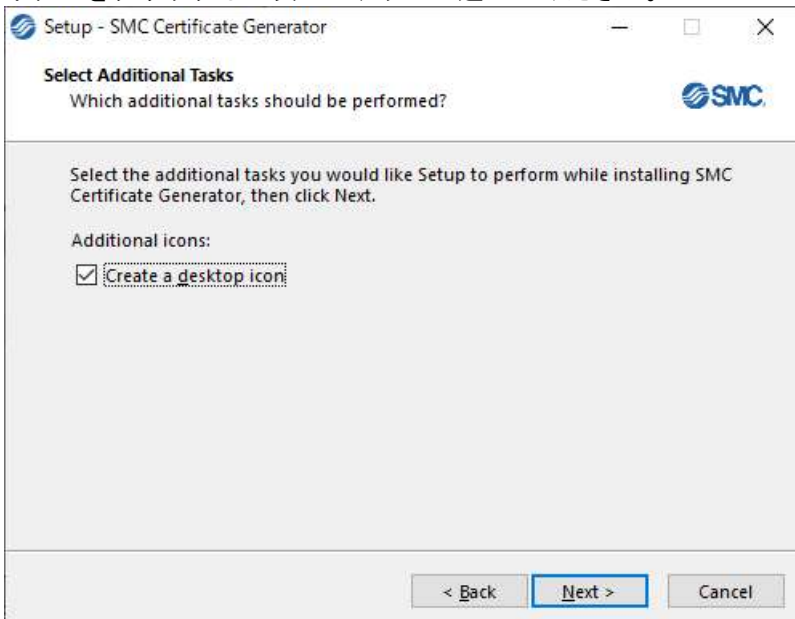
次のステップでは、以下の画面が表示されます。この画面の License Agreement の内容をご確認ください。内容に問題がなければ、I accept the agreement にチェックをしてください。そして、Next ボタンをクリックして次のステップへ進んでください。



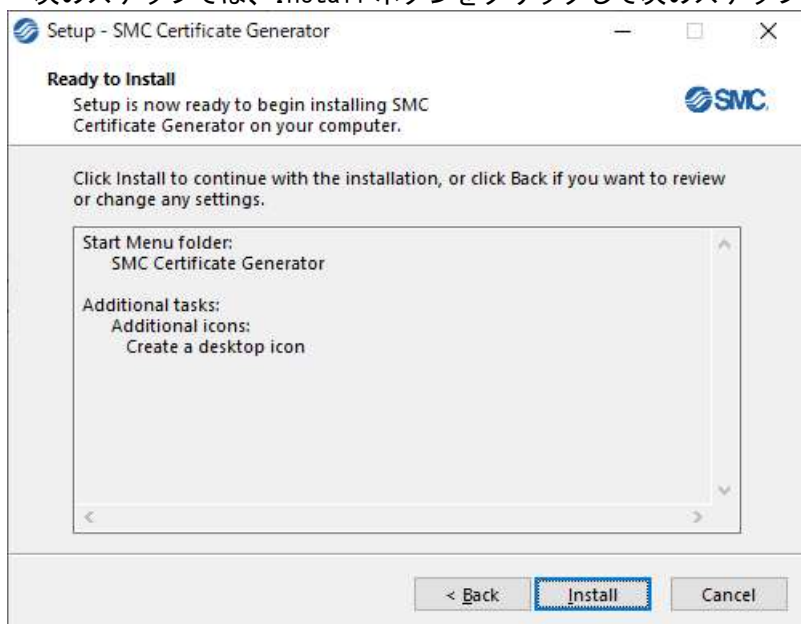
次のステップに進むと、以下の画面が表示されます。本ソフトウェアをインストールするフォルダを指定した後、Next ボタンをクリックして次のステップへ進んでください。



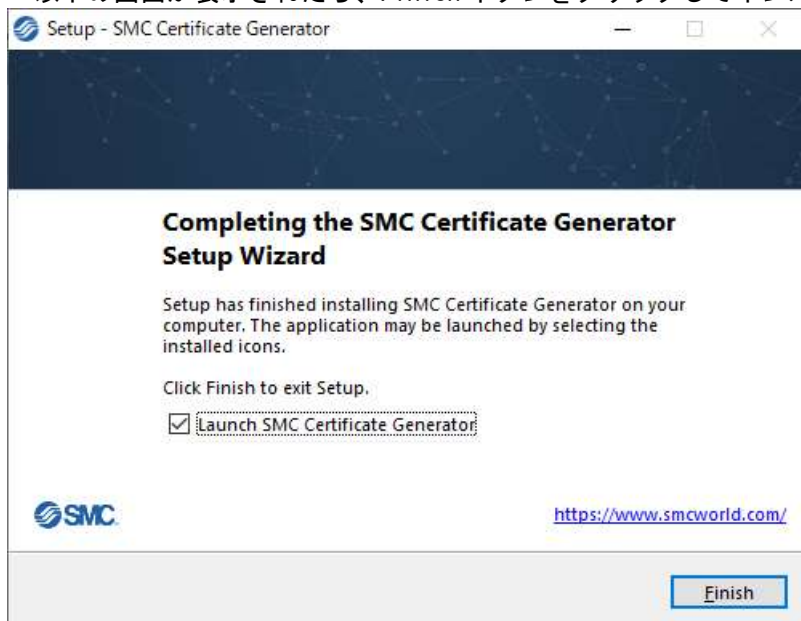
次のステップでは PC のデスクトップ上にアイコンを作成するかどうかを選択します。設定した後、Next ボタンをクリックして次のステップへ進んでください。



