TWN4

Device Security

DocRev3, November 7, 2022

ELATEC GmbH

Contents

1 Introduction

With firmware V4 of TWN4, ELATEC introduces extensive support for data security on the TWN4 family of devices. This document describes, how to activate and use TWN4 Device Security.

2 Related Documents

For usage of the program AppBlaster, please also see the document "TWN4 AppBlaster Config Cards User Guide".

3 Purpose of TWN4 Device Security

In order to get a better understanding of the object, we distinguish between following security domains:

- Security features, which are supported already today and w/o further action
- Security features, which become available by activating TWN4 Device Security
- Security features, which depend on the custom specific application and require an individual evaluation and implementation

3.1 Comparison of Security Domains

Here is a list of various aspects around security of TWN4 and how to achieve required level of security:

Feature	Generally Supported	**Supported by TWN4 Device Security**	To be Implemented in Application
TWN4 read protection of firmware	Yes	Generally supported	-
TWN4 read protection of App	Yes	Generally supported	-
Encrypted firmware in image (bix) file	Yes	Generally supported	-
Encrypted App in image file	No	Yes	-
Save storage of secret data (keys) in the App	No	Yes	-
Encrypted AppBlaster project file	No	Yes	-
Custom-specific encrypted firmware in image (bix) file	No	Yes	-
Custom-specific encrypted App in image (bix) file	No	Yes	-
TWN4 protection against being programmed with unwanted firmware images	No	Yes	-
TWN4 protection against being configured with unwanted CONFIG Cards	No	Yes	-
Protect firmware images against being used in 3rd party TWN4	No	Yes	-
Protect CONFIG Cards against being used against 3rd party TWN4	No	Yes	-
Custom specific encrypted App in image (bix) file	No	Yes	-
Save storage of secret data (keys) on mass storage of TWN4	No	Yes (e.g. key stored securely in the App)	Yes (depending on data being stored)
TWN4 custom-specific host communication	No	No	Yes
TWN4 custom-specific transponder communication	No	No	Yes

3.2 Typical Use Cases for TWN4 Device Security

- Solution providers send firmware images and project files containing secret data even over public communication channels, e.g. email.
- Solution providers ensure, that their TWN4 in the field are programmed with wanted firmware images only.
- TWN4 cannot be programmed with firmware, which is intended for use in a different application or by 3rd party.
- Protect TWN4 against being configured by others.
- TWN4 does only accept CONFIG Cards, which are wanted by the solution provider.
- Firmware images and CONFIG Cards cannot by used by 3rd party.

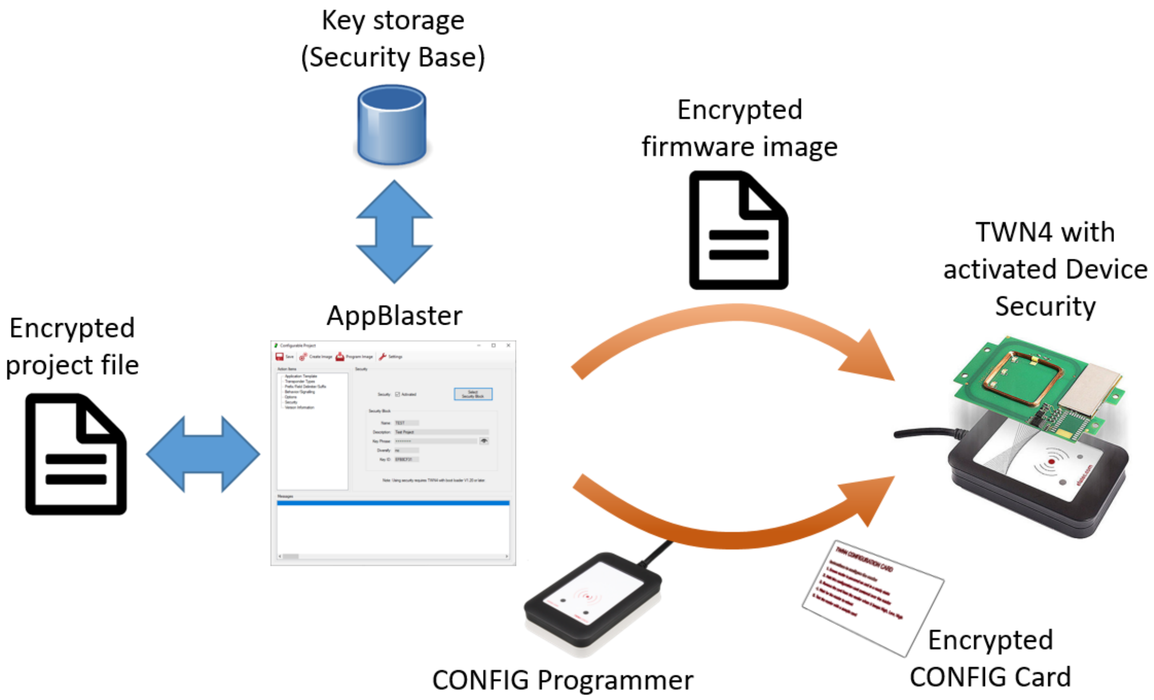
4 How does TWN4 Device Security Work?

