

UTILIZING i.MX RT10XX SECURE BOOT

With PEmicro Production Programming

Kevin Perreault, President, PEmicro
Clark Jarvis, MCUXpresso Ecosystem
Product Marketer, NXP
MARCH 2021



SECURE CONNECTIONS
FOR A SMARTER WORLD



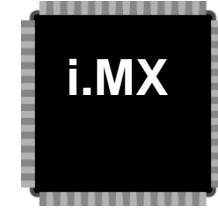
PUBLIC

NXP, THE NXP LOGO AND NXP SECURE CONNECTIONS FOR A SMARTER WORLD ARE TRADEMARKS OF NXP B.V.
ALL OTHER PRODUCT OR SERVICE NAMES ARE THE PROPERTY OF THEIR RESPECTIVE OWNERS. © 2021 NXP B.V.



FEATURES OF CYCLONE NXP I.MX RT10XX PROGRAMMING

- **Simple i.MX RT10xx security configuration**
- **Supported i.MX RT10xx device protections**
 - Boot authorized code only
 - Flash secured against copying\inspection
 - Sensitive fuses protected against reading
 - Secure access to i.MX devices after programming
- **Automatic sign and encrypt operations during SAP image build**
- **Data security maintained through the manufacturing process**



PRODUCTION PROGRAMMING TOPICS

- Cyclone Programmer – Introduction and Security
- i.MX RT10xx Security Features
- i.MX RT10xx Configuration with Secure Boot Utility
- Programming and Security Workflow Overview
- Demonstration

Cyclone Programmer Introduction and Security



SECURE CONNECTIONS
FOR A SMARTER WORLD

PUBLIC

NXP, THE NXP LOGO AND NXP SECURE CONNECTIONS FOR A SMARTER WORLD ARE TRADEMARKS OF NXP B.V.
ALL OTHER PRODUCT OR SERVICE NAMES ARE THE PROPERTY OF THEIR RESPECTIVE OWNERS. © 2021 NXP B.V.



CYCLONE OVERVIEW : STAND-ALONE PROGRAMMER

- Can Operate Independent of a Computer
- Target Programming Connections
 - BDM, JTAG, SWD, USB, etc.
- Consumes Production Programming Images
- Controllable from the PC (Ethernet, USB, Serial)
- Powerful SDK for automation
- Secure System for storing programming data