次のステップでは、Install ボタンをクリックして次のステップへ進んでください。



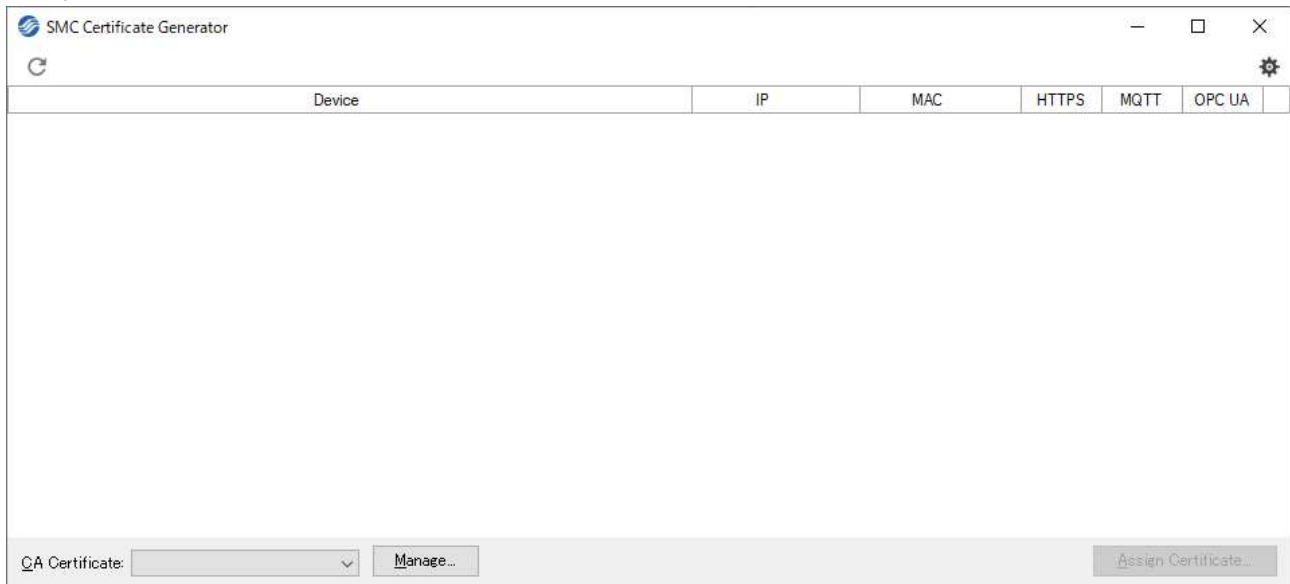
以下の画面が表示されたら、Finish ボタンをクリックしてインストールを完了してください。



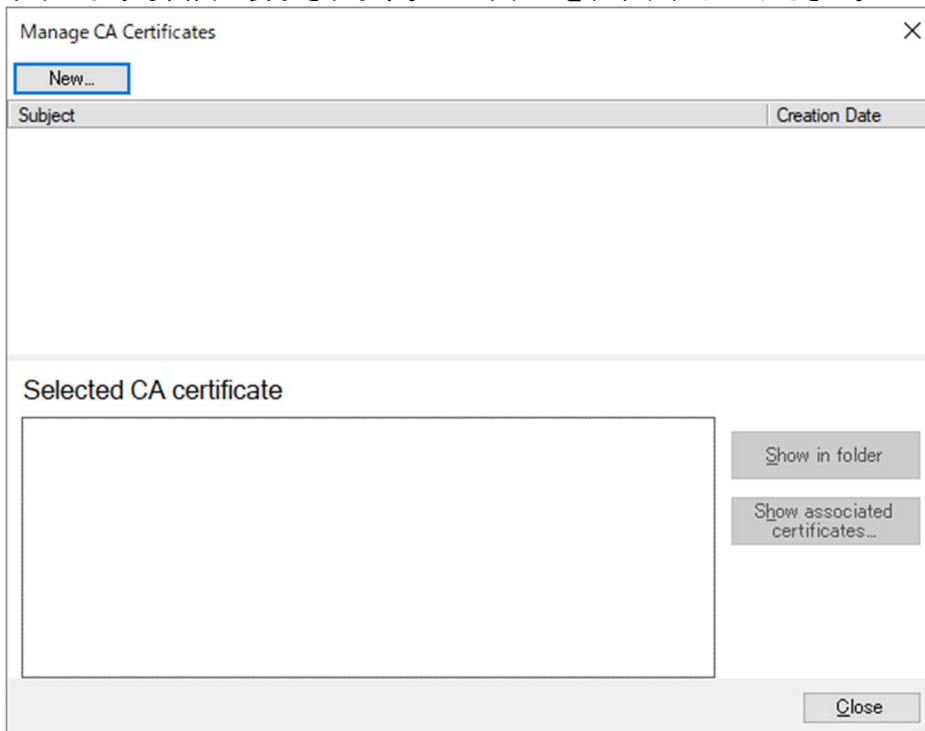
## CA 証明書の作成

PC へのインストールが完了すると、Windows の Start メニューに SMC Certificate Generator が登録されます。SMC Certificate Generator を使用して CA 証明書およびデバイス証明書を作成します。

アプリケーションソフトウェア SMC Certificate Generator を実行すると以下の画面が表示されます。最初に CA 証明書を作成します。アプリケーションウィンドウ画面下部の Manage ボタンをクリックしてください。



以下のような画面が表示されます。New ボタンをクリックしてください。



CA 証明書を作成するために、Valid Days、CAL Valid Days、および、Common Name の各項目に値を入力してください。入力する値は任意の値で問題ありません。また、Organization の各項目は必要に応じて入力してください。