TWN4 Device Security is based on symmetrical encryption. This means: An identical encryption key is known both to the instance, which is sending encrypted data and the instance, which is receiving and decrypting data.

For TWN4 Device Security, this means:

- AppBlaster is the instance, which is encrypting data (firmware images, CONFIG Cards, project files)
- AppBlaster is also the instance, which is decrypting data (project files)
- TWN4 is the instance which is decrypting data (CONFIG Cards, project files)

As an illustration, see flow of data in the picture picture below:



5 How to use TWN4 Device Security

In order to use TWN4 Device Security on a specific device following basic tasks must be performed:

- Setup Security Block
- Activation of Device Security on TWN4
- Create suitable firmware image - or - Create suitable CONFIG Card

5.1 Prerequisites

In order to use TWN4 Device Security there are minimum requirements for the firmware installed on TWN4:

- TWN4 minimum version of boot loader is 1.20. The boot loader is installed on TWN4 by ELATEC during production. It cannot be installed by the user or solution provider.
- TWN4 minimum version of firmware is 4.01. The firmware is part of the development pack is according version, e.g. TWN4DevPack401.zip. It can be downloaded from ELATEC's web site.

5.2 Security Blocks

Before any encryption can be used, appropriate security information must be setup. The information, which is needed to activate Device Security on TWN4, encrypt firmware images or CONFIG Cards is called "Security Block".

Security Blocks are stored in the so called Security Base. The Security Base is located in the registry of current Windows user.

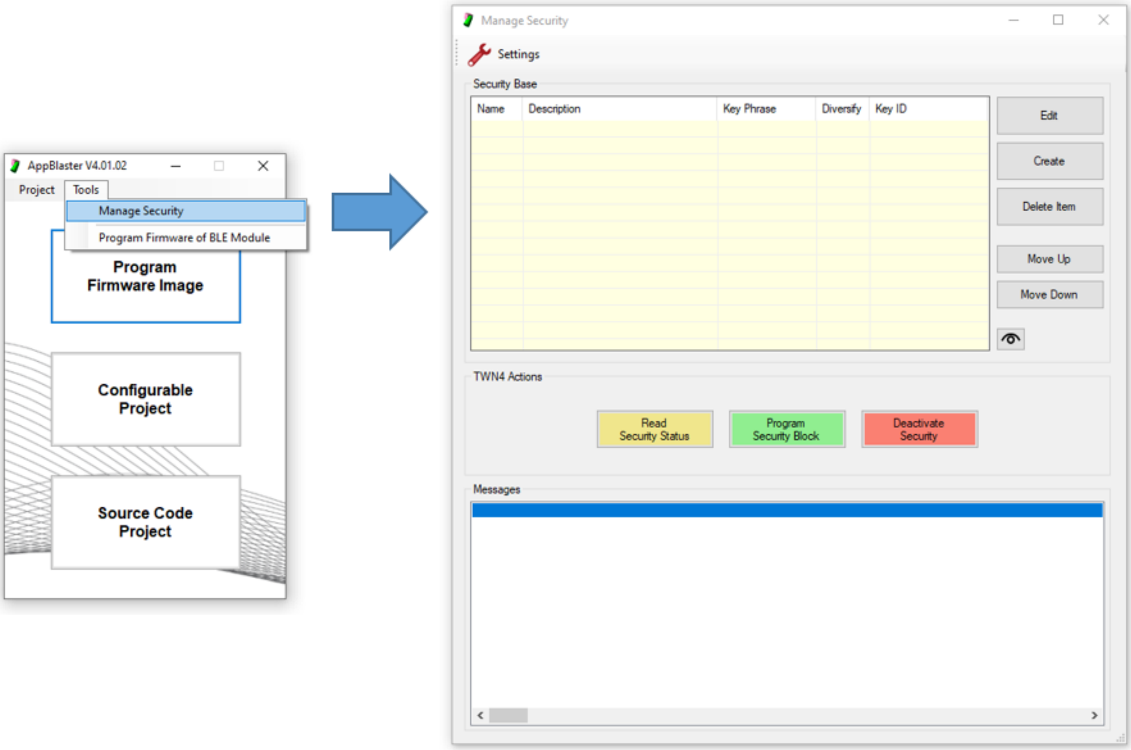
Please Note:

- The save storage of the Security Base directly depends on the security of the underlying operating system. For this reason, ELATEC recommends, to turn on encryption of the hard disc where the registry is located. Typically, this is drive C: of the computer.

In order to setup a Security Block start AppBlaster. In the top menu select "Tools - Manage Security". The dialog "Manage Security" will be opened.

