R9A02G011/R9J02G012

Firmware development guide for USB Type-C™ Authentication

Introduction

This document describes the method of firmware development for Renesas USB Type-C Authentication (C-Auth) device.

Target Device

R9J02G012, R9A02G011 with R5H30313XB08

Contents

1. Overview

This document guides the firmware development method for USB Type-C Authentication (C-Auth) on Renesas USB Power Delivery (USB PD) controller. Renesas USB PD controller has a Flash ROM. User can define a behavior of the USB PD controller. This document provides information to develop the firmware for C-Auth on Renesas USB PD controller.

Renesas provides 2 firmware development tools, the flash memory image data generator software (PDC-IMGGEN) and Renesas software development kit (SDK). User can choose one development tool to develop the firmware. This document describes how a user develops firmware for C-Auth for each software development tool.

The document also describes the debug method for C-Auth firmware. Renesas provides 2 debugging tools, USB PD exerciser on RTK-251-DRPEVB, and C-Auth test suite. User can confirm the firmware behavior by sending commands from the USB PD exerciser. C-Auth test suite provides the features for C-Auth compliance test.

1.1 Related Documents

Use this document in combination with the following documents.

The related documents indicated in this publication may include preliminary versions. However, preliminary versions are not marked as such.

- Universal Serial Bus Power Delivery Specification Revision 3.0
- Universal Serial Bus Type-C Cable and Connector Specification Revision 1.3
- Universal Serial Bus Power Delivery Firmware Update Specification Revision 1.0
- Universal Serial Bus Type-C Authentication Specification Revision 1.0

- R9A02G011 Data Sheet: R19DS0088EJ
- R9A02G011 User’s Manual: R19UH01202EJ
- R9J02G012 Data Sheet: R19DS0097EJ
- R9J02G012 User’s Manual: R19UH0107EJ
- R5H30313XB08 Data sheet: R01DS0314EJ

- R9A02G011/R9J02G012 Flash memory Programming Guide: R19AN0060EJ
- Renesas Flash Programmer V3.05 Flash memory programming software User’s Manual: R20UT4307
- Flash memory image data generator software G011/G012 edition (PDC-IMGGEN): BCD-ISG-19-5015
- R9A02G011/R9J02G012 Application Note (Using SMBus Slave Interface): R19AN0062EJ

- Renesas SDK Application note: BCD-ISG-19-5024
- Renesas-SDK for IAR EWRL78 Application note: BCD-ISG-19-5026
- Renesas-SDK Application note for Auth: BCD-ISG-19-5028
- Renesas USB PDC SDK IAR EWRL78 Application note for AUTH: BCD-ISG-19-5029

- C-authTestSuite ApplicationNote: BCD-ISG-17-5066
- C-authTestSuite InstructionManual: BCD-ISG-17-5067
- Renesas USB PDC Exerciser User's Manual: BCD-IMB-19-5000

1.2 Development environment

1.2.1 Hardware

- Evaluation board: RTK-251-DRPEVB, RTK-251-BuckBoostConveter2, RTK-251-1PowerBank3
- Flash writer tool: E1/E2 lite emulator, ET-D720251-0005, RTK-251-DRPEVB
- Cable: USB Type-C cable, USB Micro-B cable
- Other: PC, 19V AC adapter

1.2.2 Software

Renesas provides 2 methods to develop Main FW for R9A02G011/R9J02G012: image generator (PDC-IMGGEN) and Renesas software development kit (SDK).

PDC-IMGGEN requires the following software to develop C-Auth firmware.

- PDC-Image generator

Renesas USB PD SDK requires following software to develop C-Auth firmware.

- Renesas USB PD SDK
- Integrated Development Environment (IDE): CS+, or EWRL78

Following software may prove useful.

- USB Type-C Authentication Functional Test Application (C-Auth Test Suite) ver. 1.20 or later

1.2.3 R9A02G011/R9J02G012 memory map

R9A02G011/R9J02G012 requires a boot firmware (Boot FW). The Boot FW initializes USB PD controller, writes a main firmware in the code flash memory from 02000H to 0FFFFH, and updates the main firmware via USB Type-C programming interface. The 8 KB code flash memory from 00000H to 01FFFH includes the Boot FW. Please refer to the chapter 2 in the R9A02G011/R9J02G012 Flash memory Programming Guide.

1.3 Evaluation board

Renesas provides some evaluation/reference boards for C-Auth. Table 1-1 describes each board’s features.

Table 1-1 Renesas evaluation/reference boards for C-Auth

Part name	Authentication configuration (Shipped out configuration)	Power role	Description
RTK-251-DRPEVB	Initiator/Responder (Initiator in Sink)	DRP	Evaluation board for Renesas USB PD SDK for generic DRP.
RTK-251-BuckBoostConveter2	Initiator/Responder (Responder in Source)	Source	Reference board for a DCDC module supporting programmable power supply (PPS).
RTK-251-1PowerBank3	Initiator/Responder (Responder in Source)	DRP Try.SRC	Reference board for a power bank module supporting PPS.
RTK-252-Paddle Card	Responder for Cable Plug	eMarker	Reference board for an eMarker in a cable.

1.4 Comparison with Image generator and SDK

Renesas provides 2 methods to develop Main FW for R9A02G011/R9J02G012: image generator (PDC-IMGGEN) and SDK. Table 1-2 shows a comparison between PDC-IMGGEN and SDK.

Please refer to each application note, Flash memory image data generator software G011/G012 edition (PDC-IMGGEN), Renesas SDK Application note, and Renesas-SDK Application note for Auth details.

Table 1-2 Comparison with PDC-IMGGEN and SDK

Item	PDC-IMGGEN	SDK (including sample code) [Note]
Supported power role	Source/Sink/DRP/eMarker	Source/Sink/DRP
Supported Authentication	Initiator/Responder	Initiator/Responder
Supported DCDC	General DCDC/RAA230161/ ISL95338 (output from Vsys)/ ISL95538B	ISL95338/ISL95538B/ ISL9241[Note 2]
GPIO behavior	Defined	Free
Behavior after authentication	Defined	Free

Note: SDK enables any function regarding USB PD, and C-Auth. And SDK also enables user defined GPIO/analog pin behavior.

Note 2: No sample code supports the C-Auth.

An external controller for R9A02G011/R9J02G012 can initiate installation of firmware generated by PDC-IMGGEN. However, the external controller for R9A02G011/R9J02G012 cannot initiate installation of firmware generated by SDK. SDK firmware supports no SMBus Slave interface for C-Auth, such as the “try authentication” command and “send secure request message” command.

1.5 USB Type-C Authentication (C-Auth)

C-Auth has 2 roles, Initiator and Responder. Figure 1-1 shows examples of Initiator and Responder. An initiator tries to authenticate a responder. In the example, responders are cable and PD source device. However, PD sink device may be an initiator and PD source device may be a responder.

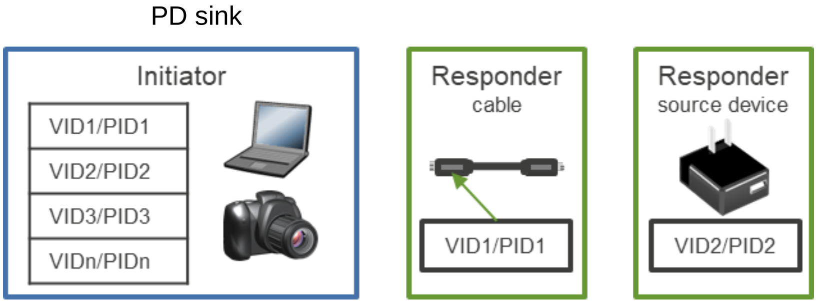


Figure 1-1 Initiator/Responder devices

Figure 1-2 C-Auth steps describe the authentication sequences:

1. 5V contract with cable and source device
2. Cable authentication
3. Source device authentication
4. PDOn (n>1) contract with source device to charge

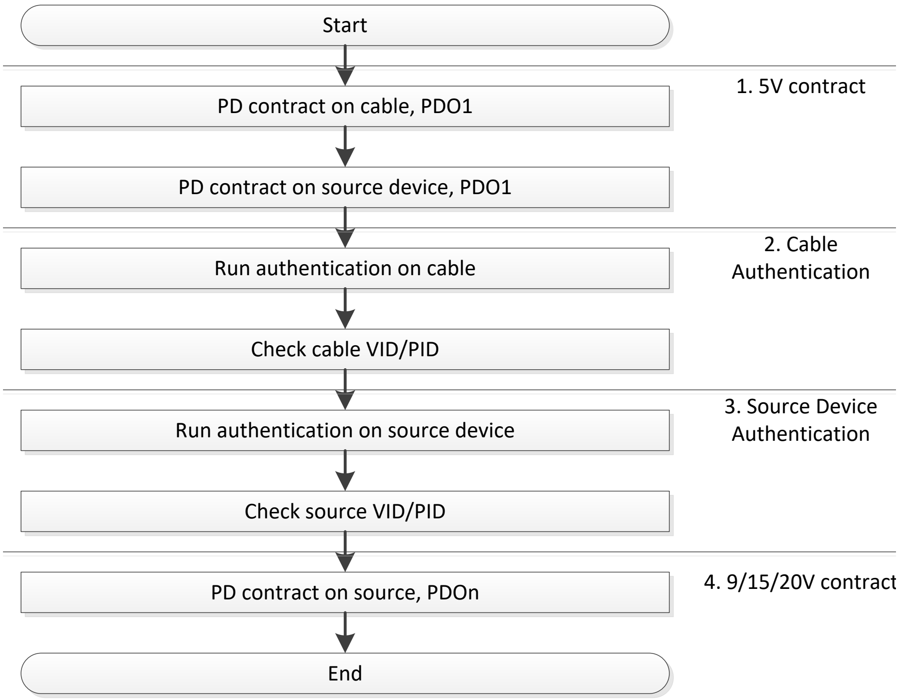

Start
PD contract on cable, PDO1
PD contract on source device, PDO1
Run authentication on cable
Check cable VID/PID
Run authentication on source device
Check source VID/PID
PD contract on source, PDOn
End
1. 5V contract
2. Cable Authentication
3. Source Device Authentication
4. 9/15/20V contract

Figure 1-2 C-Auth steps

The sequences execute as follows[note]:

a) Initiator

- R9A02G011/R9J02G012 automatically runs
- External controller initiates through R9A02G011/R9J02G012 SMBus Slave interface.

1. If Authentication operation of R9A02G011/R9J02G012 is enabled: External controller should send Try Authentication command.
2. If Authentication operation of R9A02G011/R9J02G012 is disabled: External controller should send Security Request message.

b) Responder

- R9A02G011/R9J02G012 automatically runs

VID/PID check is enabled/disabled independently. Cable and source device authentication are enabled/disabled independently as well.

Note: R9A02G011 with R5H30313XB08, which is an alternative C-Auth solution to R9J02G012, can also execute the above sequence.

Note 2: An initiator device should supply Vconn power as a Vconn source to authenticate a cable regardless of power role.

2. Hardware connections

This chapter describes hardware connection regarding SMBus interface and Vconn.

R9J02G012 is a single-chip solution based on R9A02G011 and R5H30313XB08. The SMBus master interface on R9A02G011 connects with the SMBus slave interface on R5H30313XB08. R9J02G012 has a crypto engine on-chip and does not use an SMBus to connect to an external crypto engine. In both cases, an external controller like an MCU can control R9A02G011/R9J02G012 through their SMBus slave interface as shown in Figure 2-3.

Initiator should supply Vconn power to authenticate a cable eMarker.

2.1 R9J02G012 connections

Please refer to chapter 3 in the R9J02G012 user's manual. Especially, C-Auth system requires the miscellaneous pins connection. In the diagrams below, note REGC and NVCC.