CYCLONE OVERVIEW : STAND-ALONE PROGRAMMING (SAP) IMAGES

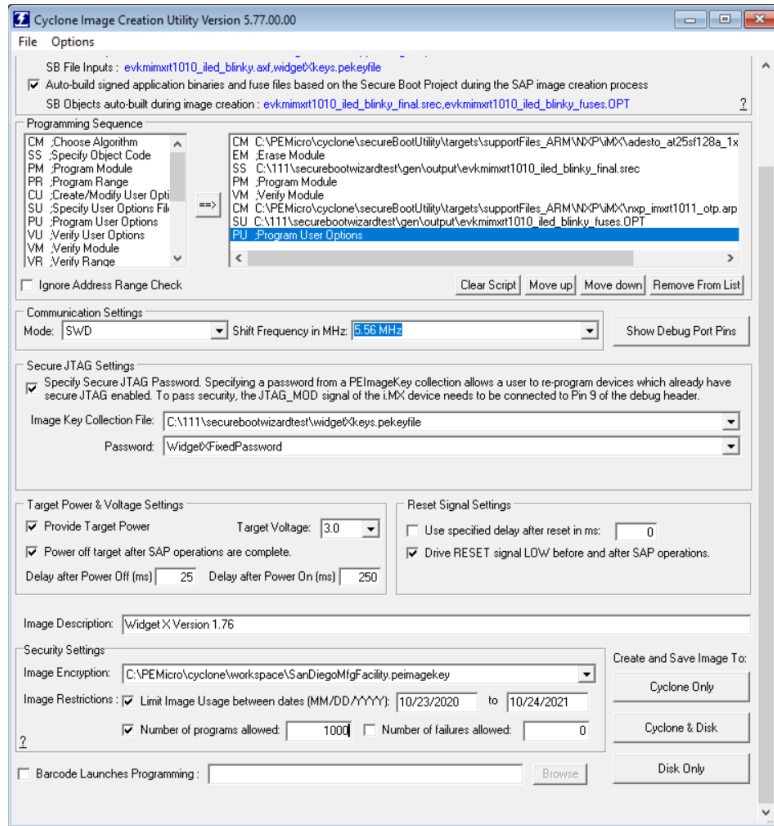
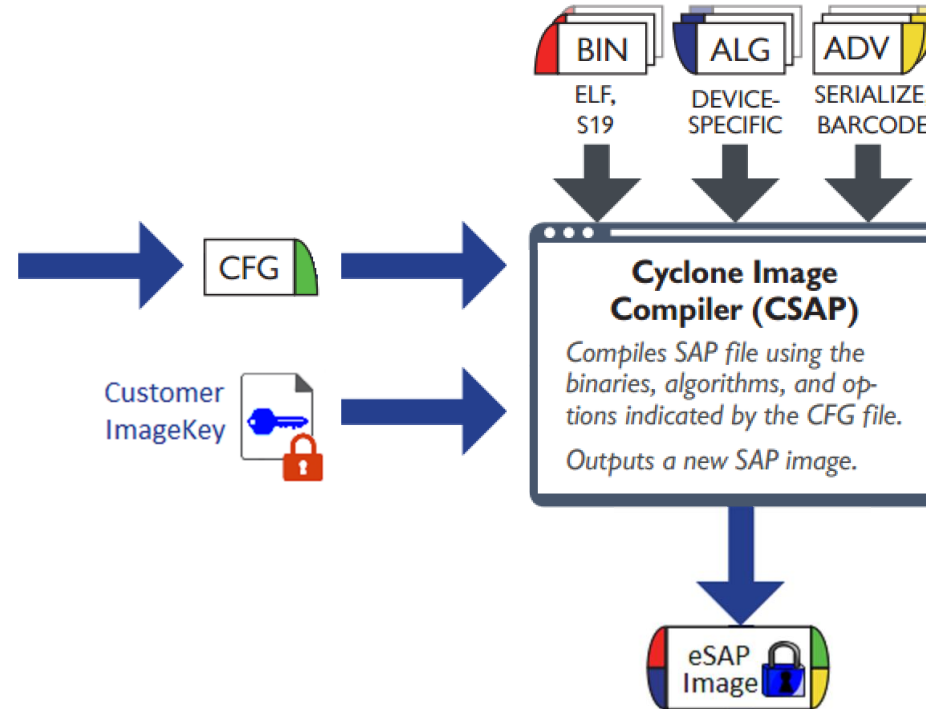
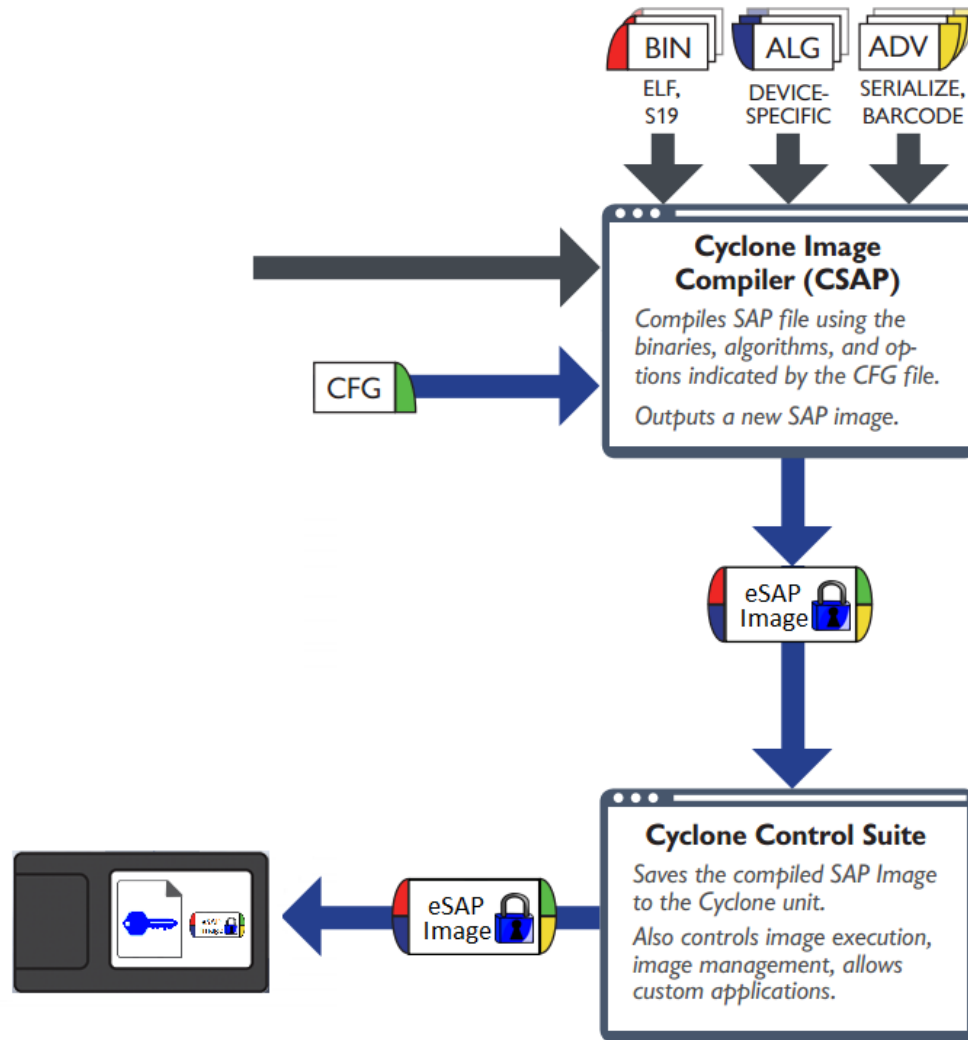


Image Creation Utility



CYCLONE SECURITY : IMAGE ENCRYPTION



Infrequent Events :