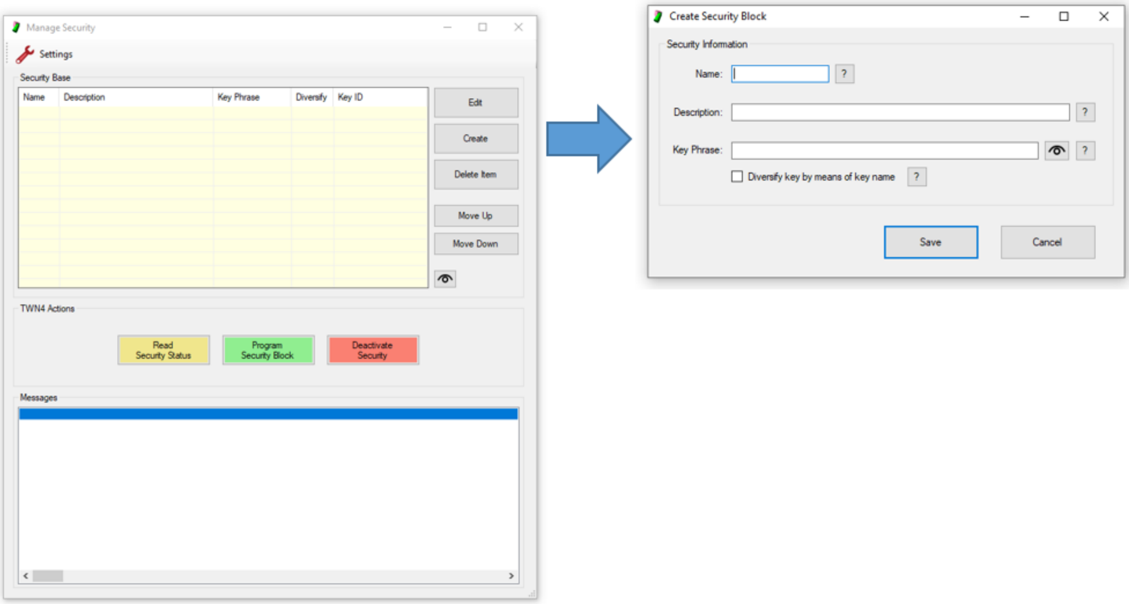
The dialog "Manage Security" is divided into three sections:

1. "Security Base": In this section, Security Blocks are managed, thus created, modified and deleted.
2. "TWN4 Actions": This section allows to activate or deactivate security or check current security status of a connected TWN4.
3. "Messages" This section is used to show currently running actions or display the result of an action.



6 Create Security Block

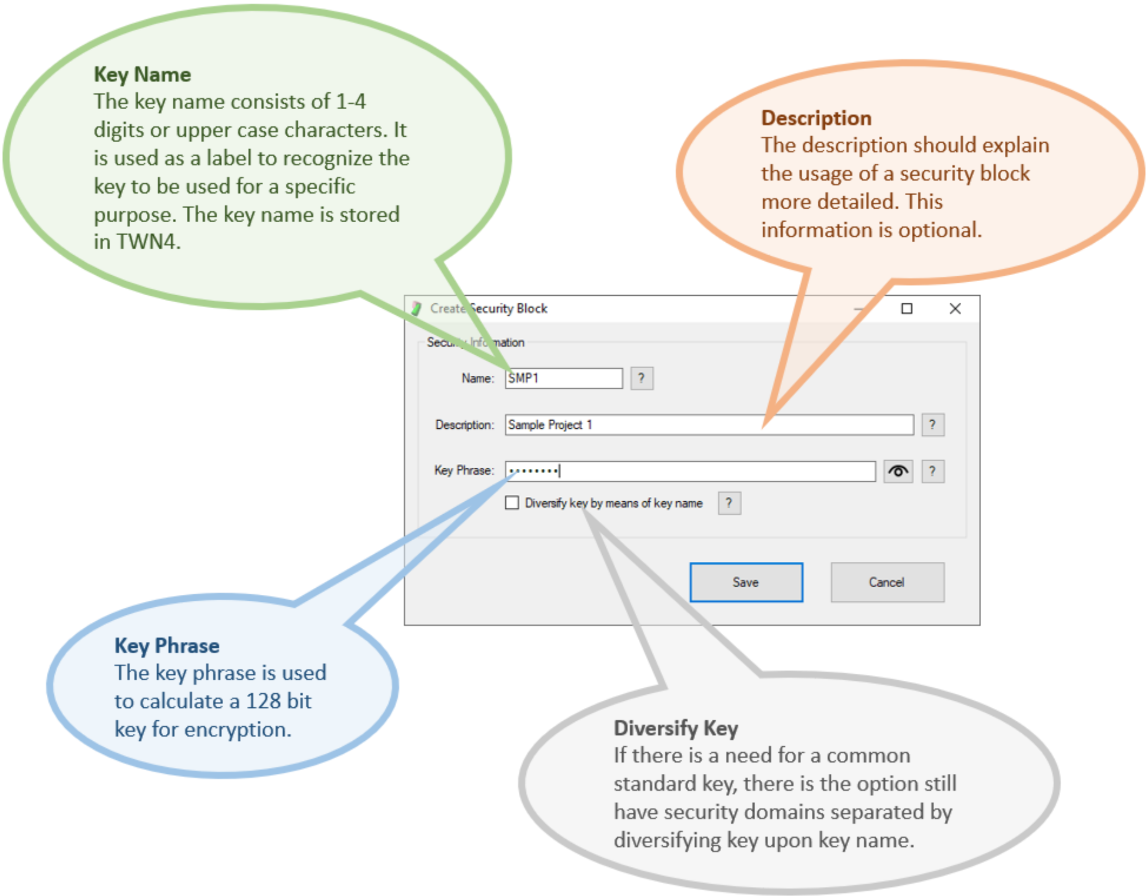
In order to create the actual Security Block, a new item in the Security base must be created. Click button "Create" to achieve this. A new dialog is opened:



The dialog requires following information to be entered:

- Key name
- Description
- Key phrase
- Diversify key (yes/no)

The picture below is explaining in detail, which information is needed:



Create Security Block

Security Information

Name: SMP1

Description: Sample Project 1

Key Phrase: ••••••••

□ Diversify key by means of key name

Key Name
The key name consists of 1-4 digits or upper case characters. It is used as a label to recognize the key to be used for a specific purpose. The key name is stored in TWN4.