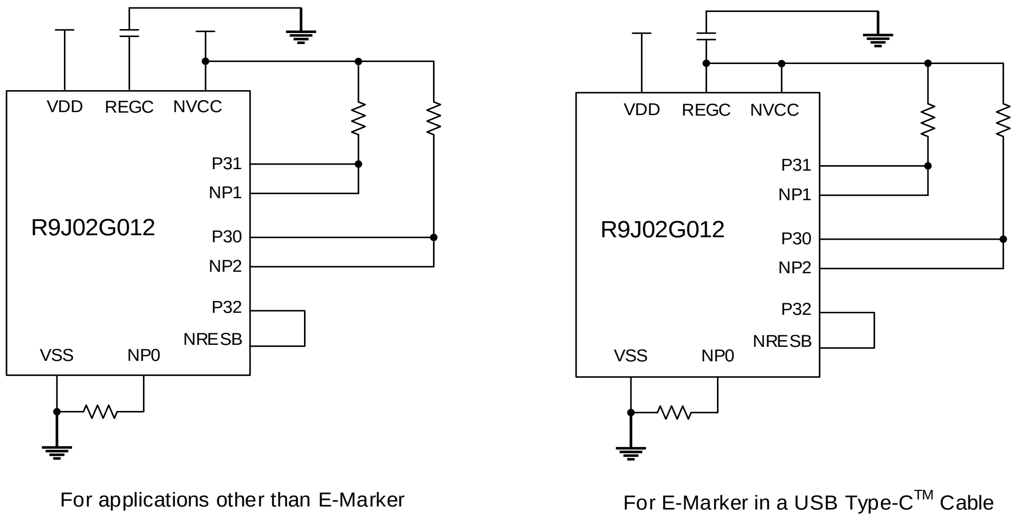


Figure 2-1 Miscellaneous Pins connections

2.2 R9A02G011 connection with R5H30313XB08

Please refer to section 3.2 SMBus Connection in the R9A02G011 user's manual and R5H30313XB08 Data sheet. R9A02G011 SMBus Master interface should connect to R5H30313XB08 SMBus Slave interface.

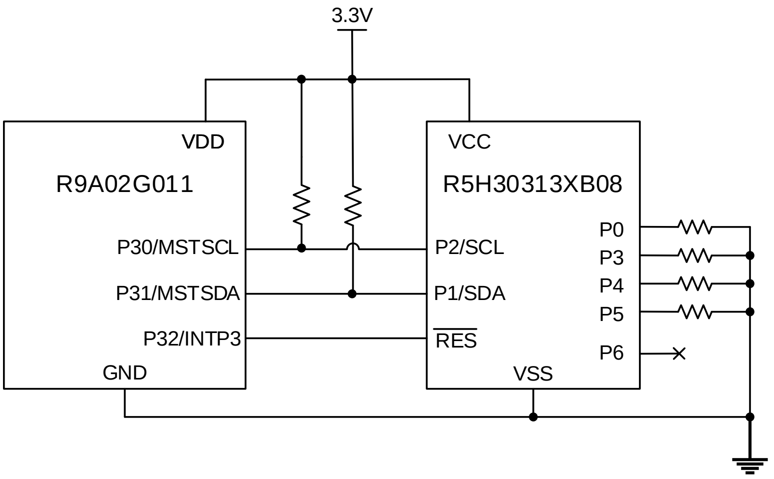


Figure 2-2 Connection example of R9A02G011 with R5H30313XB08

2.3 Connection with an external system controller

Please refer to section 1.3 Block Diagram in the R9A02G011/R9J02G012 Application Note (Using SMBus Slave Interface). The following block diagram shows the connection between the system controller and the Renesas PDC (R9A02G011/R9J02G012). SLVALTB is the alert signal and it is optional [Note]. The data communication for C-Auth can be made by using SLVSCL and SLVDA. SLVADDR1 and SLVADDR0 are the last two bits of the slave address [7:1].

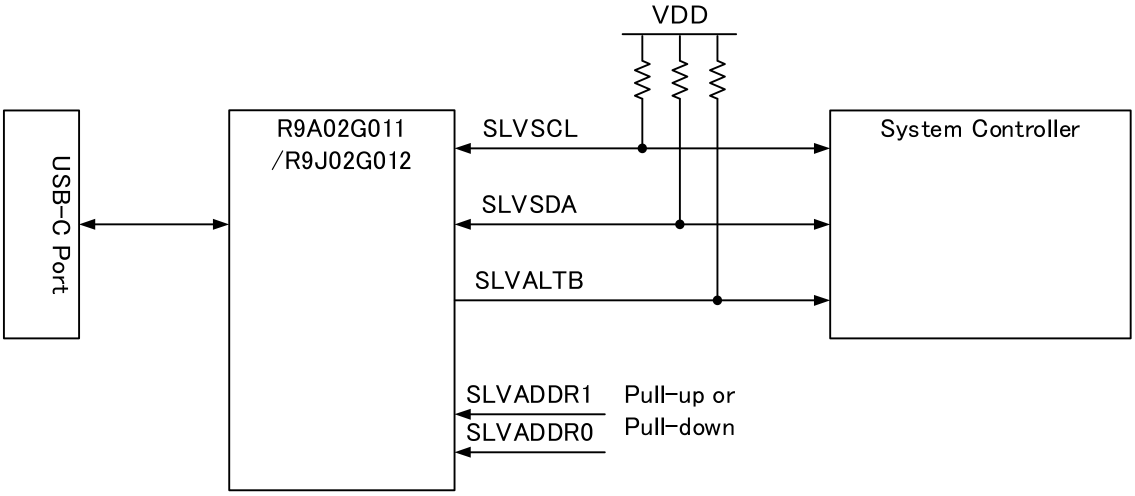


Figure 2-3 Connection with an external system controller

Note: SLVSALTB is mandatory for systems using Sleep and/or Deep Sleep Mode.

2.4 Vconn source

An initiator should supply Vconn power to authenticate a cable regardless of power role. Please refer to section 3.3 USB PD Port Connection in the R9A02G011/R9J02G012 User’s Manual.

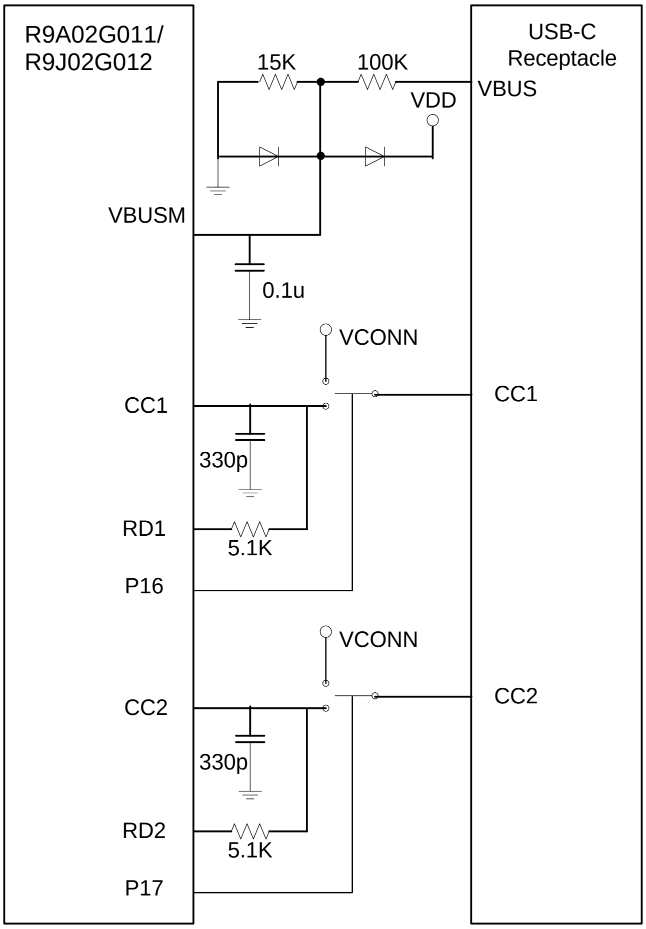


Figure 2-4 DRP (Source/Sink) or Sink Only Connection

3. Firmware development

Renesas provides 2 firmware development tools: PDC-IMGGEN and SDK. User can choose which development tool to use to develop the firmware for C-Auth. This chapter describes each development method for C-Auth.

3.1 Image Generator (PDC-IMGGEN)

PDC-IMGGEN provides the easy way to develop the C-Auth firmware. User can configure the firmware setting on the GUI based software and write the firmware into the Flash ROM on R9A02G011/R9J02G012.

Renesas provides several versions of Main FW each supporting DCDC and Authentication functions. (DCDC refers to the DC-to-DC voltage regulator.) Each Main FW supports Generic DCDC, RAA230161, ISL95338, or ISL95538B. Supported Authentication role is determined according to the Main FW version.

The Main FW versions have some GPIO behavior functions, like LED control. PDC-IMGGEN provides configuration parameters to determine behavior of GPIO pins. And PDC-IMGGEN also provides the pin assignment configuration. User can change the pin assignment according to their board design.

3.1.1 Main FW

Main FW for PDC-IMGGEN has several versions for various combinations of authentication role and supporting voltage regulator. Please refer to the release note included with USBPD-RenesasPDC-FW zip file.

3.1.2 FW parameter

PDC-IMGGEN provides configurations for determining behaviors regarding C-Auth. Table 3-1 PDC-IMGGEN configuration list regarding C-Auth, lists the configurations. These parameter items are in the Authentication Configuration of PDC-IMGGEN.

The parameter items regarding initiator will appear if user sets the Main FW supporting the initiator function at the Firmware Version in the Common.

Table 3-1 PDC-IMGGEN configuration list regarding C-Auth

Category	Parameter Items	Attributes	Descriptions
Authentication Configuration	**Responder Feature**	**Enable**	C-Auth responder mode is enabled
		Disable	C-Auth initiator mode is enabled, or C-Auth is disabled.
	Authentication Mode	**External**	Security Request/Response Messages are initiated through SMBus Slave interface. C-Auth function requires no crypto engine.
		Internal	C-Auth function requires a crypto engine with a USB PD controller. • Responder mode: It automatically responds to initiator during C-Auth sequence. • Initiator mode: It relies on “Autonomous Internal Initiator” setting.
		Disable	C-Auth is disabled. Security Request/Response message is not initiated through SMBus Slave interface.
	Auto Internally Initiator	**Enable**	R9A02G011/R9J02G012 automatically starts C-Auth sequence to the responder. The SMBus Slave interface returns no result of the C-Auth. The system realizes Authentication success by obtaining the appropriate PD power from source device.
		Disable	C-Auth start is initiated by an external controller through SMBus Slave interface.
Initiator check target	**Far source/sink**	**Check box**	Set the check mark if R9A02G011 with R5H3013XB08 or R9J02G012 authenticates the far end device. “Autonomous Internal initiator” should be enabled.
	Cable plug in sink/source	**Check box**	Set the check mark if R9A02G011 with R5H3013XB08 or R9J02G012 authenticates the cable. “Autonomous Internal initiator” should be enabled.

Note: R9A02G011 with R5H30313XB08, which is an alternative C-Auth solution to R9J02G012, can also execute above sequence.

Table 3-2 PDC-IMGGEN configuration list regarding C-Auth (continued)

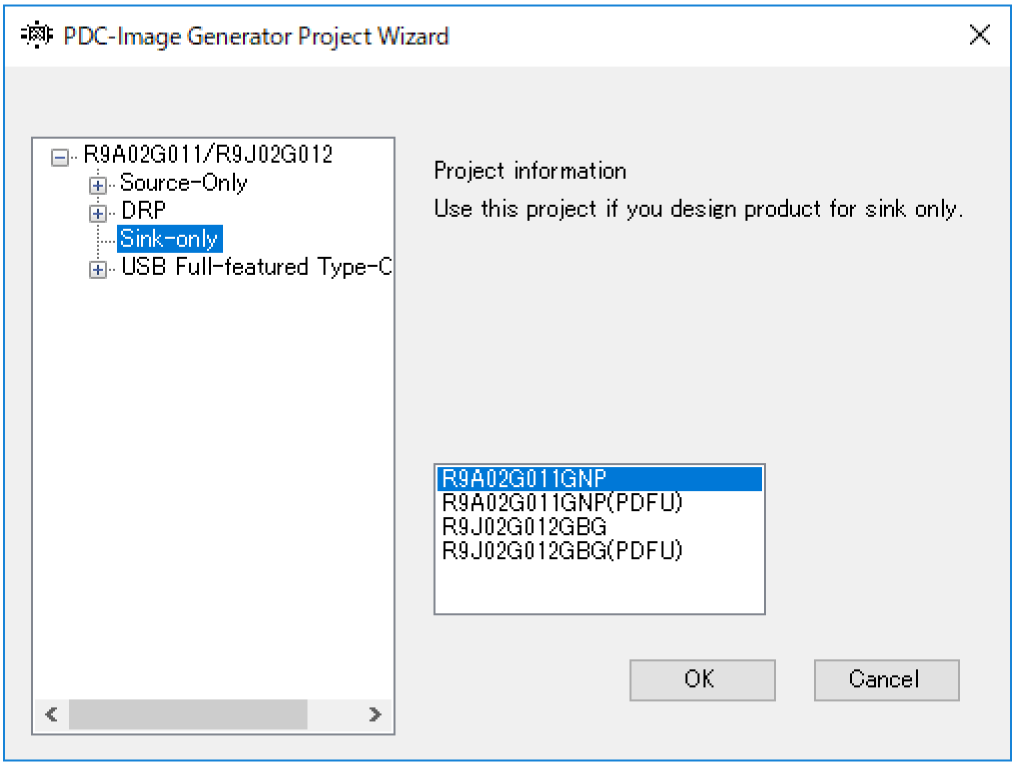
Category	Parameter Items	Attributes	Descriptions
Initiator Search Settings	**VID/PID search**	Black List Search	R9A02G011 with R5H3013XB08/R9J02G012 checks if VID/PID is on the list. When it matches, USB-C authentication fails.
		White List Search	R9A02G011 with R5H3013XB08/R9J02G012 checks if VID/PID is on the list. When it matches, USB-C authentication passes.
		Disable	R9A02G011 with R5H3013XB08/R9J02G012 doesn’t check VID/PID.
	Cache Invalidation	Disable	Use cache and run only “Digest” of authentication sequences to responders previously connected.
		Enable	Don’t use cache and always run authentication to responders.
	Slot-n search	n: 0 to 7	Set bits to 1 on the slot number to be used for C-Auth other than slot 0. C-Auth specification defines slot 0 as the default and optional slot 1 to 7 [Note].
	Number of auth devices	1 to 32	The number of devices (VID/PID) to be listed for check. It can be set for up to 32 devices.
	VIDn	n: 1 to 32	VID value for 32 devices
	PIDn	n: 1 to 32	PID value for 32 devices

Note: Slot 0 to 3 is used by USB-IF and only slot 0 is occupied for the existing usage.