入力が終わりましたら、Generate CA Certificate ボタンをクリックしてください。

Algorithm	Organization	Identity
Key Algorithm RSA	Country Name (C) 	Common Name (CN) 
Key Size 2048	State or Province (ST) 	
Signature Algorithm SHA-256	Locality (L) 	
Valid Days 365	Organization Name (O) SMC Corporation	
CRL Valid Days 365	Organizational Unit (OU) 	
	Email Address 	

以下の画面が表示されたら、CA 証明書の作成は完了です。

また、下記画面の Show in folder ボタンをクリックすると、CA 証明書が作成されたフォルダを開きます。CA 証明書のファイルが必要な場合は、これらのファイルを参照してください。

Subject	Creation Date
EXA1	2023/07/14

**Selected CA certificate**

Version: 3 (x2)  
Serial Number: 10bc:03:82:ce:4a:91:19:e0:d0:cc:a3b5f9:16:5c:bd:aa:ea:0a  
Signature Algorithm: SHA-256  
Issuer: O = SMC Corporation, CN = EXA1  
Validity:  
Not Before: Jul 14 07:47:42 2023 GMT  
Not After: Jul 13 07:47:42 2024 GMT  
Subject: O = SMC Corporation, CN = EXA1  
Key Algorithm: RSA  
Key Size: 2048 bit



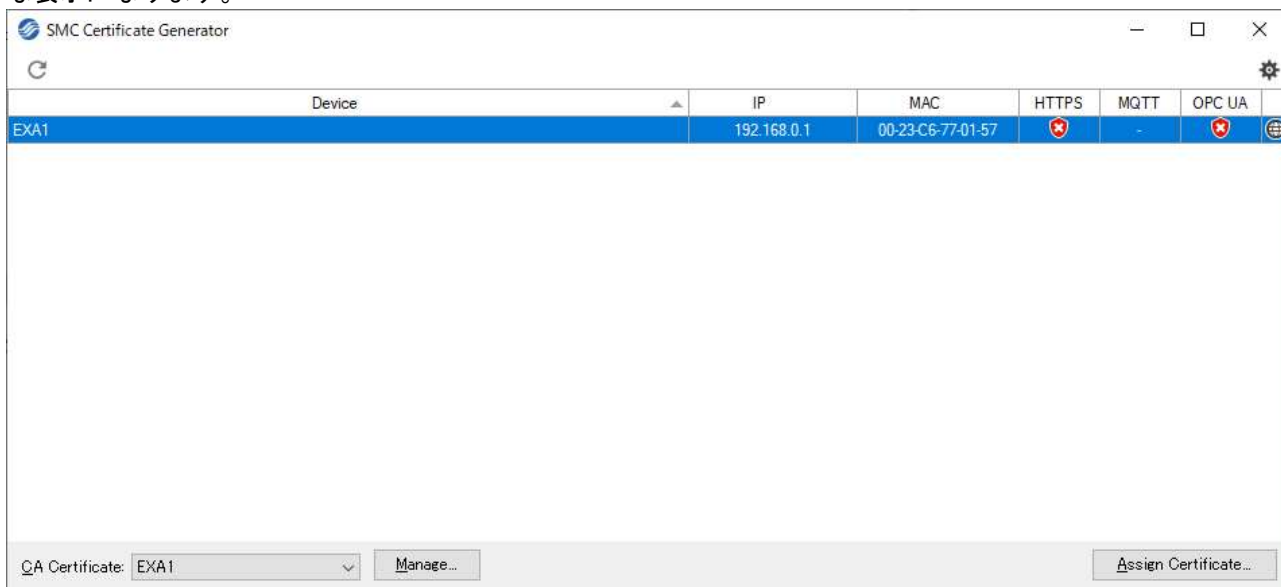
## デバイス証明書の作成およびセットアップ

次にデバイス証明書の作成とセットアップを行います。

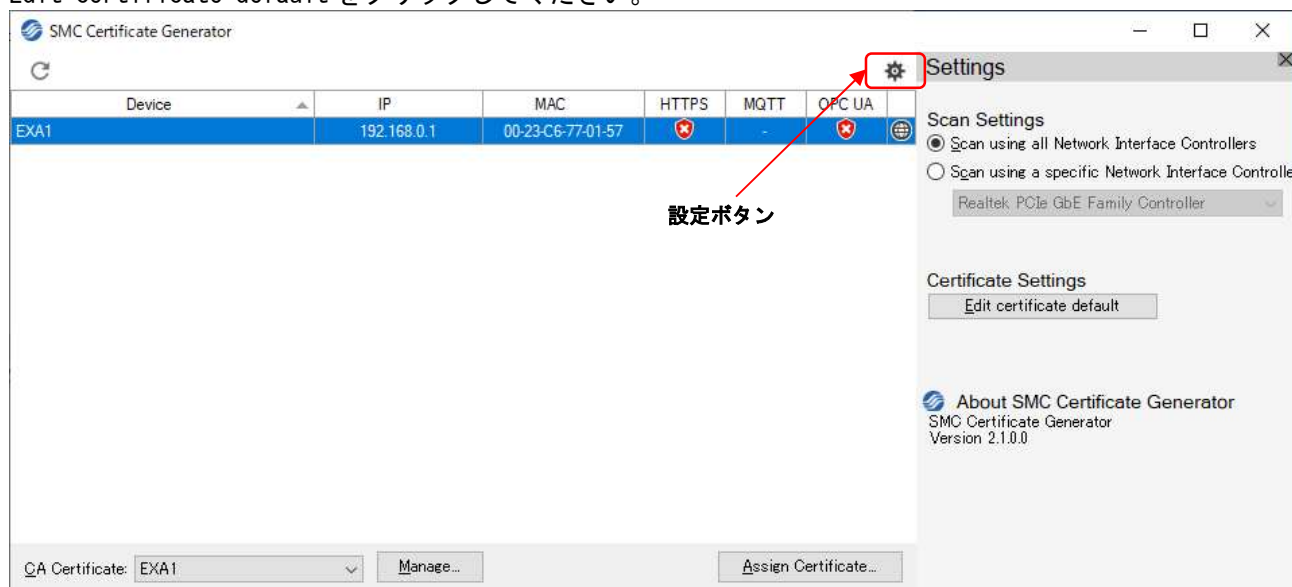
デバイス証明書のセットアップを行うため、PC とご使用になる OPC UA™対応製品を LAN ケーブルで接続してください。そして、OPC UA™対応製品の電源を投入して起動されてください。