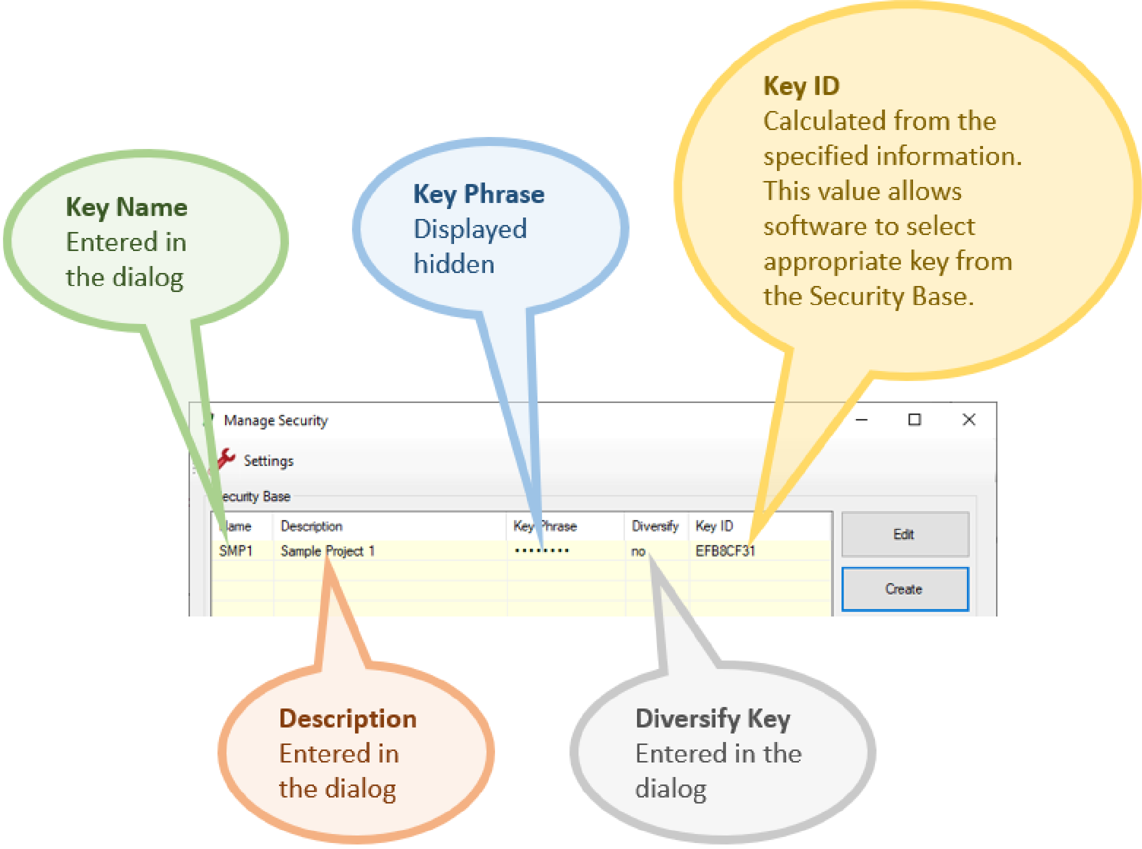
Description
The description should explain the usage of a security block more detailed. This information is optional.

Key Phrase
The key phrase is used to calculate a 128 bit key for encryption.

Diversify Key
If there is a need for a common standard key, there is the option still have security domains separated by diversifying key upon key name.

Click button "Save" to store the information in the Security Base.

The newly created item is display in the dialog "Manage Security":



lame	Description	Key Phrase	Diversify	Key ID
SMP1	Sample Project 1	••••••••	no	EFB8CF31

Key Name Entered in the dialog

Key Phrase Displayed hidden

Key ID Calculated from the specified information. This value allows software to select appropriate key from the Security Base.

Description Entered in the dialog

Diversify Key Entered in the dialog

We are now ready to activate Device Security on TWN4.