3.1.3 Image Generator operations

3.1.3.1 Configuration

Execute "PDC-IMGGEN". Click File->New in the menu bar. The project wizard window appears (Figure 3-1 Project Wizard window). Select power role and device. Selected item depends on your project.



Project information

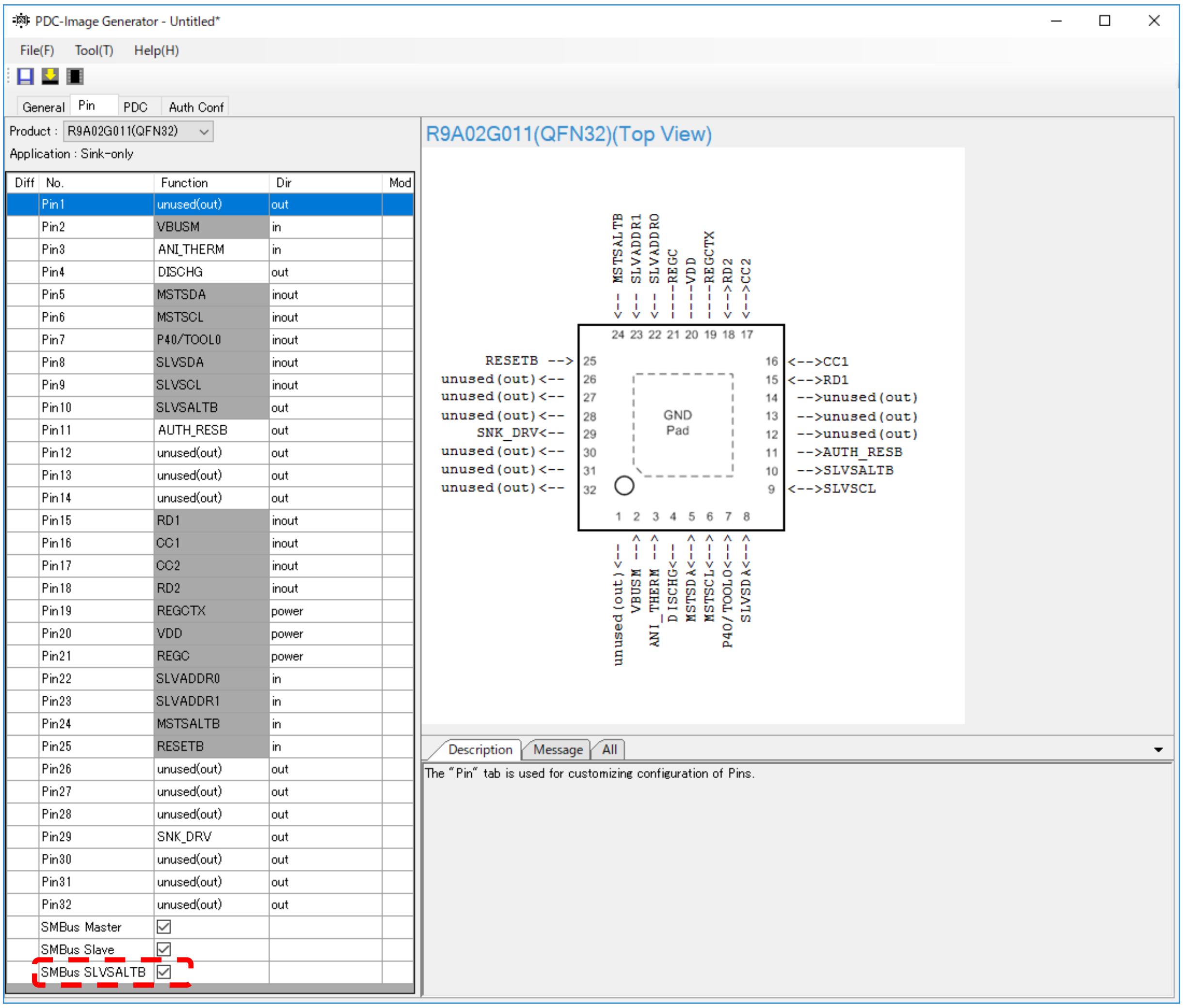
Use this project if you design product for sink only.

R9A02G011GNP
R9A02G011GNP(PDFU)
R9J02G012GBG
R9J02G012GBG(PDFU)

Figure 3-1 Project Wizard window

Set parameters following your project. Please refer to the Flash memory image data generator software G011/G012 edition (PDC-IMGGEN): BCD-ISG-19-5015 in detail.

Note: SMBus Slave alert (SMBus SLVALTB) pin should be enabled for C-Auth operation. Open the Pin tab. Check SMBus SLVALTB check box. Figure 3-2 Enable SMBus SLVSALTB shows SMBus SLVALTB checked configuration.



Product : R9A02G011(QFN32)

Application : Sink-only

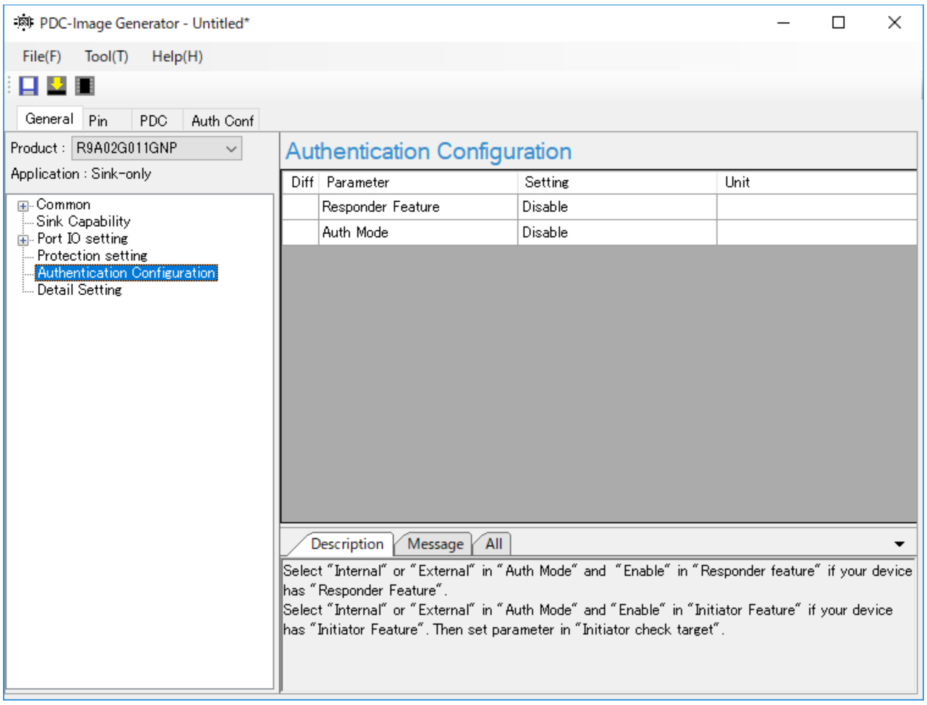
Diff	No.	Function	Dir	Mod
	Pin1	unused(out)	out	
	Pin2	VBUSM	in	
	Pin3	ANI_THERM	in	
	Pin4	DISCHG	out	
	Pin5	MSTSDA	inout	
	Pin6	MSTSCL	inout	
	Pin7	P40/TOOL0	inout	
	Pin8	SLVSDA	inout	
	Pin9	SLVSCL	inout	
	Pin10	SLVSALTB	out	
	Pin11	AUTH_RESB	out	
	Pin12	unused(out)	out	
	Pin13	unused(out)	out	
	Pin14	unused(out)	out	
	Pin15	RD1	inout	
	Pin16	CC1	inout	
	Pin17	CC2	inout	
	Pin18	RD2	inout	
	Pin19	REGCTX	power	
	Pin20	VDD	power	
	Pin21	REGC	power	
	Pin22	SLVADDR0	in	
	Pin23	SLVADDR1	in	
	Pin24	MSTSALTB	in	
	Pin25	RESETB	in	
	Pin26	unused(out)	out	
	Pin27	unused(out)	out	
	Pin28	unused(out)	out	
	Pin29	SNK_DRV	out	
	Pin30	unused(out)	out	
	Pin31	unused(out)	out	
	Pin32	unused(out)	out	
	SMBus Master	☑		
	SMBus Slave	☑		
	SMBus SLVSALTB	☑		

The "Pin" tab is used for customizing configuration of Pins.

Figure 3-2 Enable SMBus SLVSALTB

3.1.3.2 Initiator mode

At first, parameters regarding initiator are invisible (Figure 3-3 No parameter regarding initiator configuration).



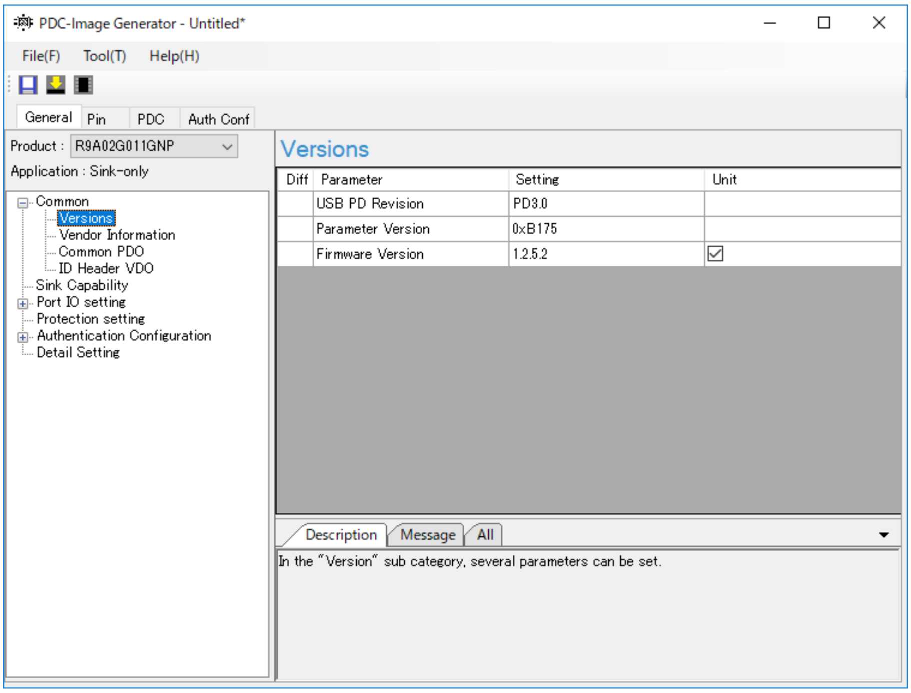
Authentication Configuration

Diff	Parameter	Setting	Unit
	Responder Feature	Disable	
	Auth Mode	Disable	

Select "Internal" or "External" in "Auth Mode" and "Enable" in "Responder feature" if your device has "Responder Feature".
Select "Internal" or "External" in "Auth Mode" and "Enable" in "Initiator Feature" if your device has "Initiator Feature". Then set parameter in "Initiator check target".