また、デバイス証明書のセットアップのために、OPC UA™対応製品の IP アドレスを設定しておく必要があります。IP アドレスの設定方法については、OPC UA™対応製品の取扱説明書を参照ください。

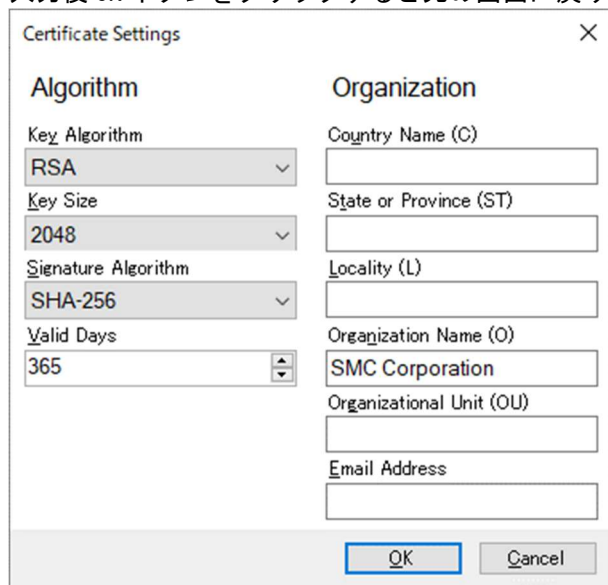
PC と OPC UA™対応製品との接続が行われると、PC 上の SMC Certificate Generator の画面は以下のような表示になります。



ここで、画面上部の設定ボタンをクリックすると、以下のような表示になります。Setting メニューにある Edit certificate default をクリックしてください。



Valid Days の値を確認してください。また、Organization の各項目は必要に応じて入力してください。入力後 OK ボタンをクリックすると元の画面に戻ります。



The dialog box is titled "Certificate Settings" and is divided into two main sections: "Algorithm" and "Organization".

**Algorithm Section:**

- Key Algorithm: RSA (dropdown menu)
- Key Size: 2048 (dropdown menu)
- Signature Algorithm: SHA-256 (dropdown menu)
- Valid Days: 365 (spin box)

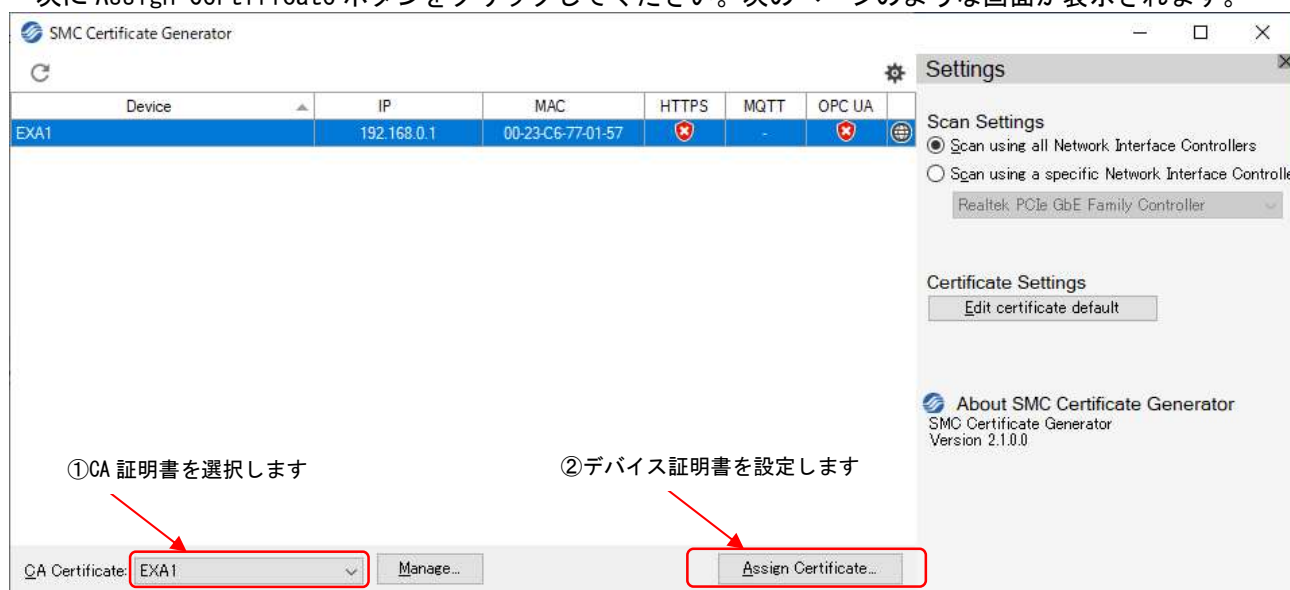
**Organization Section:**

- Country Name (C): [Empty text box]
- State or Province (ST): [Empty text box]
- Locality (L): [Empty text box]
- Organization Name (O): SMC Corporation
- Organizational Unit (OU): [Empty text box]
- Email Address: [Empty text box]

At the bottom of the dialog are "OK" and "Cancel" buttons.