- ImageKey Creation
- Storing ImageKey to Cyclones

Frequent Events :

- Building Encrypted Images (eSAPs)
- Storing eSAPs to Cyclones



i.MX RT10xx Security Features



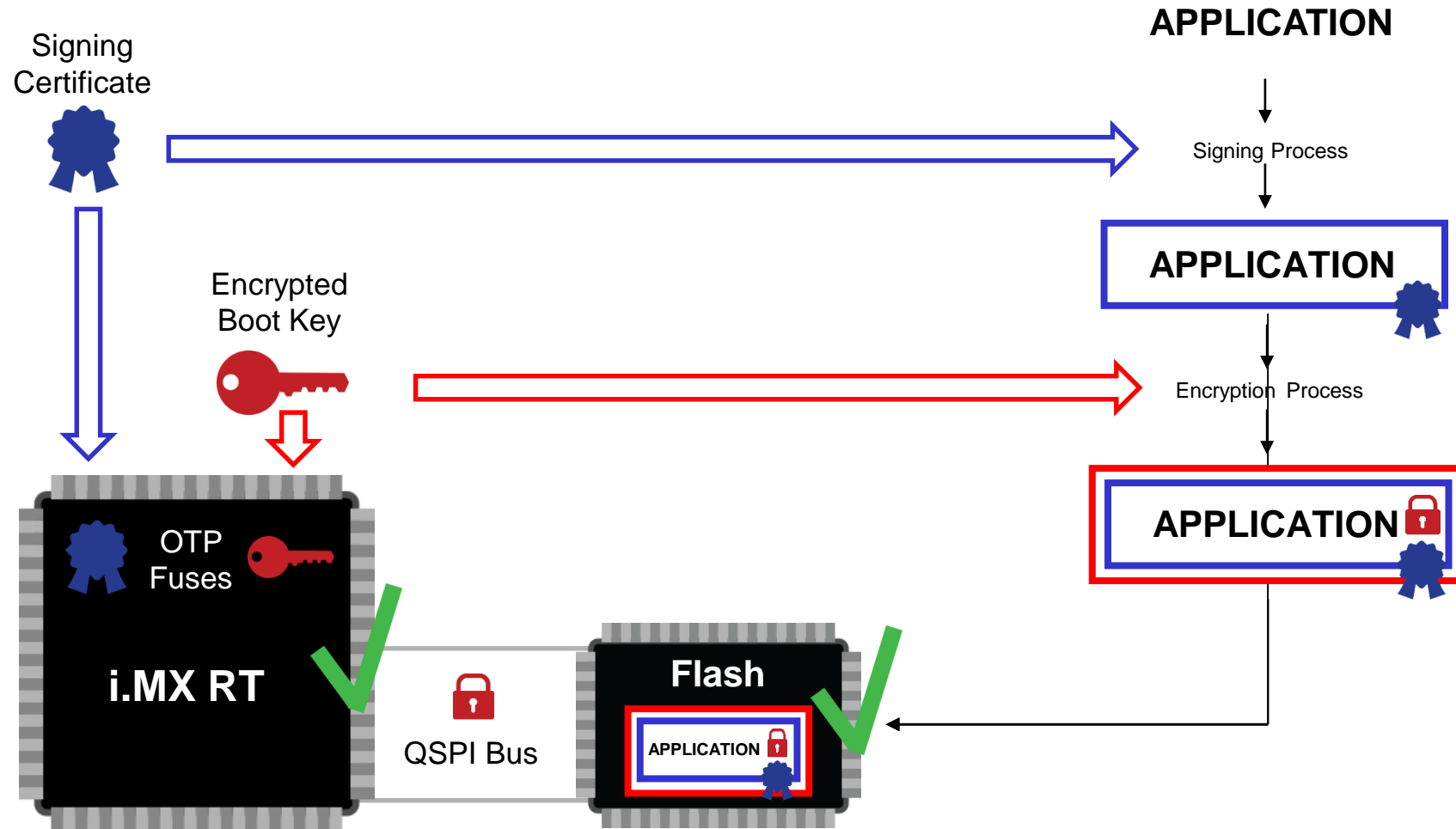
SECURE CONNECTIONS
FOR A SMARTER WORLD

PUBLIC

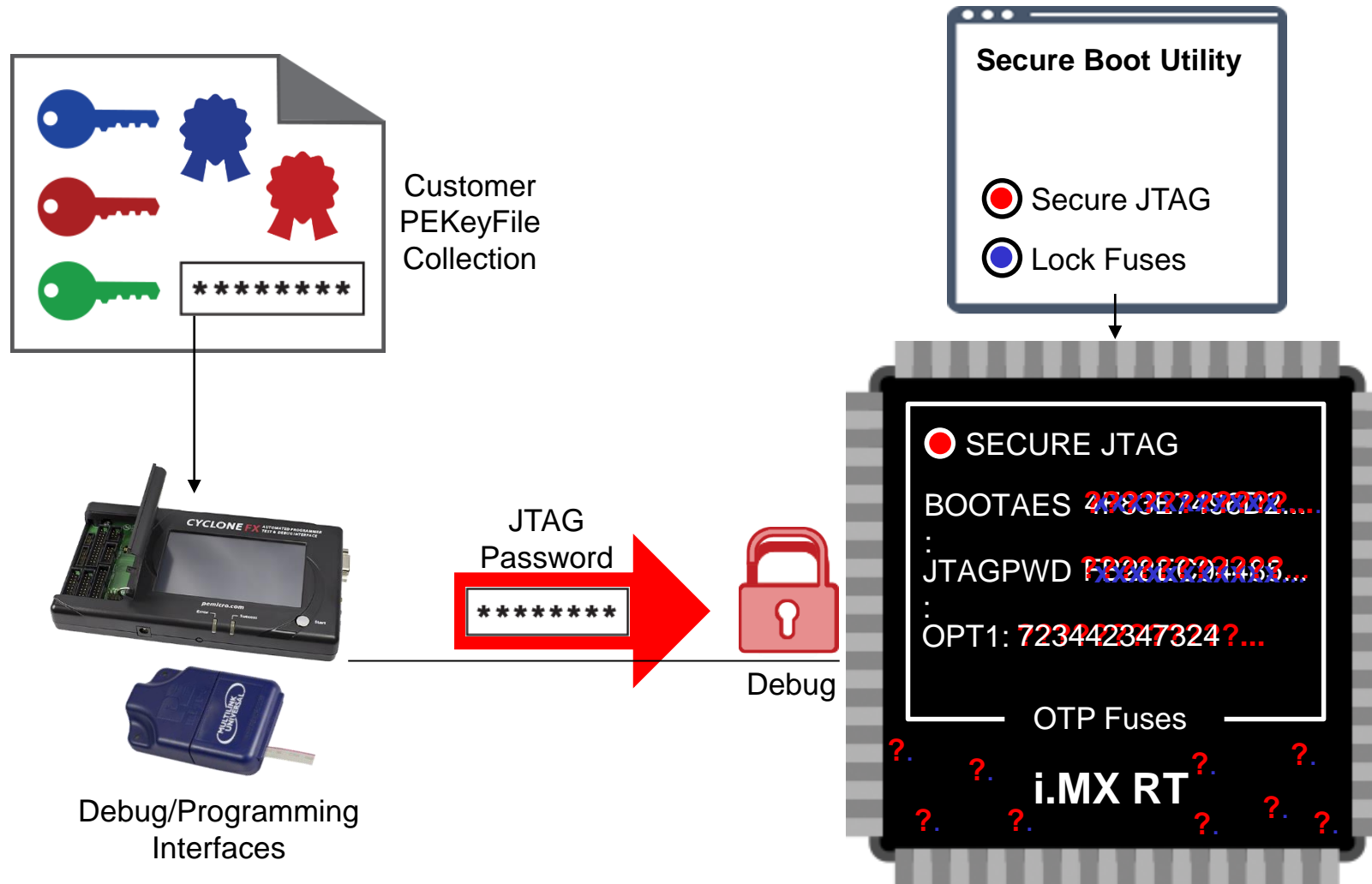
NXP, THE NXP LOGO AND NXP SECURE CONNECTIONS FOR A SMARTER WORLD ARE TRADEMARKS OF NXP B.V.
ALL OTHER PRODUCT OR SERVICE NAMES ARE THE PROPERTY OF THEIR RESPECTIVE OWNERS. © 2021 NXP B.V.



SIGNING AND ENCRYPTING I.MX APPLICATIONS



SECURE JTAG



Secure Boot Utility



SECURE CONNECTIONS
FOR A SMARTER WORLD

PUBLIC

NXP, THE NXP LOGO AND NXP SECURE CONNECTIONS FOR A SMARTER WORLD ARE TRADEMARKS OF NXP B.V.
ALL OTHER PRODUCT OR SERVICE NAMES ARE THE PROPERTY OF THEIR RESPECTIVE OWNERS. © 2021 NXP B.V.