Figure 3-3 No parameter regarding initiator configuration

User needs to set Main FW supporting the Initiator mode (Figure 3-4 Main FW supporting the Initiator mode is set on Firmware Version).



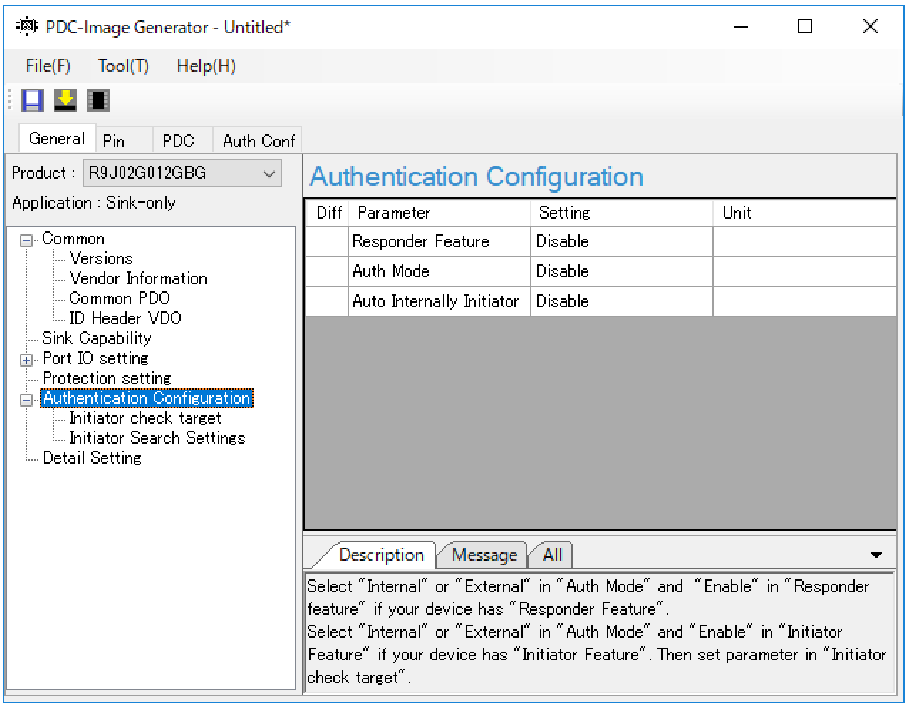
Versions

Diff	Parameter	Setting	Unit
	USB PD Revision	PD3.0	
	Parameter Version	0xB175	
	Firmware Version	1.2.5.2	☑

In the "Version" sub category, several parameters can be set.

Figure 3-4 Main FW supporting the Initiator mode is set on Firmware Version

Parameters regarding Initiator mode appear in the Authentication Configuration category (Figure 3-5 Parameters regarding Initiator mode appear).



Product : R9J02G012GBG

Application : Sink-only

Authentication Configuration

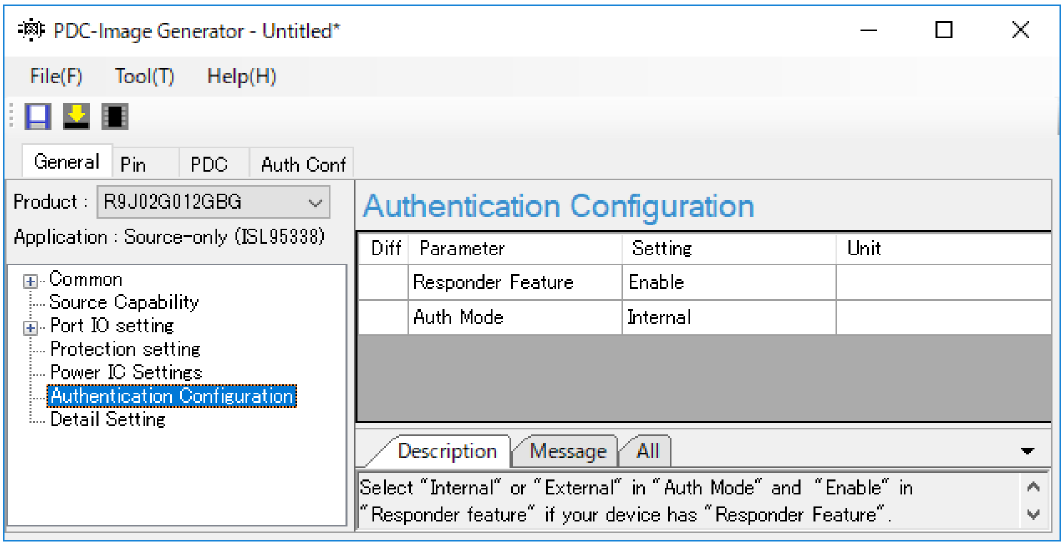
Diff	Parameter	Setting	Unit
	Responder Feature	Disable	
	Auth Mode	Disable	
	Auto Internally Initiator	Disable	

Select "Internal" or "External" in "Auth Mode" and "Enable" in "Responder feature" if your device has "Responder Feature".
Select "Internal" or "External" in "Auth Mode" and "Enable" in "Initiator Feature" if your device has "Initiator Feature". Then set parameter in "Initiator check target".

Figure 3-5 Parameters regarding Initiator mode appear

3.1.3.3 Responder mode

User can set the configuration parameters for responder, irrespective of the initiator configuration. PDC-IMGGEN enables the Responder Feature setting if user starts a source only project.



Product : R9J02G012GBG

Application : Source-only (ISL95338)

Authentication Configuration

Diff	Parameter	Setting	Unit
	Responder Feature	Enable	
	Auth Mode	Internal	

Select "Internal" or "External" in "Auth Mode" and "Enable" in "Responder feature" if your device has "Responder Feature".

Figure 3-6 Default enabled responder feature in a source project

Note: Auth Mode in a Cable project has only "Enable" or "Disable". "Enable" means same as "Internal".

3.1.3.4 Configuration examples

This section describes 3 examples of configurations in each mode. Example 1 shows configurations in the responder mode. Example 2 shows configurations in the initiator mode. In this example, R9A02G011 with R5H3013XB08/R9J02G012 authenticates cable/far end device automatically. Example 3 shows configurations in the initiator mode, too. In example 3, an external controller controls R9A02G011 with R5H3013XB08/R9J02G012 through SMBus Slave interface. Table 3-3 summarizes examples.

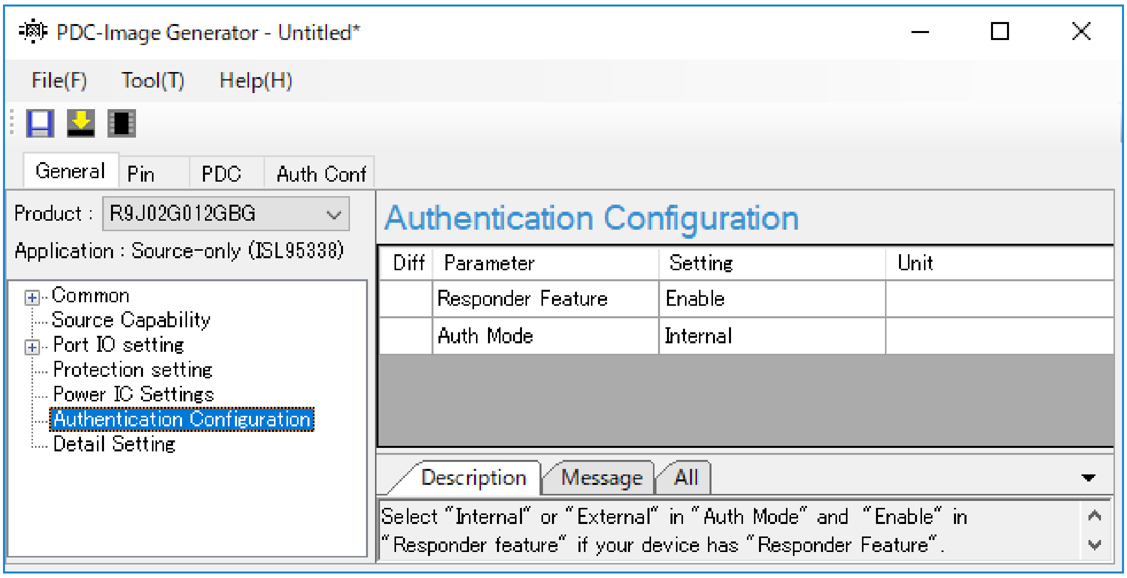
Table 3-3 Summary of configuration examples

Number	Authentication role	Auto Internally Initiator
Example 1	Responder	N/A
Example 2	Initiator	Internal
Example 3	Initiator	External

(1) Example 1. Responder mode

Table 3-4 Example 1, Responder mode configurations

Parameter Items	Setting
Responder Feature	Enabled
Authentication Mode	Internal
Autonomous Internal Initiator	N/A
Initiator operation modes [1:0]	N/A
Certificate Chains Search [7:0]	N/A
VID/PID check	N/A
PID/VID list	N/A
VIDn (n: 1 to 32)	N/A
PIDn (n: 1 to 32)	N/A



Product : R9J02G012GBG

Application : Source-only (ISL95338)

Authentication Configuration

Diff	Parameter	Setting	Unit
	Responder Feature	Enable	
	Auth Mode	Internal	

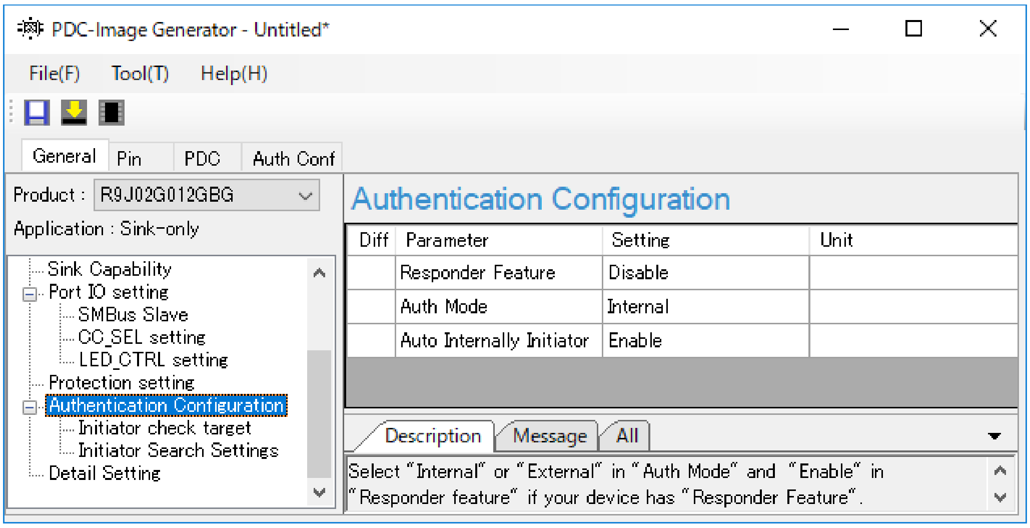
Select "Internal" or "External" in "Auth Mode" and "Enable" in "Responder feature" if your device has "Responder Feature".

Figure 3-7 Authentication configuration window for example 1

(2) Example 2. Initiator mode

Table 3-5 Example 2, Initiator mode configurations

Parameter Items	Setting
Responder Feature	Disable
Auth Mode	Internal
Auto Internally Initiator	Enable
Initiator check target	Source and Cable
Certificate Chains Search [7:0]	FFh
VID/PID check	Enabled
PID/VID list	1 - 32
VIDn (n: 1 to 32)	XXXXh
PIDn (n: 1 to 32)	YYYYh



Product : R9J02G012GBG

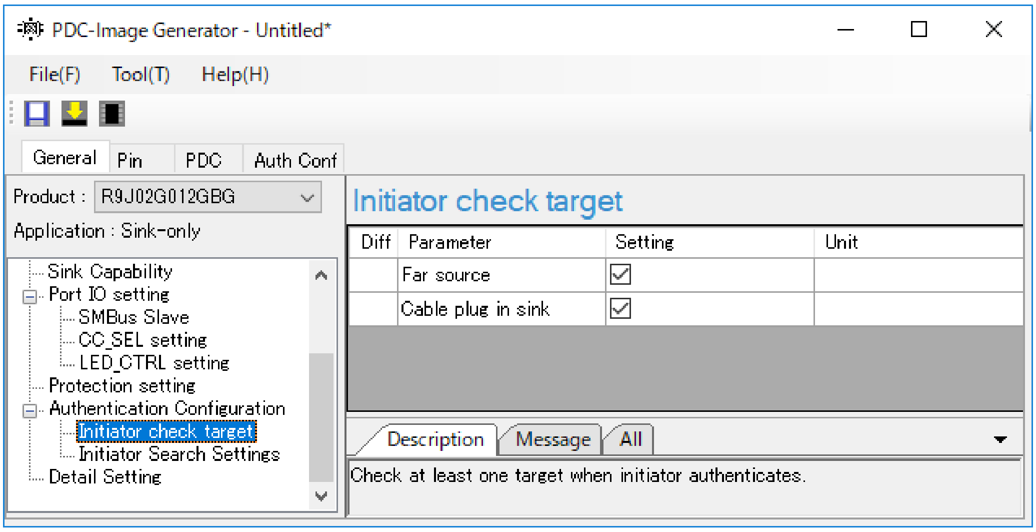
Application : Sink-only

Authentication Configuration

Diff	Parameter	Setting	Unit
	Responder Feature	Disable	
	Auth Mode	Internal	
	Auto Internally Initiator	Enable	

Select "Internal" or "External" in "Auth Mode" and "Enable" in "Responder feature" if your device has "Responder Feature".