元の画面に戻りましたら、デバイス証明書の生成に使用する CA 証明書を選択します。以下の画面の下部にある CA Certificate のメニューより使用する CA 証明書を選択してください。すでに複数の CA 証明書を作成済みである場合には、使用する CA 証明書を選択することが出来ます。

次に Assign Certificate ボタンをクリックしてください。次のページのような画面が表示されます。



The main interface of the SMC Certificate Generator shows a table of devices and a settings panel on the right.

Device	IP	MAC	HTTPS	MQTT	OPC UA
EXA1	192.168.0.1	00-23-C6-77-01-57	✖	-	✖

Annotations on the interface:

- ① CA 証明書を選択します: Points to the "CA Certificate" dropdown menu at the bottom left, which currently shows "EXA1".
- ② デバイス証明書を設定します: Points to the "Assign Certificate..." button at the bottom right.

The right-hand "Settings" panel includes "Scan Settings" (radio buttons for "Scan using all Network Interface Controllers" and "Scan using a specific Network Interface Controller"), "Certificate Settings" (with an "Edit certificate default" button), and "About SMC Certificate Generator" (version 2.1.0.0).

この画面では、デバイス証明書の設定に必要な情報を入力します。

- ・ Protocols to Assign の項目で OPC UA にチェックを追加してください。
- ・ Identity の Common Name は、ご使用になる OPC UA™対応製品により値が異なります。表 1 をご参照の上、Common Name の値を入力してください。

表 1 対応製品と Common Name の関係

OPC UA™対応製品	Common Name
EXA1-**-PN-**-**	EXA1
EXA1-**-EN-**-**	EXA1-**-EN-**-**
EXW1-BPNAC1	EXW1-BPN
EXW1-BENAC1	EXW1-BENAC*

- ・ Alternative Names には以下の項目について入力してください。  
プルダウンメニューより追加する項目 (IP、URI 等) を選択してください。  
値を入力した後、Add ボタンをクリックしてください。

[URI] : 以下の値を入力してください。この項目は必ず入力してください。

urn:[PID]:www.smcworld.com

[PID]にはご使用になる OPC UA™対応製品の PID (8 文字) を入力してください。

PID は OPC UA™対応製品の筐体に貼付けされた銘版に記載されています。

(銘版に記載されているデータマトリックスコードを読み込むと、PID 等の情報を確認できます)

#### ■入力例

PID が 17E340EF の時の [URI] の入力値

urn:17E340EF:www.smcworld.com

入力が完了したら、Continue ボタンをクリックしてください。

Configure Certificate

Protocols to Assign

- HTTPS
- OPC UA

Identity

Common Name (CN)

EXA1

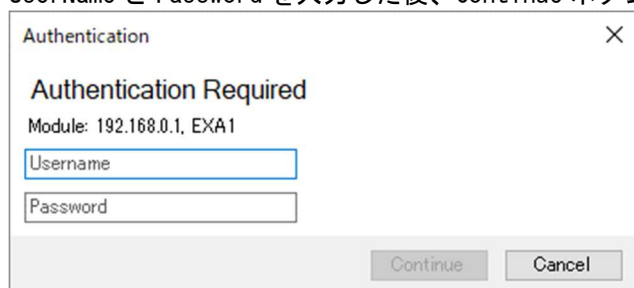
Alternative Names

Add

URI | urn:17E340EF:www.smcworld.com

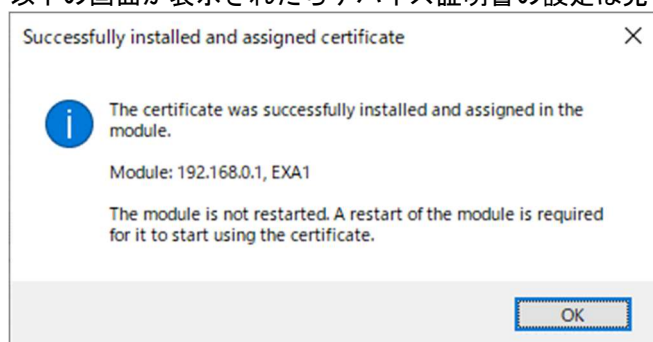
Continue Cancel

その後、以下の画面にて UserName と Password を要求されます。  
UserName と Password は、OPCUA のアカウントとして設定したものを使用してください。  
(Default 状態の UserName/Password は、admin/admin です)  
UserName と Password を入力した後、Continue ボタンをクリックしてください。



The image shows a dialog box titled "Authentication" with a close button (X) in the top right corner. The main heading is "Authentication Required". Below this, it says "Module: 192.168.0.1, EXA1". There are two input fields: "Username" and "Password". At the bottom, there are two buttons: "Continue" and "Cancel".

以下の画面が表示されたらデバイス証明書の設定は完了です。



The image shows a dialog box titled "Successfully installed and assigned certificate" with a close button (X) in the top right corner. On the left, there is a blue information icon (i). The text reads: "The certificate was successfully installed and assigned in the module." Below this, it says "Module: 192.168.0.1, EXA1". Further down, it says "The module is not restarted. A restart of the module is required for it to start using the certificate." At the bottom right, there is an "OK" button.