IMAGE CREATION UTILITY: SECURE BOOT UTILITY INTEGRATION



Secure Boot Project (.SPB) File



Cyclone Image Creation Config

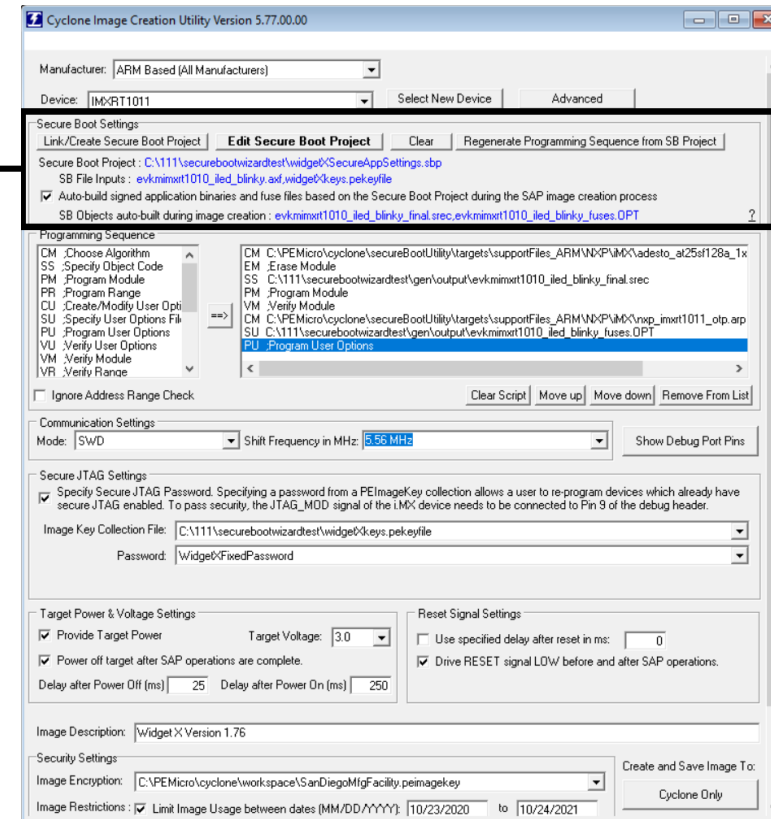
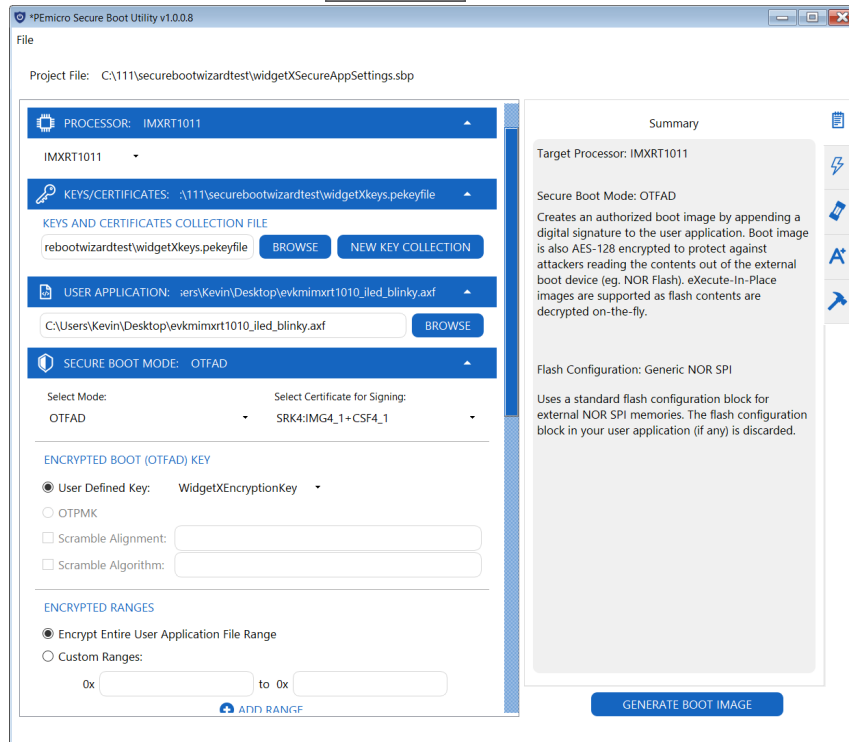


IMAGE CREATION : SECURE BOOT UTILITY

*PEmicro Secure Boot Utility v1.0.0.8

File

Project File: C:\111\securebootwizardtest\widgetXSecureAppSettings.sbp

PROCESSOR: IMXRT1011

IMXRT1011

KEYS/CERTIFICATES: \111\securebootwizardtest\widgetXkeys.pekeyfile

KEYS AND CERTIFICATES COLLECTION FILE

rebootwizardtest\widgetXkeys.pekeyfile BROWSE NEW KEY COLLECTION

USER APPLICATION: :ers\Kevin\Desktop\evkmimxrt1010_iled_blinky.axf

C:\Users\Kevin\Desktop\evkmimxrt1010_iled_blinky.axf BROWSE

SECURE BOOT MODE: OTFAD

Select Mode: OTFAD Select Certificate for Signing: SRK4:IMG4_1+CSF4_1

ENCRYPTED BOOT (OTFAD) KEY

User Defined Key: WidgetXEncryptionKey

OTPMK

Scramble Alignment:

Scramble Algorithm:

ENCRYPTED RANGES

Encrypt Entire User Application File Range

Custom Ranges:

0x to 0x

+ ADD RANGE

Summary

Target Processor: IMXRT1011

Secure Boot Mode: OTFAD

Creates an authorized boot image by appending a digital signature to the user application. Boot image is also AES-128 encrypted to protect against attackers reading the contents out of the external boot device (eg. NOR Flash). eXecute-In-Place images are supported as flash contents are decrypted on-the-fly.

Flash Configuration: Generic NOR SPI

Uses a standard flash configuration block for external NOR SPI memories. The flash configuration block in your user application (if any) is discarded.