Figure 3-8 Authentication configuration window for example 2



Product : R9J02G012GBG

Application : Sink-only

Initiator check target

Diff	Parameter	Setting	Unit
	Far source	☑	
	Cable plug in sink	☑	

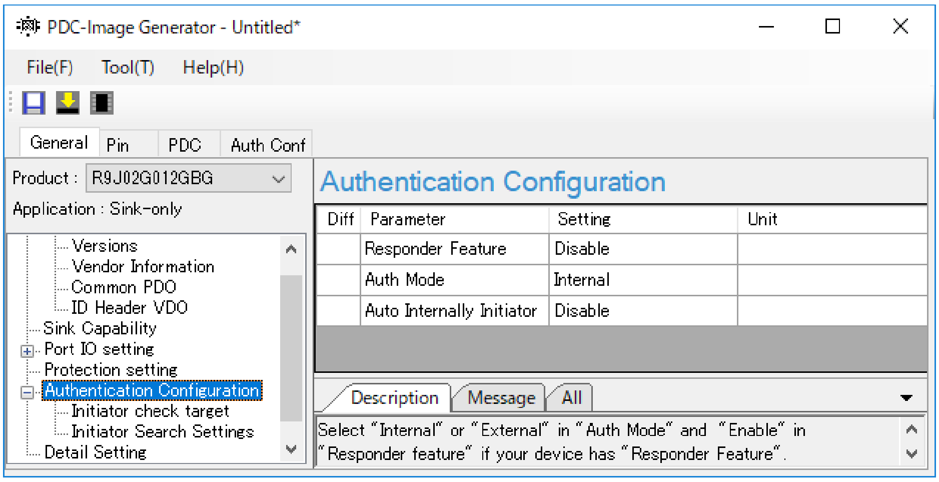
Check at least one target when initiator authenticates.

Figure 3-9 Initiator check target window for example 2

(3) Example 3. Initiator mode

Table 3-6 Example 3, Initiator mode configurations

Parameter Items	Setting
Responder Feature	Disable
Authentication Mode	Internal
Autonomous Internal Initiator	Disable
Initiator operation modes [1:0]	Source and Cable
Certificate Chains Search [7:0]	FFh
VID/PID check	Enabled
PID/VID list	1 - 32
VIDn (n: 1 to 32)	XXXXh
PIDn (n: 1 to 32)	YYYYh



Product : R9J02G012GBG

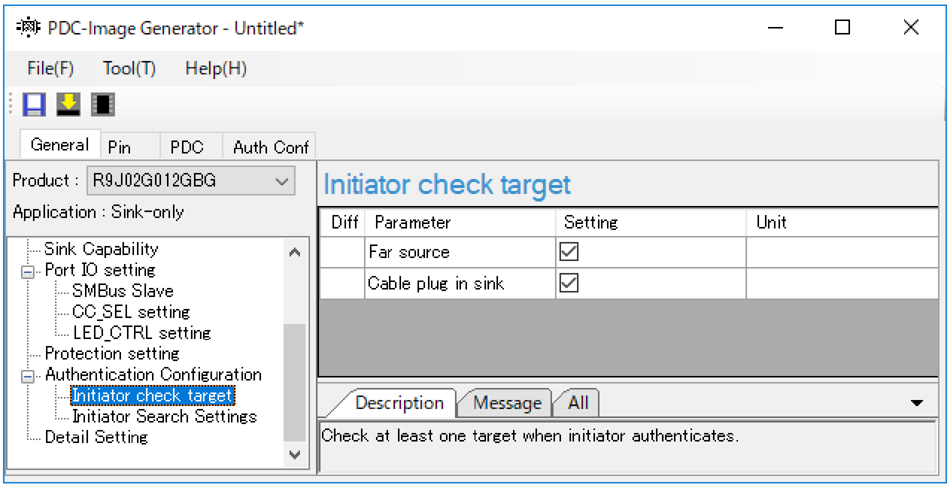
Application : Sink-only

Authentication Configuration

Diff	Parameter	Setting	Unit
	Responder Feature	Disable	
	Auth Mode	Internal	
	Auto Internally Initiator	Disable	

Select "Internal" or "External" in "Auth Mode" and "Enable" in "Responder feature" if your device has "Responder Feature".

Figure 3-10 Authentication configuration window for example 3



Product : R9J02G012GBG

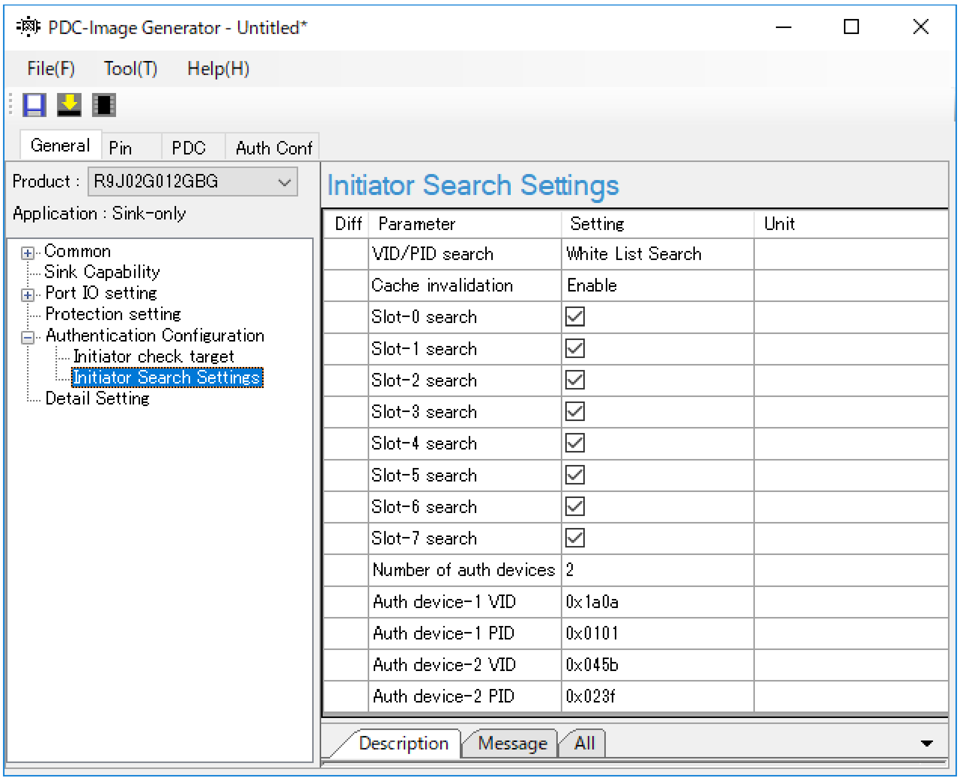
Application : Sink-only

Initiator check target

Diff	Parameter	Setting	Unit
	Far source	☑	
	Cable plug in sink	☑	

Check at least one target when initiator authenticates.

Figure 3-11 Initiator check target window for example 3



Product : R9J02G012GBG

Application : Sink-only

- Common
- Sink Capability
- Port IO setting
- Protection setting
- Authentication Configuration
  - Initiator check target
  - Initiator Search Settings
- Detail Setting

Initiator Search Settings

Diff	Parameter	Setting	Unit
	VID/PID search	White List Search	
	Cache invalidation	Enable	
	Slot-0 search	☑	
	Slot-1 search	☑	
	Slot-2 search	☑	
	Slot-3 search	☑	
	Slot-4 search	☑	
	Slot-5 search	☑	
	Slot-6 search	☑	
	Slot-7 search	☑	
	Number of auth devices	2	
	Auth device-1 VID	0x1a0a	
	Auth device-1 PID	0x0101	
	Auth device-2 VID	0x045b	
	Auth device-2 PID	0x023f	

Figure 3-12 Initiator Search Settings window for example 3

3.1.3.5 Writing FW

Connect as shown in the Figure 3-13 or Figure 3-14. Please refer to Renesas USB PDC Exerciser User's Manual, BCD-IMB-19-5000 if RTK-251-DRPEVB is used as a firmware updater tool. For RTK-251-DRPEVB, user should install Updater FW into both R9A02G011 and RL78/G1C.

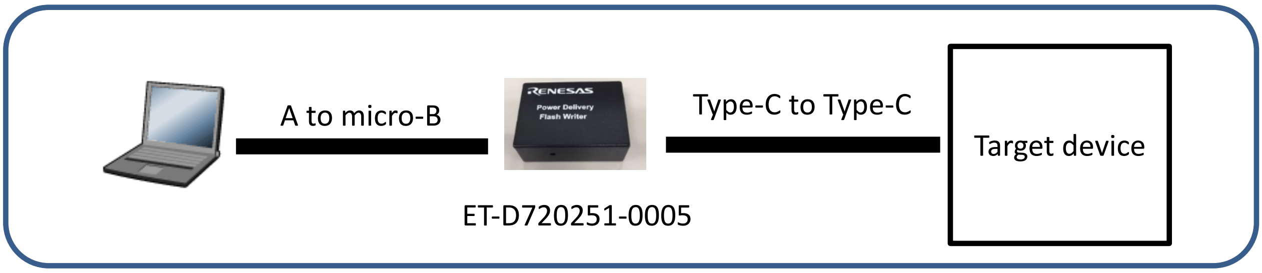


Figure 3-13 FW update by ET-D720251-0005

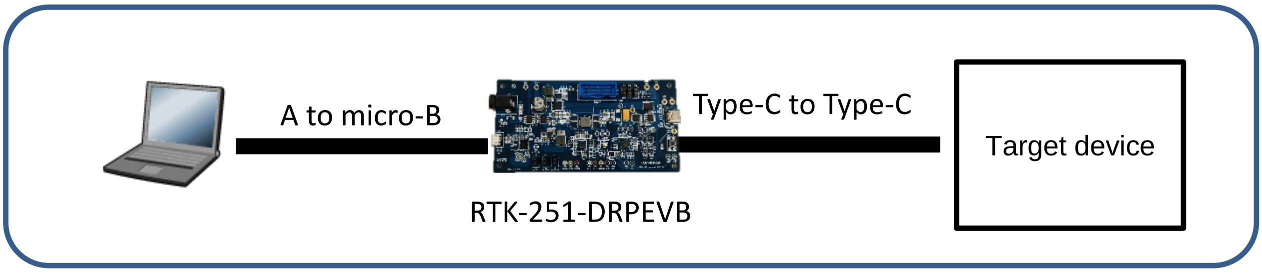
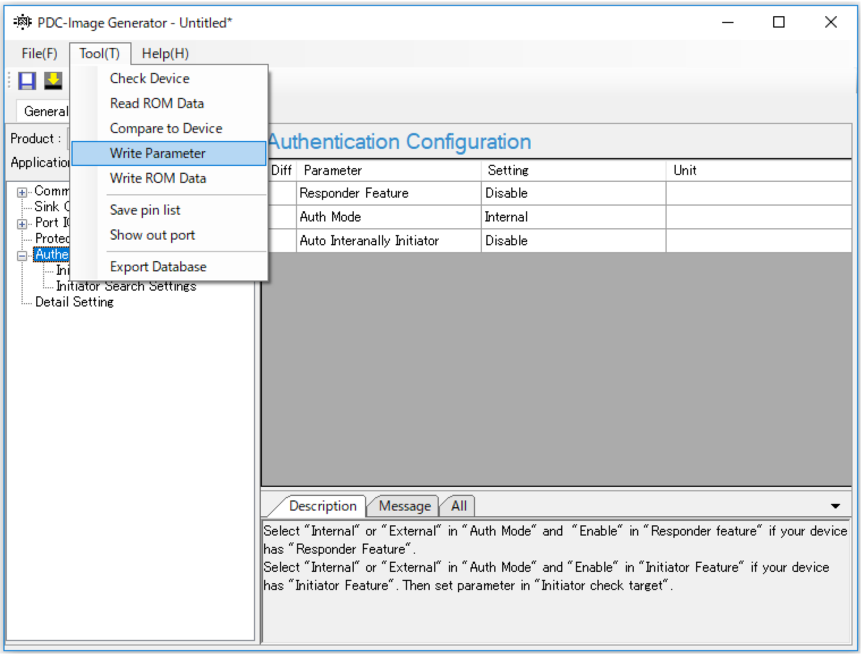


Figure 3-14 FW update by RTK-251-DRPEVB

Follow the process to write the FW.