6.1 Considerations for Security Blocks

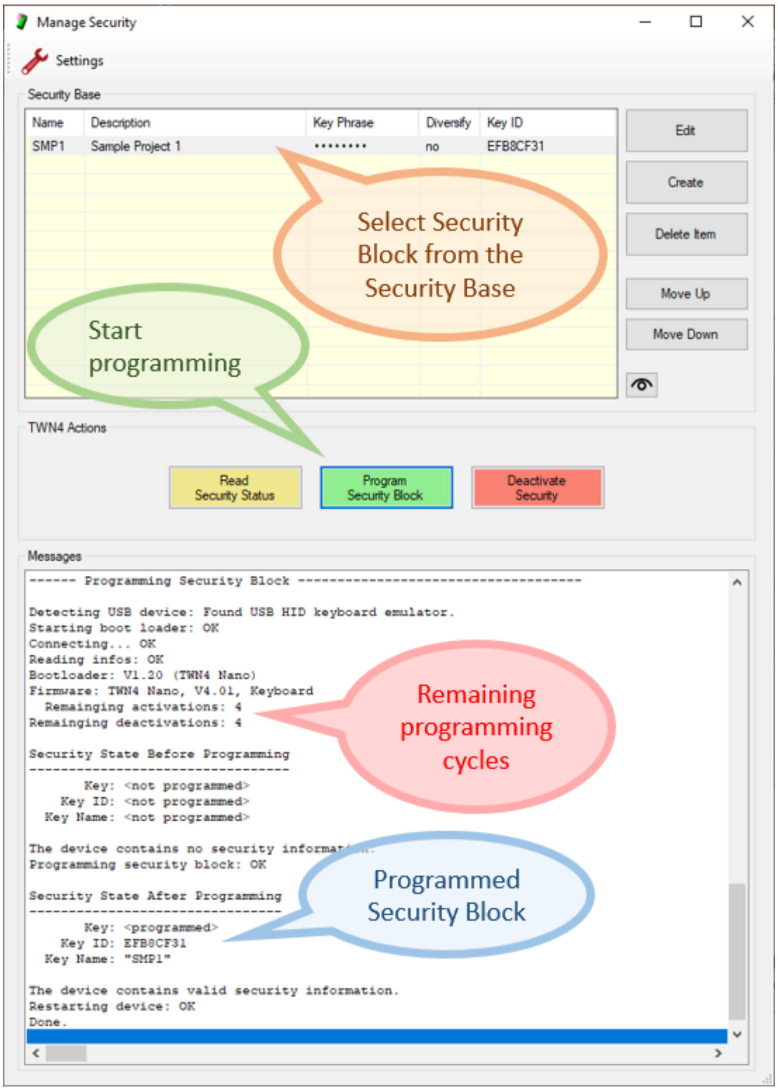
Here are some considerations about creation of Security Blocks:

- **Should there be a common key for all devices of all customers?**
  This strongly depends on the requirements from point of view of a system provider. If the only requirement is to ensure compatibility of firmware images to the solution provider itself, this can be ok.
- **To which customers should firmware images be compatible?**
  Compatibility between devices and firmware images basically requires identical Security Block. If firmware images must be interchanged between several projects or customers, the key must be identical.
- **How should I call a Key Name?**
  It depends on the intention for using security. One approach could be to take identical Key Name and App name for a specific project or application. Another one could be to use different keys for different customers. In this case you would choose a key name which is assigned to a specific customer.
- **Should diversification be used?**
  Diversification allows to use identical password for several projects or customers while maintaining that firmware images cannot be exchanged between projects or customers.
- **How to ensure identical key between several Security Blocks?**
  Even though, it is rather uncommon to specify several Security Blocks, which have identical key, it is possible. Equality of key can be determined by comparing the Key ID of Security Blocks in question.

7 Activation of Device Security on TWN4

In order to activate TWN4 Device Security, follow these few steps:

- **Step 1 - Connect TWN4**
  In order to activate TWN4 Device Security, connect a TWN4 to the host computer. Typically, TWN4 is connected to the host using USB. If TWN4 should be connected via RS232, please choose appropriate COM port in the "Settings" dialog. It is available on the top of the dialog "Manage Security".
- **Step 2 - Select Security Block**
  Open dialog "Manage Security" and choose desired Security Block from the Security Base.
- **Step 3 - Start Programming**
  Click button "Program Security Block". AppBlaster will establish a connection to the connected TWN4 and program appropriate Security Block into TWN4 automatically. Once operation is completed, the result is displayed in the section "Messages" of the dialog.



Name	Description	Key Phrase	Diversify	Key ID
SMP1	Sample Project 1	••••••••	no	EFB8CF31

```
------ Programming Security Block ------------------------------------

Detecting USB device: Found USB HID keyboard emulator.
Starting boot loader: OK
Connecting... OK
Reading infos: OK
Bootloader: V1.20 (TWN4 Nano)
Firmware: TWN4 Nano, V4.01, Keyboard
  Remainging activations: 4
Remainging deactivations: 4

Security State Before Programming
---------------------------------
       Key: <not programmed>
    Key ID: <not programmed>
  Key Name: <not programmed>

The device contains no security information.
Programming security block: OK

Security State After Programming
--------------------------------
       Key: <programmed>
    Key ID: EFB8CF31
  Key Name: "SMP1"

The device contains valid security information.
Restarting device: OK
Done.
```

7.1 Deactivation of Device Security on TWN4

For a limited number of cycles it is possible to activate and deactivate Device Security. Typically, it is possible to activate and deactivate Device Security four times. the number of possible rounds depends on other programmed options, which share identical memory.