GENERATE BOOT IMAGE

SECURE BOOT UTILITY: SECURITY SETTINGS

SECURE BOOT MODE: OTFAD

Select Mode: **OTFAD** | Select Certificate for Signing: **SRK1:IMG1_1+CSF1_1**

ENCRYPTED BOOT (OTFAD) KEY

User Defined Key: WidgetXEncryptionKey

SECURITY OPTIONS

Security Configuration :	Closed
Lock Fuses :	Yes
JTAG Security :	Secure JTAG
Secure JTAG Response Password :	WidgetXFixedPassword

Signed

Encrypted

JTAG Password

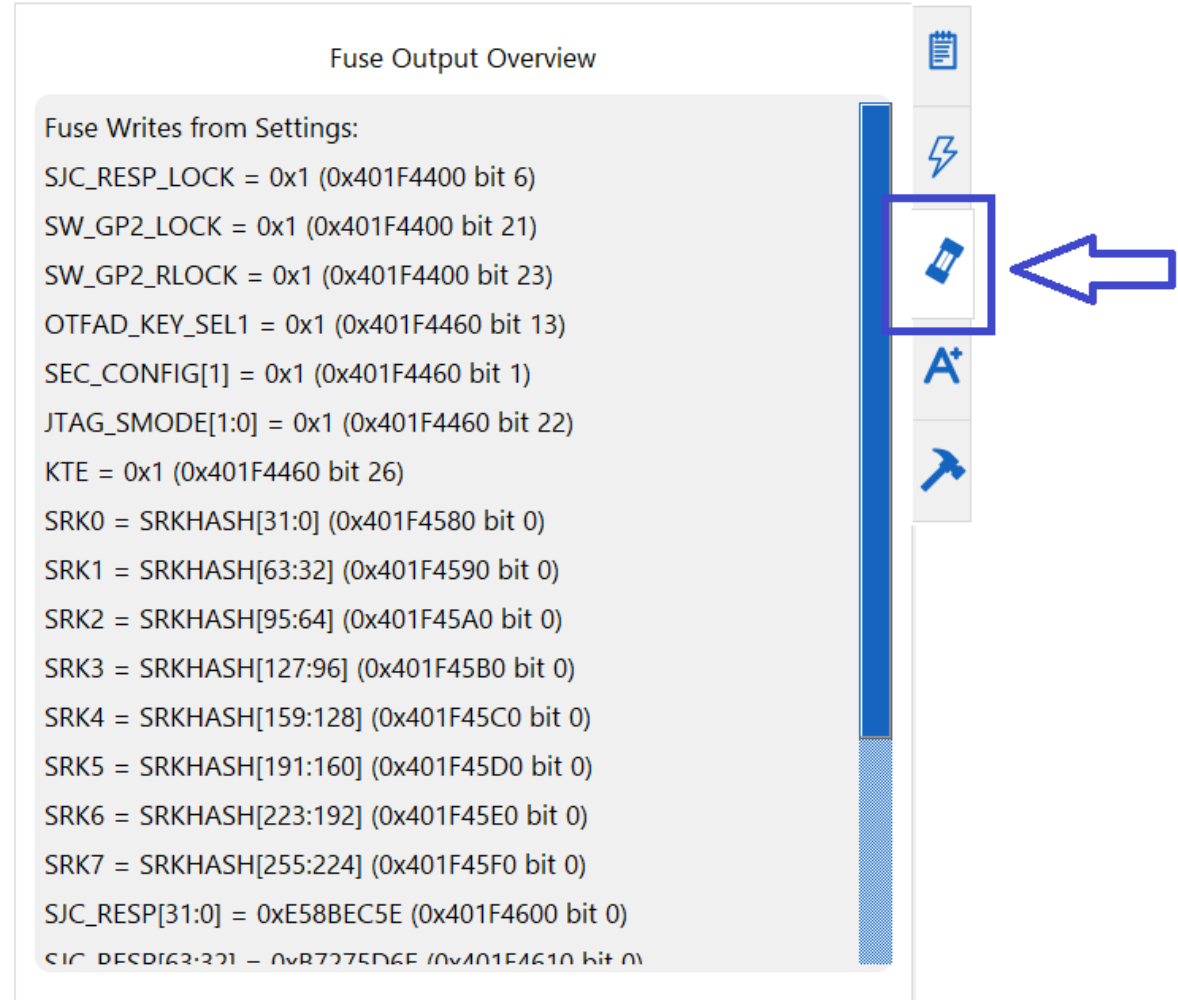
Fuses Locked

SECURE BOOT UTILITY: FUSE OUTPUT

Fuse Output Overview

Fuse Writes from Settings:

- SJC_RESP_LOCK = 0x1 (0x401F4400 bit 6)
- SW_GP2_LOCK = 0x1 (0x401F4400 bit 21)
- SW_GP2_RLOCK = 0x1 (0x401F4400 bit 23)
- OTFAD_KEY_SEL1 = 0x1 (0x401F4460 bit 13)
- SEC_CONFIG[1] = 0x1 (0x401F4460 bit 1)
- JTAG_SMODE[1:0] = 0x1 (0x401F4460 bit 22)
- KTE = 0x1 (0x401F4460 bit 26)
- SRK0 = SRKHASH[31:0] (0x401F4580 bit 0)
- SRK1 = SRKHASH[63:32] (0x401F4590 bit 0)
- SRK2 = SRKHASH[95:64] (0x401F45A0 bit 0)
- SRK3 = SRKHASH[127:96] (0x401F45B0 bit 0)
- SRK4 = SRKHASH[159:128] (0x401F45C0 bit 0)
- SRK5 = SRKHASH[191:160] (0x401F45D0 bit 0)
- SRK6 = SRKHASH[223:192] (0x401F45E0 bit 0)
- SRK7 = SRKHASH[255:224] (0x401F45F0 bit 0)
- SJC_RESP[31:0] = 0xE58BEC5E (0x401F4600 bit 0)
- SJC_RESP[63:32] = 0x87275D6E (0x401F4610 bit 0)



SECURE BOOT UTILITY: SECURITY ANALYSIS

Security Overview

- Prevents unauthorized code from executing: Yes
 - Processor Closed: Yes
- Prevents unauthorized debug access: Yes
 - JTAG Security: Secure JTAG
- Prevents reading of plaintext code from external flash: Yes
 - User application encrypted: Yes
- Prevents unauthorized duplication of system: Yes
 - User application is encrypted: Yes
- Secure boot fuses locked: Yes

During development, it is not necessary to protect against all security vulnerabilities. For production programming, any outstanding vulnerabilities should be evaluated.