1. Tool -> Write Parameter



Authentication Configuration

Diff	Parameter	Setting	Unit
	Responder Feature	Disable	
	Auth Mode	Internal	
	Auto Interanally Initiator	Disable	

Select "Internal" or "External" in "Auth Mode" and "Enable" in "Responder feature" if your device has "Responder Feature".
Select "Internal" or "External" in "Auth Mode" and "Enable" in "Initiator Feature" if your device has "Initiator Feature". Then set parameter in "Initiator check target".

Figure 3-15 Click Write Parameter

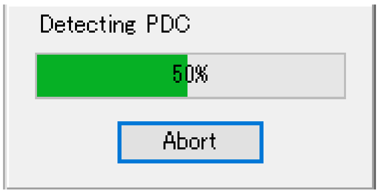


Figure 3-16 Detecting PDC window

2. Select the target PDC and click "OK".

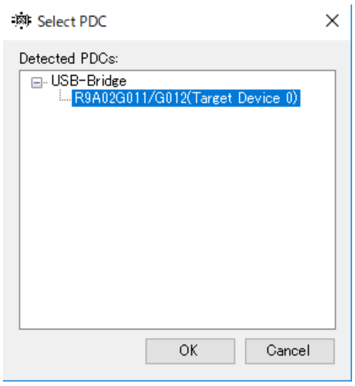
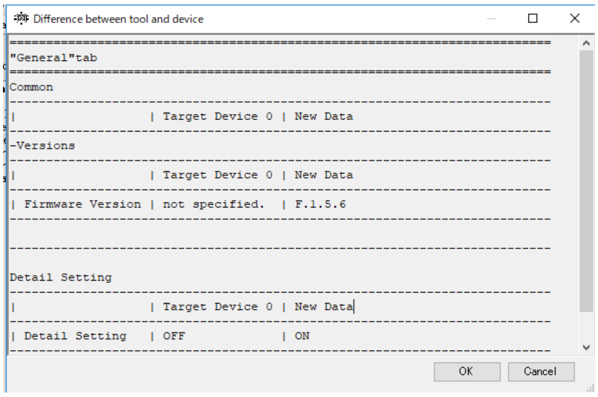


Figure 3-17 Select PDC window

3. Click “OK”.



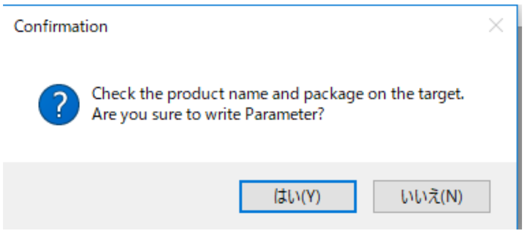
```
==========================================================================
"General"tab
==========================================================================
Common
--------------------------------------------------------------------------
|                  | Target Device 0 | New Data
--------------------------------------------------------------------------
-Versions
--------------------------------------------------------------------------
|                  | Target Device 0 | New Data
--------------------------------------------------------------------------
| Firmware Version | not specified.  | F.1.5.6
--------------------------------------------------------------------------

--------------------------------------------------------------------------

Detail Setting
--------------------------------------------------------------------------
|                  | Target Device 0 | New Data
--------------------------------------------------------------------------
| Detail Setting   | OFF             | ON
--------------------------------------------------------------------------
```

Figure 3-18 Difference between tool and device window

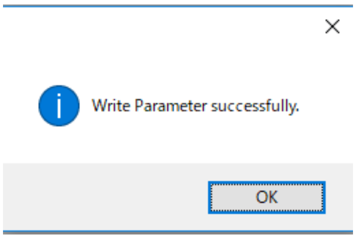
4. Click “Yes”



Check the product name and package on the target.
Are you sure to write Parameter?

Figure 3-19 Confirmation window

5. Finished

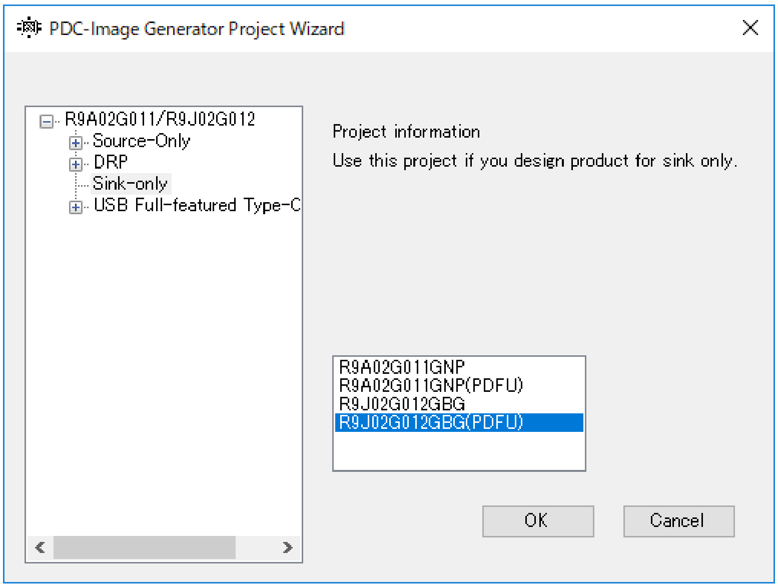


Write Parameter successfully.

Figure 3-20 Parameter writing result window

3.1.3.6 PDFU

PDC-IMGGEN supports generating PDFU FW. Please open project wizard window, select power role, and select device R9A02G011GNP(PDFU) or R9J02G012GBG(PDFU).



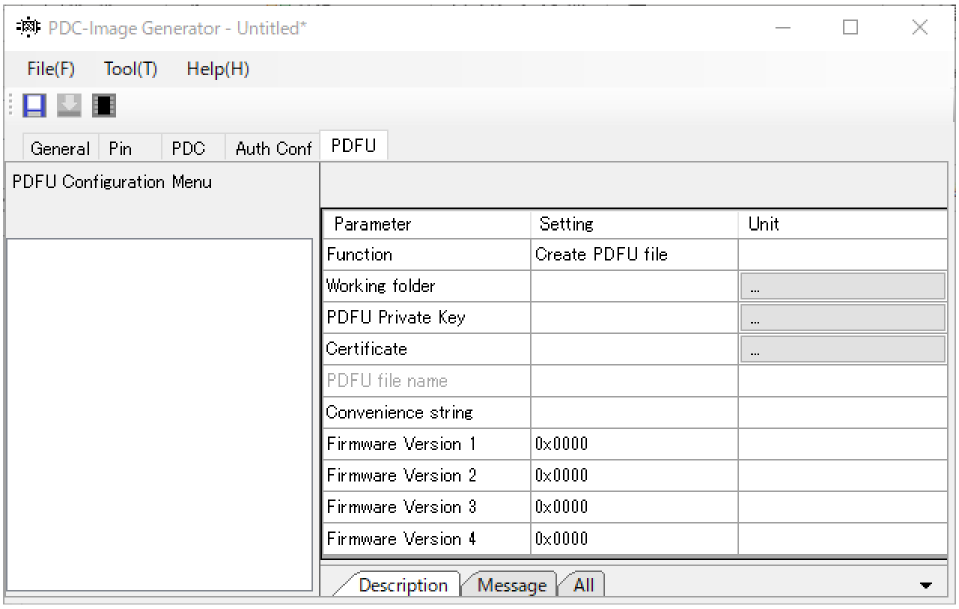
Project information

Use this project if you design product for sink only.

R9A02G011GNP
R9A02G011GNP(PDFU)
R9J02G012GBG
R9J02G012GBG(PDFU)

Figure 3-21 Project wizard window to start a PDFU project

PDFU tab window appears if PDFU project is started. Please refer to the Help(H) -> Help to operate PDFU function in the PDC-IMGGEN.



Parameter	Setting	Unit
Function	Create PDFU file	
Working folder		...
PDFU Private Key		...
Certificate		...
PDFU file name		
Convenience string		
Firmware Version 1	0x0000	
Firmware Version 2	0x0000	
Firmware Version 3	0x0000	
Firmware Version 4	0x0000	

Figure 3-22 PDFU tab window

3.1.4 External controller initiates Initiator through SMBus Slave interface

An external controller can initiate initiator through SMBus Slave interface. This section describes how to access SMBus Slave interface registers to control the initiator operation.

3.1.4.1 SMBus Slave interface register

Table 3-7 Status 1 (03H)

Bit	Name	Reset Value	Description
15:4	-	-	Refer to section 6.2.7 in R9A02G011/R9J02G012 user manual.
3:1	Last Command	000b	Indication of Last Command Valid only if Status1.Command State = 0b (no command in progress) 000b: Command accepted and completed, or command never received 001b: Command aborted 010b: Invalid command 011b: Far-end device reject 110b: Try Authentication command failed 111b: Try Authentication command canceled 100b: Wait
0	Command State	0b	Refer to section 6.2.7 in R9A02G011/R9J02G012 user manual.

Table 3-8 describes the Last Command code definitions for Try Authentication command.

Table 3-8 Last Command code definitions

Command Code	Descriptions
Accepted	The command completed successfully.
Aborted	The command failed due to an event such as: • Protocol Error • Soft Reset • Hard Reset • Error Recovery
Invalid	Timing and settings are invalid to process the command. USB-C authentication feature is not configured correctly. The command is not able to be initiated.
Reject	The command was rejected due to an event that occurred. • A reject message or Not Supported message was received. • The responder doesn't support USB-C authentication. • The cable responder, eMarker, is not detected. • Initiator is not able to become VCONN source for cable authentication.
Wait	The command cannot be processed immediately, e.g. • The voltage value is changing. • The power direction is changing • Auto Internal Initiator is enabled in FW parameter setting and Authentication is in progress.
Failed	Authentication failed. It contains VID/PID check failure when the function is enabled in FW parameter setting.
Cancelled	Authentication canceled due to a PD message received.

Table 3-9 Command (07H)

Bit	Name	Reset Value	Description
15:8	Battery Reference	00h	Refer to the section 6.2.11 of R9A02G011/R9J02G012 user manual.
7:0	Command	00h	PDC command 02h: Send Go to Min message to far-end device 07h: Send Get Source Cap message to far-end device 08h: Send Get Sink Cap message to far-end device 09h: Send Data Role Swap message to far-end device 0Ah: Send Power Role Swap message to far-end device 0Dh: Send Soft Reset 21h: Send Source Capabilities message to far-end device 22h: Send Request message to far-end device. 60h: Send Hard Reset 61h: Send Cable Reset 80h: Abort last sent Command 81h: Enable Type-C Controller 82h: Disable Type-C Controller 84h: Enter Deep Sleep mode 85h: Enter Sleep mode The following commands are used for USB PD3.0 Only. 10h: Send Not Supported message to far-end device 11h: Send Get Source Cap Extended message to far-end device 12h: Send Get Status message to far-end device 14h: Send Get PPS Status message to far-end device 16h: Send Get Sink Cap Extended message to far-end device 25h: Send Battery Status message to far-end device 26h: Send Alert message to far-end device 43h: Send Get Battery Cap message to far-end device 44h: Send Get Battery Status message to far-end device 45h: Send Battery Capabilities message to far-end device 46h: Send Get Manufacturer Info message 47h: Send Manufacturer Info message to far-end device 50h: Send Security Request message [Note] 83h: Try Authentication All other values are reserved.

Note: Send Security Request message command is used when the authentication operation of R9A02G011/R9J02G012 is disabled and the external controller creates PD message payload.

3.1.4.2 Try Authentication Command sequence

Figure 3-23 describes how an external controller initiates the Try Authentication command.

1. Check 5V PD contract in place.
2. Write Object Data Mode to determine PD Message destination, 1) cable, 2) source.
3. Execute Try Authentication command.