- **Step 1 - Connect TWN4**
  Connect a TWN4 to the host computer like during activation.
- **Step 2 - Deactivate Device Security**
  Click button "Deactivate Security". AppBlaster will establish a connection to the connected TWN4 and deactivate security. Once operation is completed, the result is displayed in the section "Messages" of the dialog.
  Note:
  In order to deactivate security on TWN4, the key currently active in TWN4 must be known by AppBlaster. This means, currently in TWN4 active Security Block must also be part of the Security Base. It is not necessary for the user to select appropriate Security Block. It is selected automatically by AppBlaster.

7.2 Checking Security Status of TWN4

At any time, it is possible to check, if security on TWN4 is currently turned on or off and which Security Block is currently programmed in TWN4. Following steps:

- **Step 1 - Connect TWN4**
  Connect a TWN4 to the host computer like during activation.
- **Step 2 - Read Security Status**
  Click button "Read Security Status". AppBlaster will establish a connection to the connected TWN4 and read security status. Once operation is completed, the result is displayed in the section "Messages" of the dialog.

8 Preparing a Configuration for TWN4

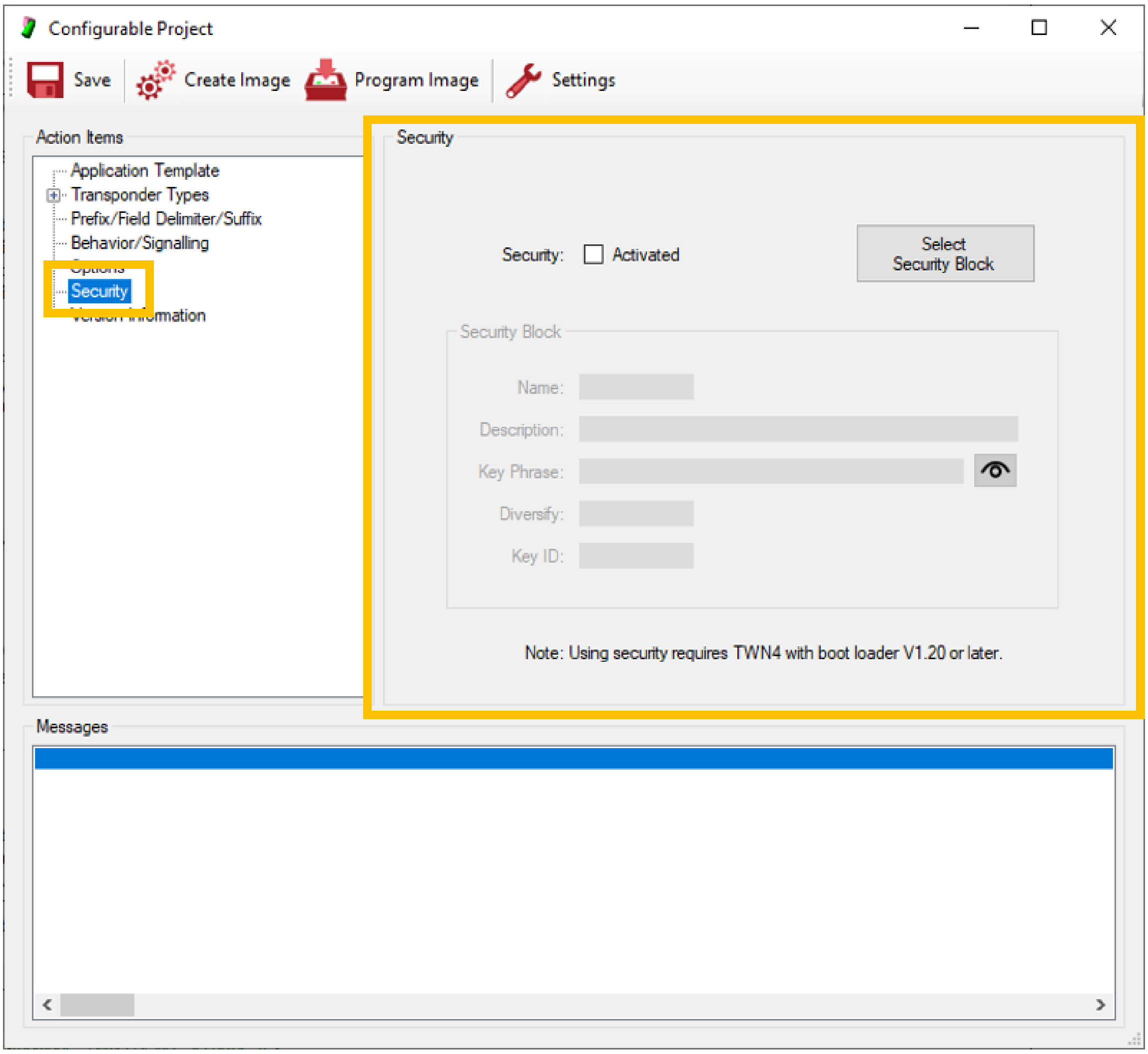
With AppBlaster 4.01, a new dialog "Security" has been established as part of projects (both configurable and source code projects).

This dialog is used to create configurations with activated security. Configurations can be either firmware images or CONFIG Cards.