## デバイス証明書の確認方法

OPC UA™対応製品の Web サーバーでは、デバイス証明書の設定を確認することができます。また、Web サーバーでは、設定したデバイス証明書を削除することも可能です。

PC 上で Web ブラウザソフトウェアを起動した後、Web ブラウザの URL にご使用の OPC UA™対応製品の IP アドレスを入力すると Web サーバーへアクセス出来ます。Web サーバーへアクセスした後、OPCUA の Certificate を設定するページを選択してください。Web サーバーの仕様の詳細については、ご使用になる OPC UA™対応製品の取扱説明書をご参照ください。

ここで、EXA1-\*\*-PN-\*\*の Web サーバーへアクセスした際の例を以下に示します。Certificate のページを選択すると、Device Certificate の項目に設定されたデバイス証明書が表示されます。

また、例えばデバイス証明書を再度セットアップする場合等において、このデバイス証明書を削除したい場合は、この画面上で Delete ボタンをクリックしてください。デバイス証明書が削除されます。

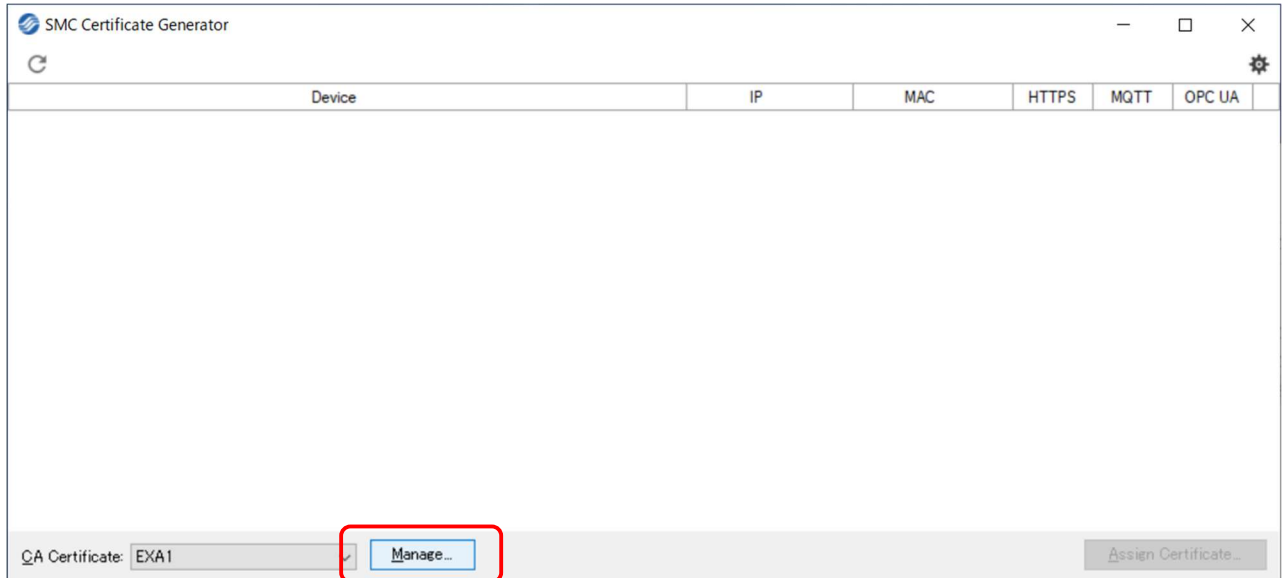
The screenshot shows the SMC Air Management System (AMS) web interface. The page title is 'CERTIFICATE'. The sidebar on the left contains the following navigation items: EXA1-40-PN, Home, Air Management Hub, OPC UA, Certificate (highlighted with a red box), System log, Wireless log, 001 EXW1-RDM, System, Network, Setting, Logout, and Link. The main content area is divided into two sections: 'Certificate authorities' and 'Device certificate'. The 'Certificate authorities' section has a table with columns: Name, Issuer, Expires, and Delete. Below the table is an 'Add...' button. The 'Device certificate' section has a table with columns: Name, Issuer, Issued, Expires, and Delete. The table contains one entry: EXA1, O=SMC Corporation, CN=EXA1, 2023-07-14 08:08:54, 2024-07-13 08:08:54, and a Delete button. Below the table is an 'Add...' button. At the bottom of the page, there is a footer: 'Air Management System (AMS) © 2022 SMC Corporation All Rights Reserved. Version Q 1.10'.