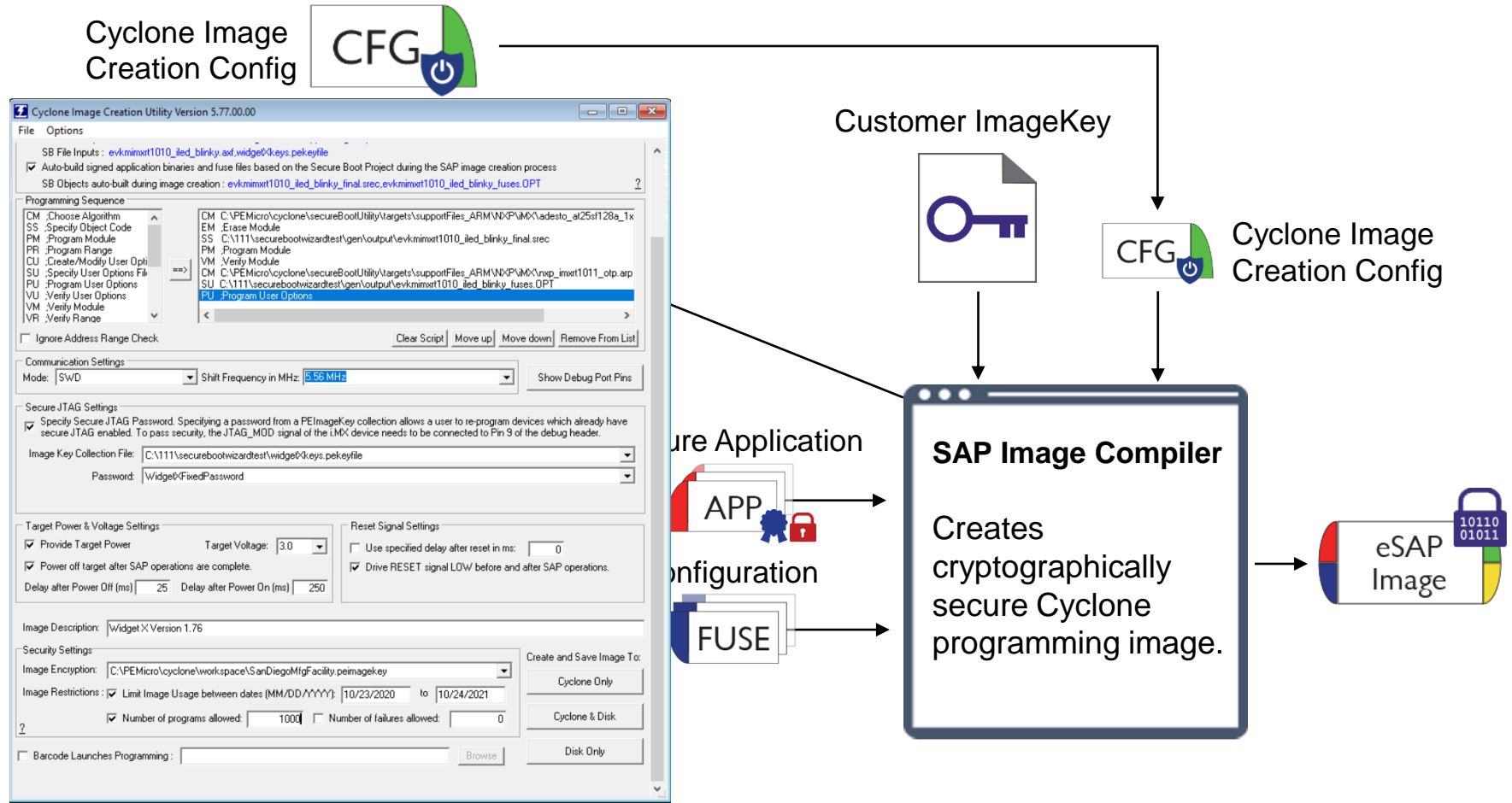


IMAGE CREATION PROCESS: SECURE BOOT BUILD



Programming and Security Workflow



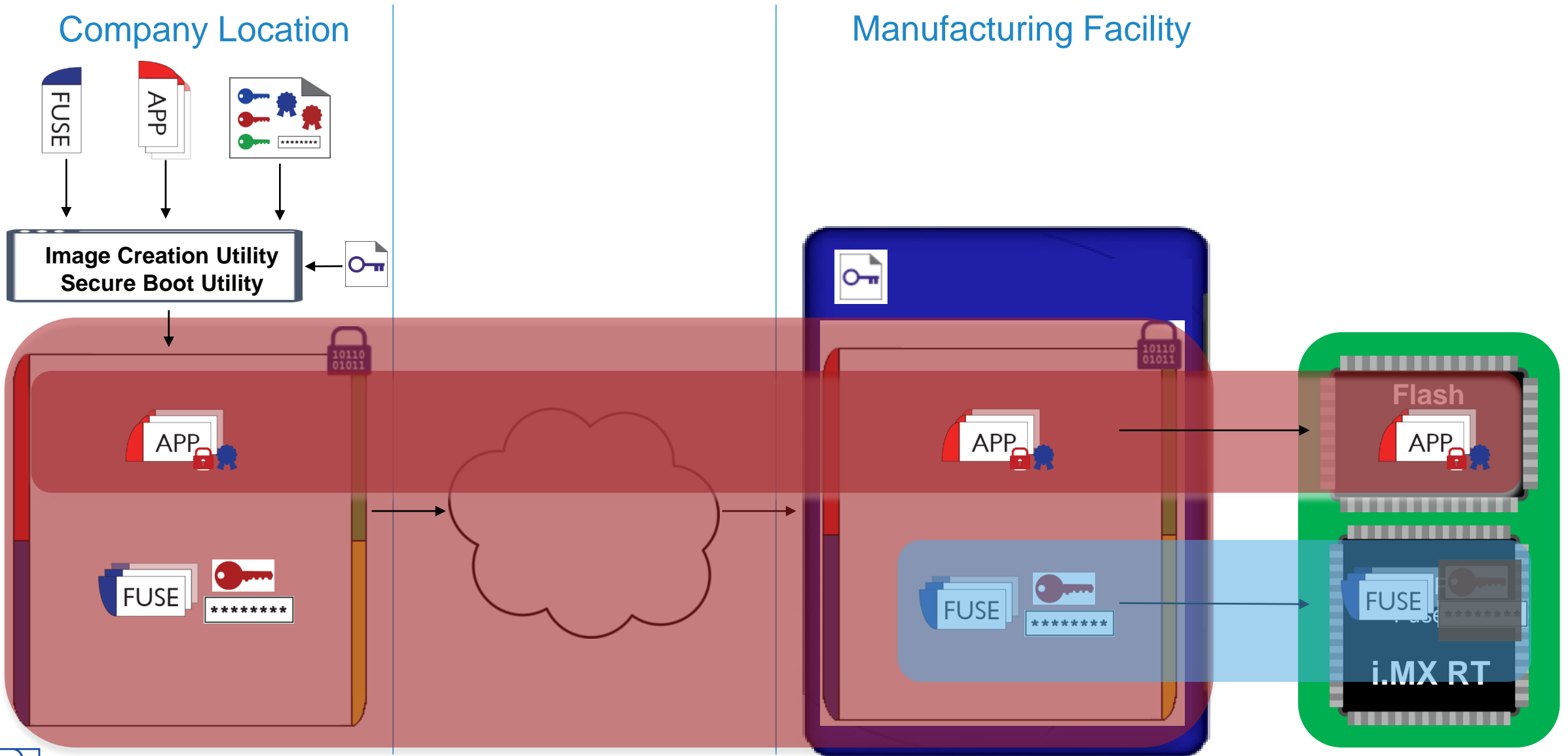
SECURE CONNECTIONS
FOR A SMARTER WORLD

PUBLIC

NXP, THE NXP LOGO AND NXP SECURE CONNECTIONS FOR A SMARTER WORLD ARE TRADEMARKS OF NXP B.V.
ALL OTHER PRODUCT OR SERVICE NAMES ARE THE PROPERTY OF THEIR RESPECTIVE OWNERS. © 2021 NXP B.V.



PROGRAMMING AND SECURITY FLOW



Demonstration



SECURE CONNECTIONS
FOR A SMARTER WORLD

PUBLIC

NXP, THE NXP LOGO AND NXP SECURE CONNECTIONS FOR A SMARTER WORLD ARE TRADEMARKS OF NXP B.V.
ALL OTHER PRODUCT OR SERVICE NAMES ARE THE PROPERTY OF THEIR RESPECTIVE OWNERS. © 2021 NXP B.V.





SECURE CONNECTIONS
FOR A SMARTER WORLD