Activating security has following impact:

- Firmware images (both contained firmware and App) are encrypted using a key specified by the selected Security Block.
- CONFIG Cards are encrypted using identical key.
- AppBlaster project files are encrypted using identical key.

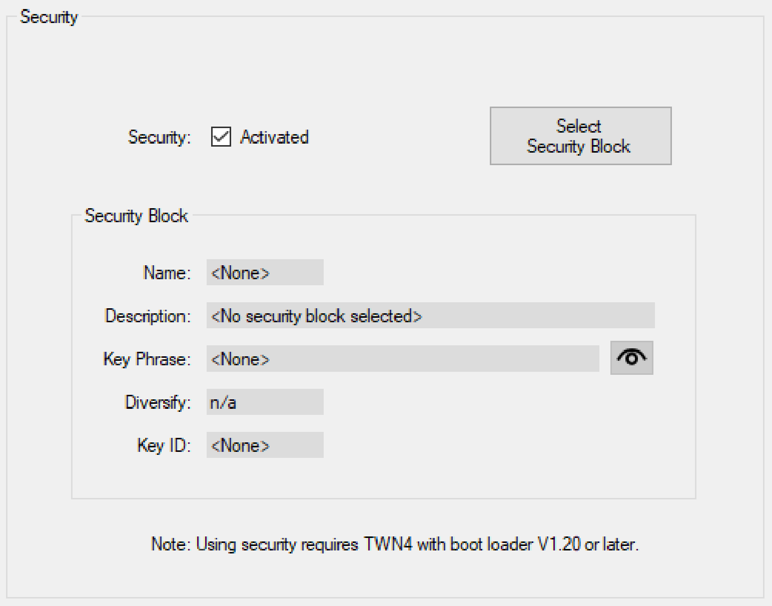
By default, the security dialog of a project looks like below:



Security: □ Activated

Note: Using security requires TWN4 with boot loader V1.20 or later.

In order to turn on security, mark the check box "Activated"



Security: ☑ Activated

Name: <None>

Description: <No security block selected>

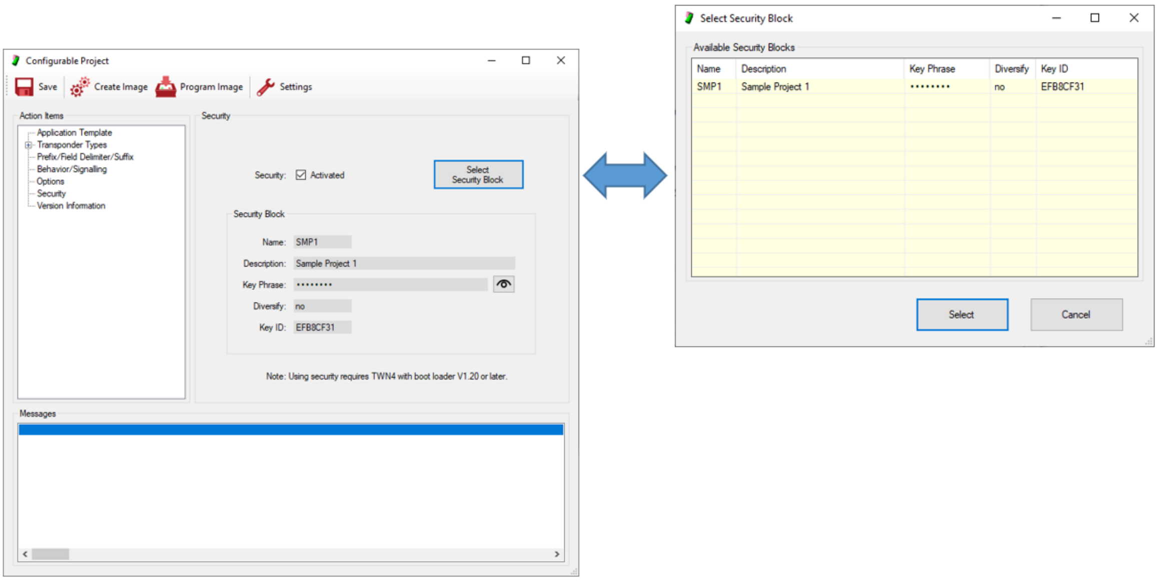
Key Phrase: <None>

Diversify: n/a

Key ID: <None>

Note: Using security requires TWN4 with boot loader V1.20 or later.

In the second step, select desired Security block. This is achieved by



Security: ☑ Activated

Name: SMP1

Description: Sample Project 1

Key Phrase: •••••••••

Diversify: no

Key ID: EFB8CF31

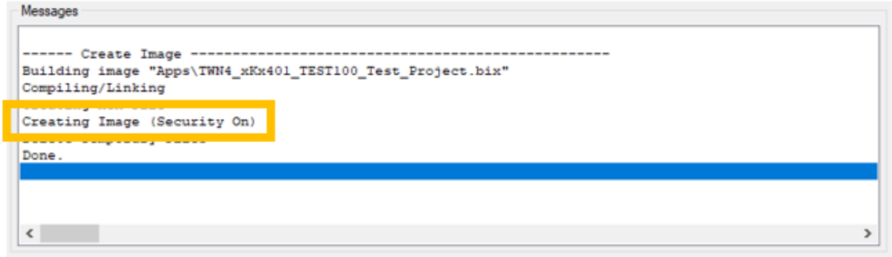
Note: Using security requires TWN4 with boot loader V1.20 or later.