## その他

### ● デバイス証明書のファイルのみ作成する方法

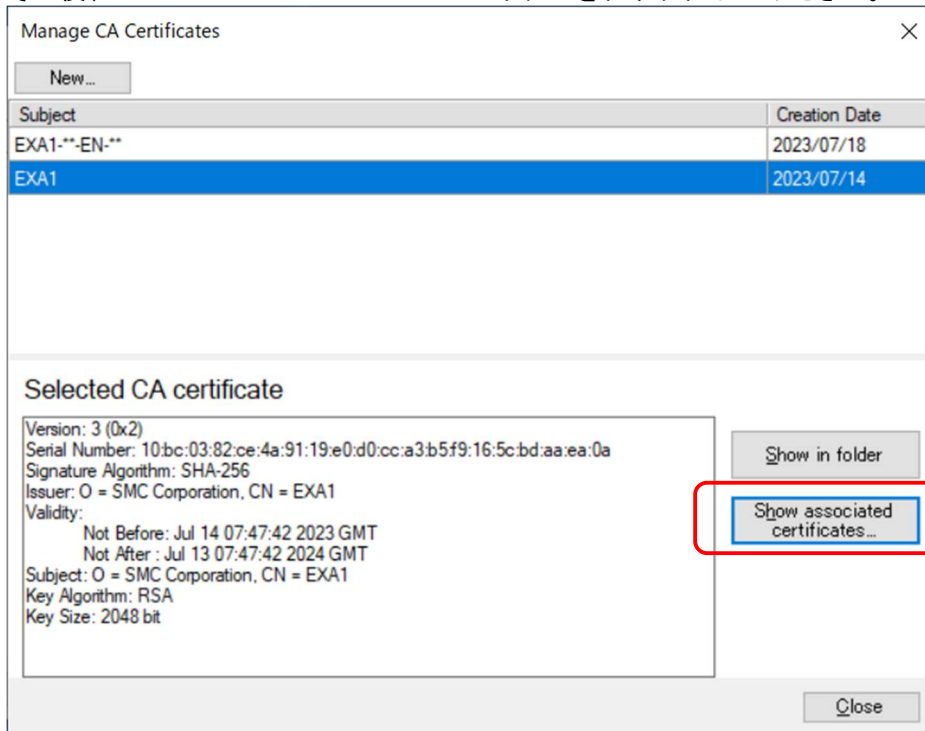
本ソフトウェアでは、OPC UA™対応製品へデバイス証明書をセットアップせずに、デバイス証明書のファイルのみを作成する事も可能です。ここでは、デバイス証明書のファイルのみを作成する方法を説明します。

最初に、SMC Certificate Generator を起動してください。起動すると、以下の画面が表示されます。

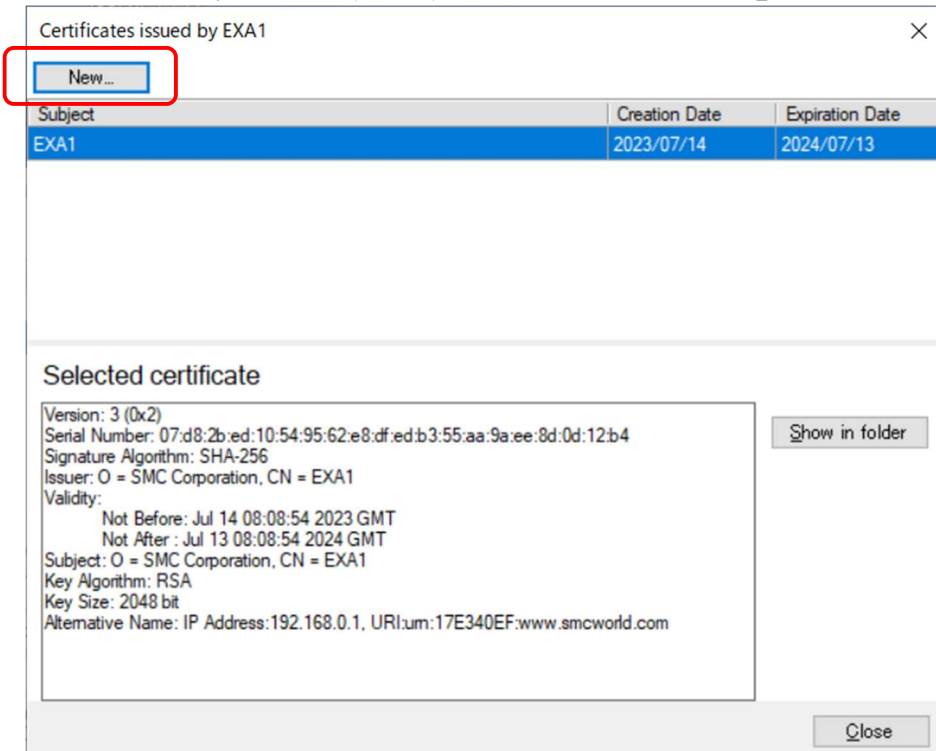


上記画面の Manage ボタンをクリックしてください。すると、以下の画面が表示されます。この画面では、既に作成したデバイス証明書が表示されます。複数表示された場合は、デバイス証明書の生成に用いる CA Certificate を選択してください。