Table 3-10 Object Data Mode (71H) for Try Authentication command Table 3-10 describes the Object Data Mode (71h) value used for Try Authentication command.

Table 3-10 Object Data Mode (71H) for Try Authentication command

Bit	Name	Value	Description
32:24	Data Position	00h	Not used. Refer to section 6.2.24 in R9A02G011/R9J02G012 user manual for details.
23:16	Object Data Size	00h	Not used. Refer to section 6.2.24 in R9A02G011/R9J02G012 user manual for details.
15	Object Data Mode	0b	Not used. Refer to section 6.2.24 in R9A02G011/R9J02G012 user manual for details.
14:0	-	00000b	Reserved.
9:8	Recipient	01b	SOP to source device.
		10b	SOP' to cable.
7:0	Object Data Select	00h	Not used. Refer to section 6.2.24 in R9A02G011/R9J02G012 user manual for details.

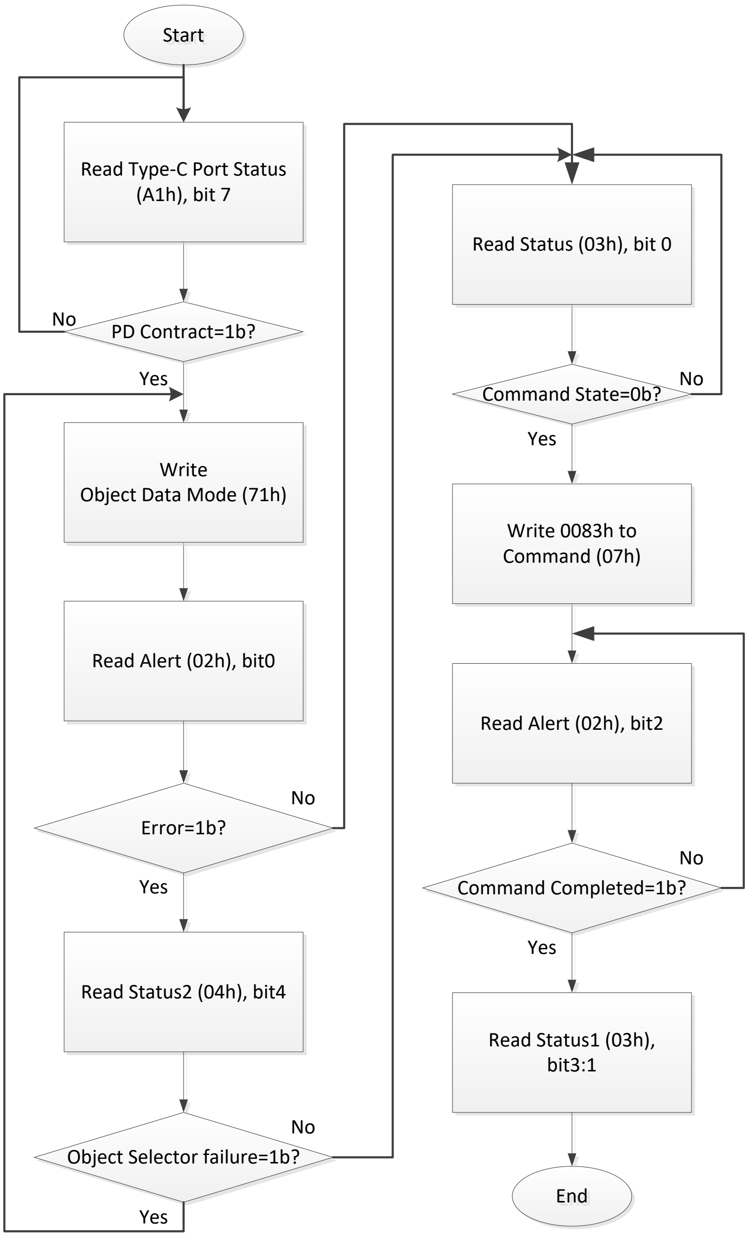


Figure 3-23 Try Authentication command sequence

Note: The external control through SMBus Slave interface doesn't support Responder mode.

3.2 SDK

Renesas provides an SDK for R9A02G011/R9J02G012. Users can develop their firmware using the SDK in a manner similar to firmware development for an MCU. User's code can access and control the USB Type-C PHY, USB Type-C protocol manager, and other peripherals via the SDK libraries. Please refer to the Rensas SDK Application note, BCD-ISG-19-5024.

Renesas provides another SDK for C-Auth in addition to the SDK for PD. Please refer to the Renesas SDK Application note for Auth, BCD-ISG-19-5028.

3.2.1 Sample project

The SDK has some sample projects. Users can make their own C-Auth firmware. Table 3-11 shows the feature list for each target board of the sample project.

Table 3-11 SDK Auth sample project feature list

Target board of sample	Mounted Power IC	Power role	Authentication
RTK-251-1PowerBank3 (RTK0EUG011D06010BJ)	ISL95538B	DRP Try.SRC	Responder (in Source)
RTK-251-BuckBoostConverter2 (RTK0EUG011D07010BJ)	ISL95338	Source	Responder
RTK-251-DRPEVB (RTK0EUG011D08010BJ)	ISL95338	DRP	Initiator (in Sink)/ Responder (in Source)

User can change the configuration on the sample project.

3.2.2 Initiator configuration

SDK provides Initiator function in Sink as a sample. Please set the symbolic constant depending on your expectation at AUTH_TYP. Figure 3-24 and Figure 3-25 show an example of the initiator. In this example, the initiator tries to authenticate the connected source device. AUTH_SPRT_INIT is passed as an argument to auth_init() function unless AUTH_SNK_INITATOR_DIS is set at AUTH_TYP. Initiator feature is enabled if auth_init() passed AUTH_SPRT_INIT is called.

user_main_authentication.h

```
#define AUTH_SNK_INITIATOR_DIS(0)
#define AUTH_SNK_INITIATOR_FARSRC(1)
#define AUTH_SNK_INITIATOR_CP(2)
#define AUTH_SNK_INITIATOR_CP_FARSRC(3)
#define AUTH_TYP    AUTH_SNK_INITIATOR_FARSRC
```

Figure 3-24 Example using #define to authenticate the far end source device in user_main_authentication.h

user_main.c

```
auth_init((ULONG)&relamcu_reset_err, AUTH_SPRT_INIT|AUTH_SPRT_RESP_SRC);
```

Figure 3-25 Example of the auth_init function in user_main.c

3.2.3 Responder configuration

Please set AUTH_SPRT_RESP_SRC or AUTH_SPRT_RESP_SNK as a second argument for auth_init() function. Figure 3-26 shows an example of the auth_init() function to enable the source responder. In the sample code, this function is called if AUTH_SNK_INITIATOR_DIS is defined as AUTH_TYP.

user_main.c

```
auth_init((ULONG)&relamcu_reset_err, AUTH_SPRT_RESP_SRC);
```

Figure 3-26 Example of the auth_init function to enable the source responder

3.2.4 Writing FW

Please refer to chapter 2 in Renesas SDK Application note, BCD-ISG-19-5024 or Renesas SDK for IAR EWRL78 Application note, BCD-ISG-19-5028.

Please refer to Renesas USB PDC Exerciser User's Manual, BCD-IMB-19-5000 if RTK-251-DRPEVB is used as a firmware updater tool. User should install Updater FW into R9A02G011 and RL78/G1C.

3.2.5 PDFU

PDFU FW can be created from SDK FW. Please refer to section 1.5 Create PDFU format data in the Renesas SDK Application note for Auth, BCD-ISG-19-5029. (PDFU refers to Power Delivery Firmware Update.)

4. Debug

Renesas provides 2 tools to debug C-Auth behavior: RTK-251-DRPEVB and C-Auth Test Suite program.

4.1 RTK-251-DRPEVB as an exerciser

The exerciser can send USB PD messages in any timing. User can observe security response messages from a test device easily.

User should install the Exerciser FW into R9A02G011 on RTK-251-DRPEVB. Please refer to Renesas USB PDC Exerciser User's Manual, BCD-IMB-19-5000.

4.1.1 Equipment

Please prepare the below items:

- Windows PC
- RTK-251-DRPEVB as an exerciser
- 19V adapter for RTK-251-DRPEVB
- USB A to Micro-B cable
- USB Type-C cable
- Test device

4.1.2 Connection

Figure 4-1 shows the connection for an exerciser with PC and test device.

1. PC connects with RTK-251-DRPEVB.
2. RTK-251-DRPEVB connects with 19V AC adapter.
3. Insert plug of AC adapter in outlet.

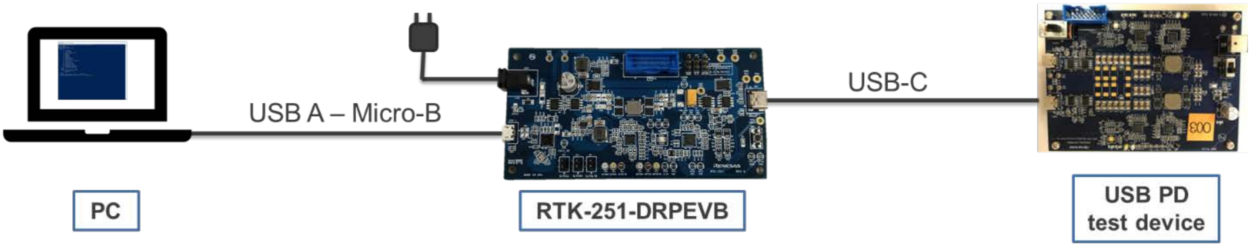


Figure 4-1 Exerciser connection with PC and a test device

4.1.3 Script sequence

Please follow below sequence. Please refer to Renesas USB PDC Exerciser User's Manual, BCD-IMB-19-5000.

1. Unblock PowerShell in Properties
2. Set Execution Policy in PowerShell
3. Launch PowerShell console, move to Exerciser_scripts directory.
4. Set COM port by executing “set_com_port” script.
5. Set exerciser authentication configuration by “set_auth_conf” script.
   Default settings are below. Please disable the Cache setting if you want to confirm CERTIFICATE message every time.

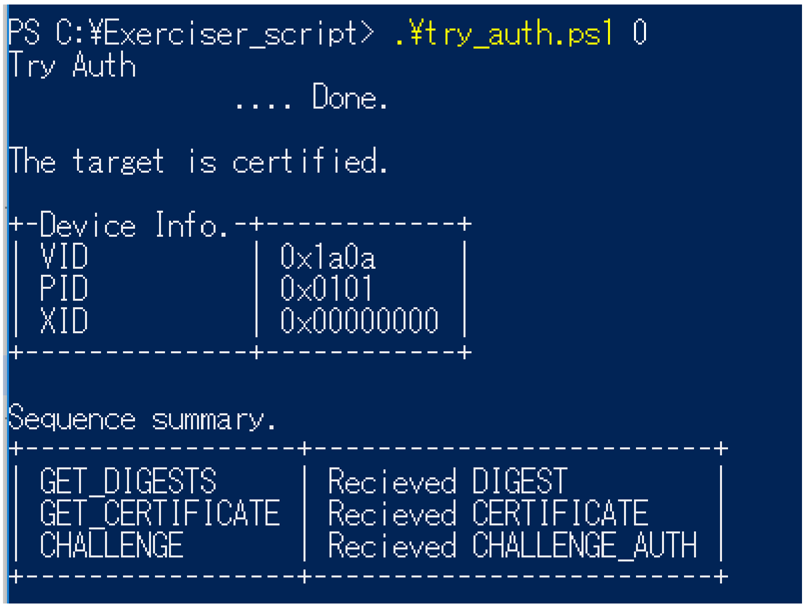
Table 4-1 Default settings of exerciser authentication

Items	Default
Responder	Disable
Cache	Enable
Search Slot	1111_1111

6. RTK-251-DRPEVB connects with the test device through USB Type-C cable.
7. Execute “try_auth” script.

4.1.4 Result

Figure 4-2 shows a result of “try_auth” script. A “certified” appears if try authentication succeeds.



```
PS C:¥Exerciser_script> .¥try_auth.ps1 0
Try Auth
              .... Done.

The target is certified.

+-Device Info.-+------------+
| VID          | 0x1a0a     |
| PID          | 0x0101     |
| XID          | 0x00000000 |
+--------------+------------+

Sequence summary.
+-----------------+-------------------------+
| GET_DIGESTS     | Recieved DIGEST         |
| GET_CERTIFICATE | Recieved CERTIFICATE    |
| CHALLENGE       | Recieved CHALLENGE_AUTH |
+-----------------+-------------------------+
```

Figure 4-2 Result of “try_auth” script

4.2 C-Auth Test Suite

C-Auth Test Suite tests if a test device has the correct certificate of the C-Auth. The C-Auth Test Suite can test C-Auth source responder and cable. User can confirm if their responder firmware can respond to an initiator device correctly.