Name	Description	Key Phrase	Diversify	Key ID
SMP1	Sample Project 1	•••••••••	no	EFB8CF31

This is everything before generating either firmware image or CONFIG Card.

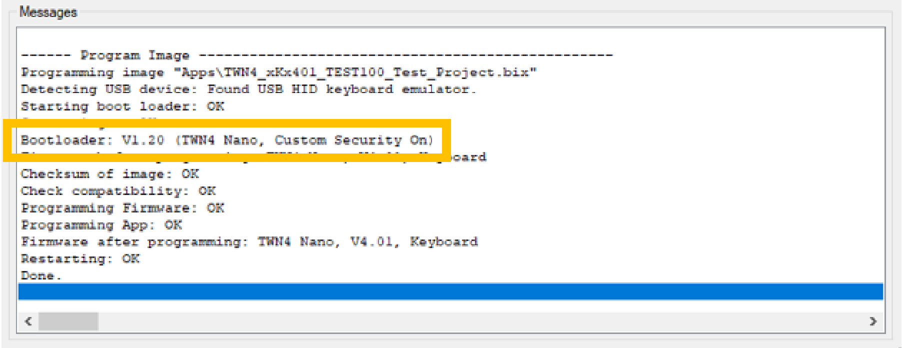
8.1 Creating a Firmware Image for TWN4

There is no difference in the steps for creation of a secured or non-secured image. During compilation of a configuration, following messages appear:



```
------ Create Image --------------------------------------------------
Building image "Apps\TWN4_xKx401_TEST100_Test_Project.bix"
Compiling/Linking
Creating Image (Security On)
Done.
```

Remarkably, creating image is displayed as "Creating Image (Security On)".

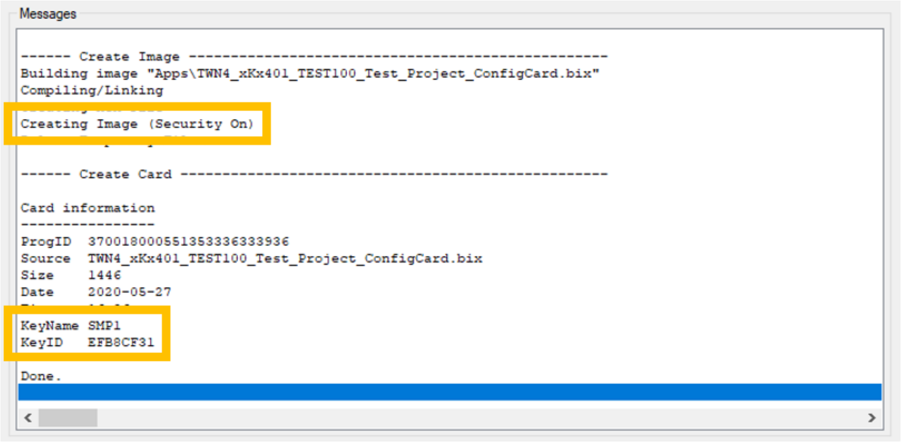


```
------ Program Image -------------------------------------------------
Programming image "Apps\TWN4_xKx401_TEST100_Test_Project.bix"
Detecting USB device: Found USB HID keyboard emulator.
Starting boot loader: OK
Bootloader: V1.20 (TWN4 Nano, Custom Security On)
Checksum of image: OK
Check compatibility: OK
Programming Firmware: OK
Programming App: OK
Firmware after programming: TWN4 Nano, V4.01, Keyboard
Restarting: OK
Done.
```

During programming, appropriate operation mode of TWN4 is detected. With Device Security turned on in TWN4, the message "Custom Security On" is displayed.

8.2 Creating a CONFIG Card for TWN4

There is also no difference in the steps for creation of a secured or non-secured CONFIG Card. During compilation of a configuration, following messages appear:



Messages

```
------ Create Image ---------------------------------------------------
Building image "Apps\TWN4_xKx401_TEST100_Test_Project_ConfigCard.bix"
Compiling/Linking

Creating Image (Security On)

------ Create Card ----------------------------------------------------

Card information
----------------
ProgID  370018000551353336333936
Source  TWN4_xKx401_TEST100_Test_Project_ConfigCard.bix
Size    1446
Date    2020-05-27

KeyName SMP1
KeyID   EFB8CF31

Done.
```

Noticeable difference during configuration again is "Creating Image (Security On)".

Card information is extended by two lines, which contain Key Name and Key ID. This information can be read back from the card at any time in order to determine purpose of the specific card.

9 Disclaimer

ELATEC reserves the right to change any information or data in this document without prior notice. The distribution and the update of this document is not controlled. ELATEC declines all responsibility for the use of product with any other specifications but the ones mentioned above. Any additional requirement for a specific custom application has to be validated by the customer himself at his own responsibility. Where application information is given, it is only advisory and does not form part of the specification.

All referenced brands, product names, service names and trademarks mentioned in this document are the property of their respective owners.