その後、Show associated certificates ボタンをクリックしてください。



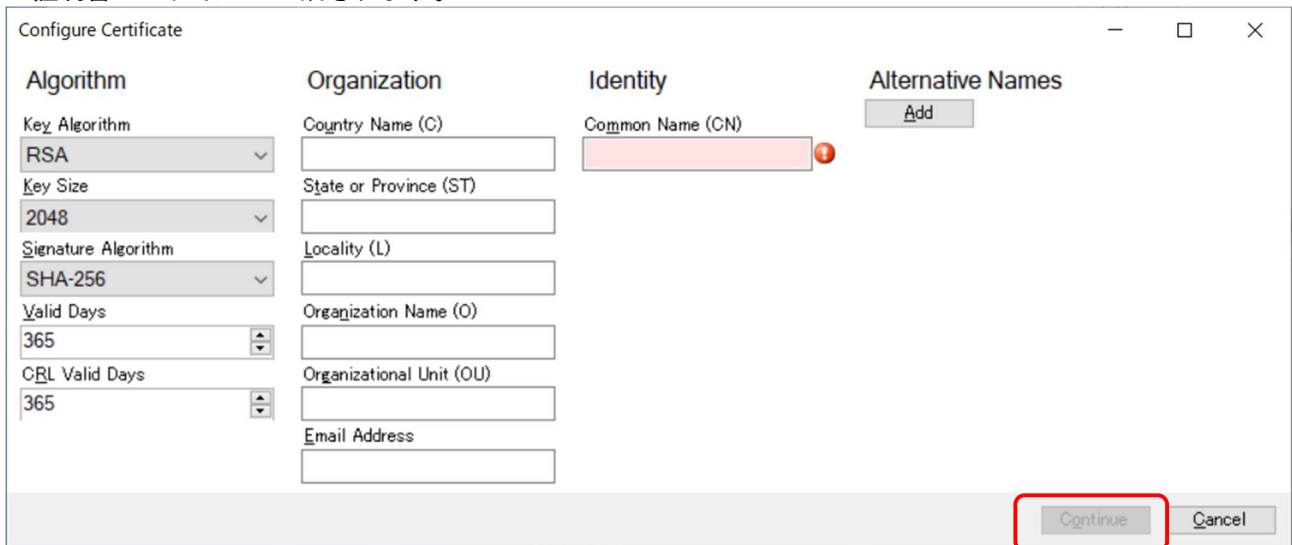
以下の画面が表示されますので、この画面上の New ボタンをクリックしてください。



以下のデバイス証明書の生成画面が表示されます。

この画面上で、デバイス証明書に必要な事項を入力してください。デバイス証明書の作成に必要な入力事項は、「デバイス証明書の作成およびセットアップ」の章で説明した内容と同じです。

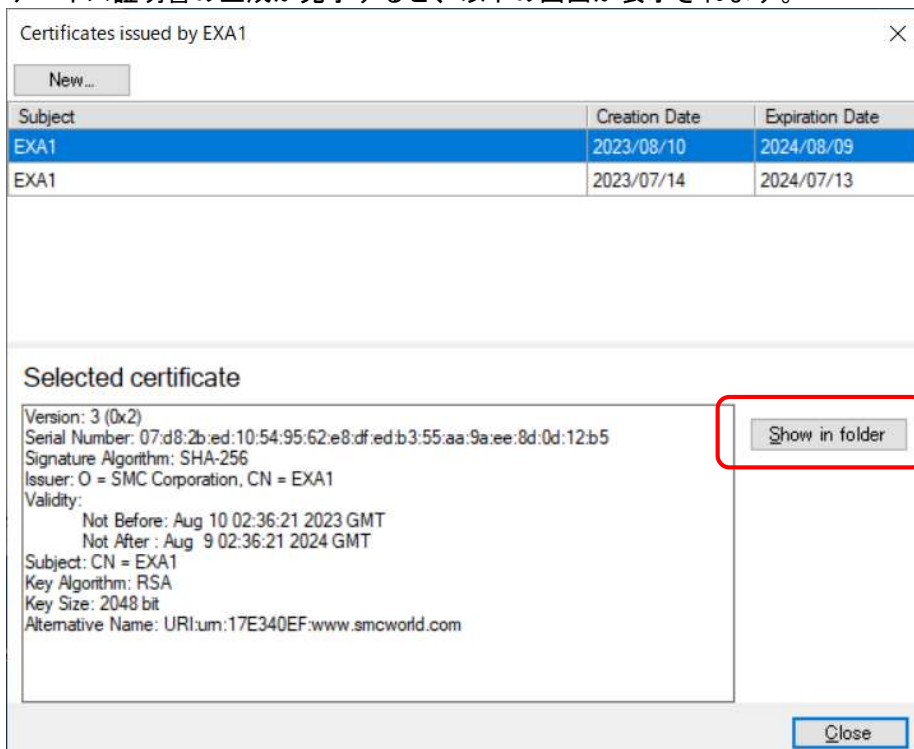
デバイス証明書の作成に必要な入力が終わりましたら、Continue ボタンをクリックしてください。デバイス証明書のファイルが生成されます。



[備考]

- ① Alternative Names の項目は Add ボタンをクリックすると、アイテムを追加できます。アイテム追加後、項目 (IP、URI 等) を選択して、値を入力してください。
- ② Identify の Common Name の項目には、表 1 記載の値を入力してください。

デバイス証明書の生成が完了すると、以下の画面が表示されます。



また、上記画面上の Show in folder ボタンをクリックすると、生成したデバイス証明書のファイルが保存されたフォルダが開きます。以下のようなデバイス証明書のファイルが生成されます。

名前	更新日時	種類	サイズ
Certificate in PEM format.crt	2023/08/10 11:36	セキュリティ証明書	2 KB
Certificate Signing Request in PEM format.csr	2023/08/10 11:36	CSR ファイル	1 KB
Private key for certificate in PEM format.key	2023/08/10 11:36	KEY ファイル	2 KB

OPC UA™対応製品の Web サーバーでは、デバイス証明書の設定を確認する事ができます。Web サーバーでは、デバイス証明書のファイル（セキュリティ証明書、および、KEY ファイル）がある場合、そのファイルをデバイス証明書としてセットアップすることも可能です。Web サーバーの仕様や操作方法等の詳細については、ご使用になる OPC UA™対応製品の取扱説明書をご参照ください。



改訂履歴

1 : 記載内容追加 [2024 年 2 月]

**SMC株式会社** お客様相談窓口

URL <https://www.smcworld.com>



**0120-837-838**

受付時間/9:00~12:00 13:00~17:00【月~金曜日, 祝日, 会社休日を除く】

⑧ この内容は予告なしに変更する場合がありますので、あらかじめご了承ください。

© SMC Corporation All Rights Reserved