Please refer to C-authTestSuite ApplicationNote, BCD-ISG-17-5066 and C-authTestSuite InstructionManual, BCD-ISG-17-5067 for further detail.

4.2.1 Equipment

Please prepare below items:

- Windows PC
- RTK-251-DRPEVB or ET-D720251-0005-C as an ACB tool
- USB A to Micro-B cable
- USB Type-C cable
- Test device

Note: You should install Bridge FW for RTK-251-DRPEVB in R9A02G011 on RTK-251-DRPEVB, and RomWriteModule hex file into RL78/G1C on RTK-251-DRPEVB if you want to use RTK-251-DRPEVB as a bridge device instead of ET-D720251-0005-C. Please ask the local agent FAE to get these FW.

4.2.2 Connection

Figure 4-3 shows the connection between PC and test device.

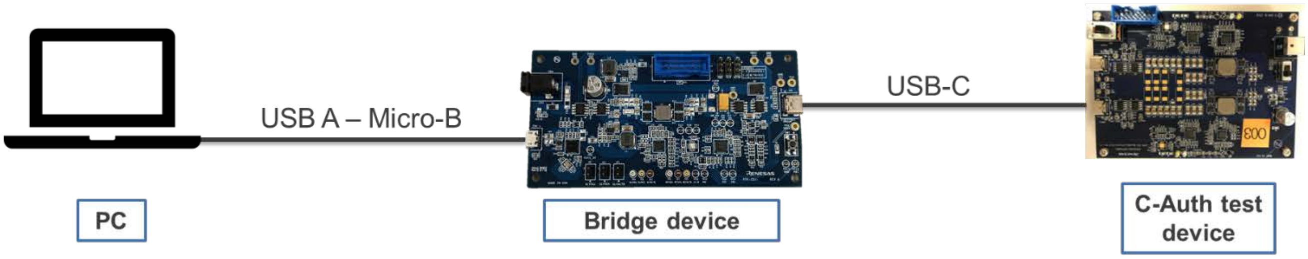


Figure 4-3 C-Auth Test Suite connection between PC and a test device

Note: C-Auth Test Suite can also test USB Type-C cable as a C-Auth test device.

4.2.3 Test Sequence

Please follow below sequence.

1. Execute C-AuthTest.exe

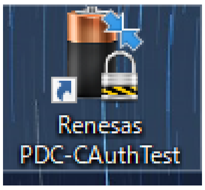
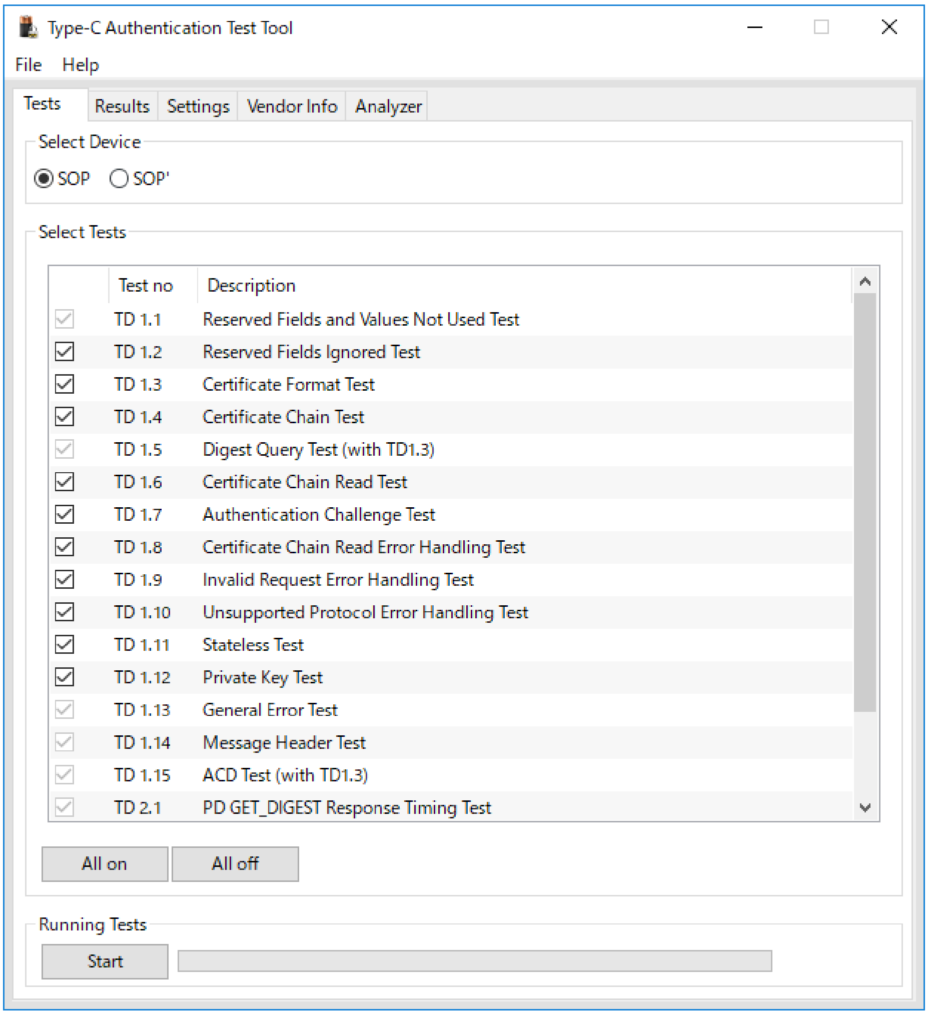


Figure 4-4 C-AuthTest.exe icon

2. Select SOP or SOP' in "Select Device".



Select Device

● SOP ○ SOP'

Select Tests

	Test no	Description
☑	TD 1.1	Reserved Fields and Values Not Used Test
☑	TD 1.2	Reserved Fields Ignored Test
☑	TD 1.3	Certificate Format Test
☑	TD 1.4	Certificate Chain Test
☑	TD 1.5	Digest Query Test (with TD1.3)
☑	TD 1.6	Certificate Chain Read Test
☑	TD 1.7	Authentication Challenge Test
☑	TD 1.8	Certificate Chain Read Error Handling Test
☑	TD 1.9	Invalid Request Error Handling Test
☑	TD 1.10	Unsupported Protocol Error Handling Test
☑	TD 1.11	Stateless Test
☑	TD 1.12	Private Key Test
☑	TD 1.13	General Error Test
☑	TD 1.14	Message Header Test
☑	TD 1.15	ACD Test (with TD1.3)
☑	TD 2.1	PD GET_DIGEST Response Timing Test

Running Tests

Figure 4-5 Select "Select Device" in Tests tab window

Note: SOP' (Start Of Packet) Communication is recognized by electronics in one Cable Plug which is the Cable Plug that detected VCONN at Attach. Please refer to C-Auth Test Suite Application Note, BCD-ISG-17-5066 page 7.

3. Open “Vendor Info” tab
4. Select “slot0”
5. Click “Browse” and set Root Certification

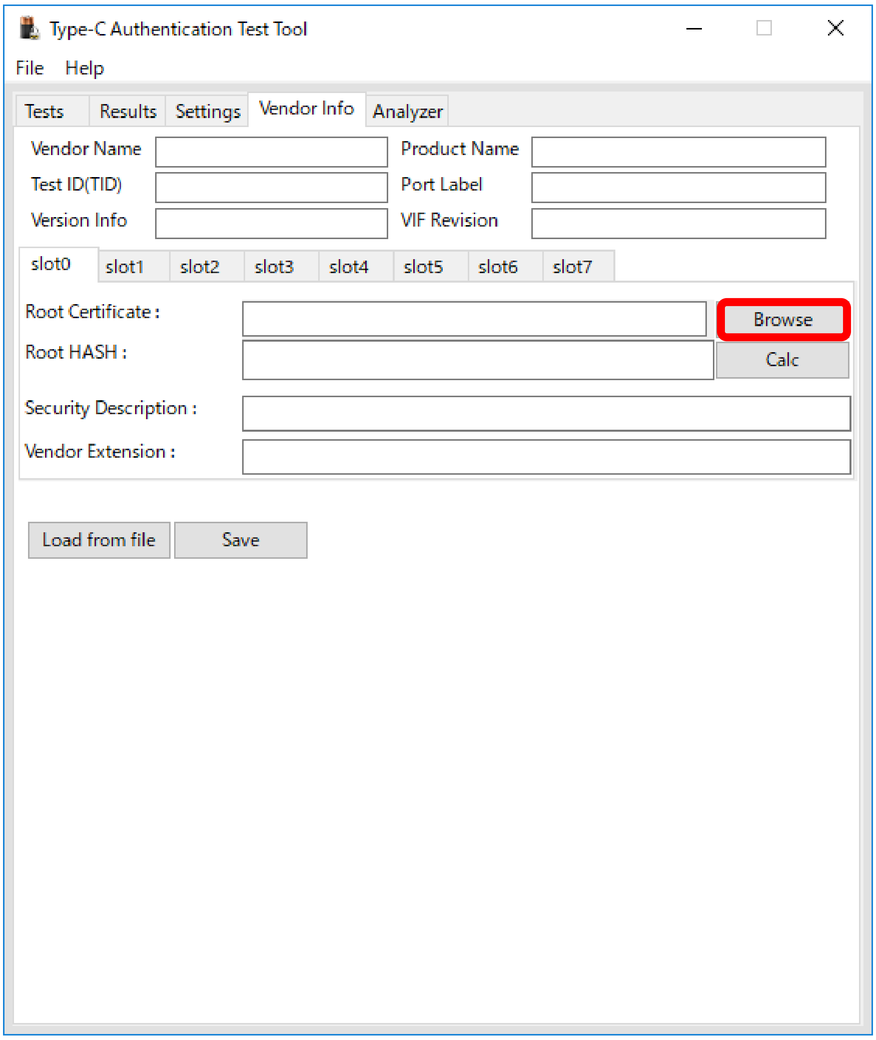
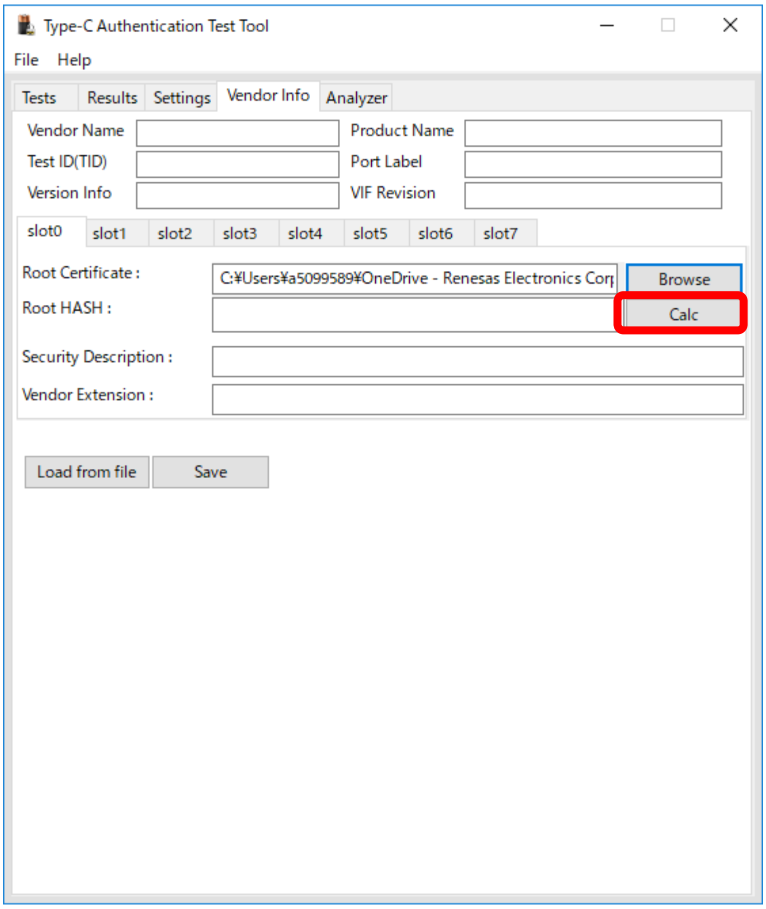


Figure 4-6 Vendor Info tab window

6. Click “Calc” to calculate the Root HASH

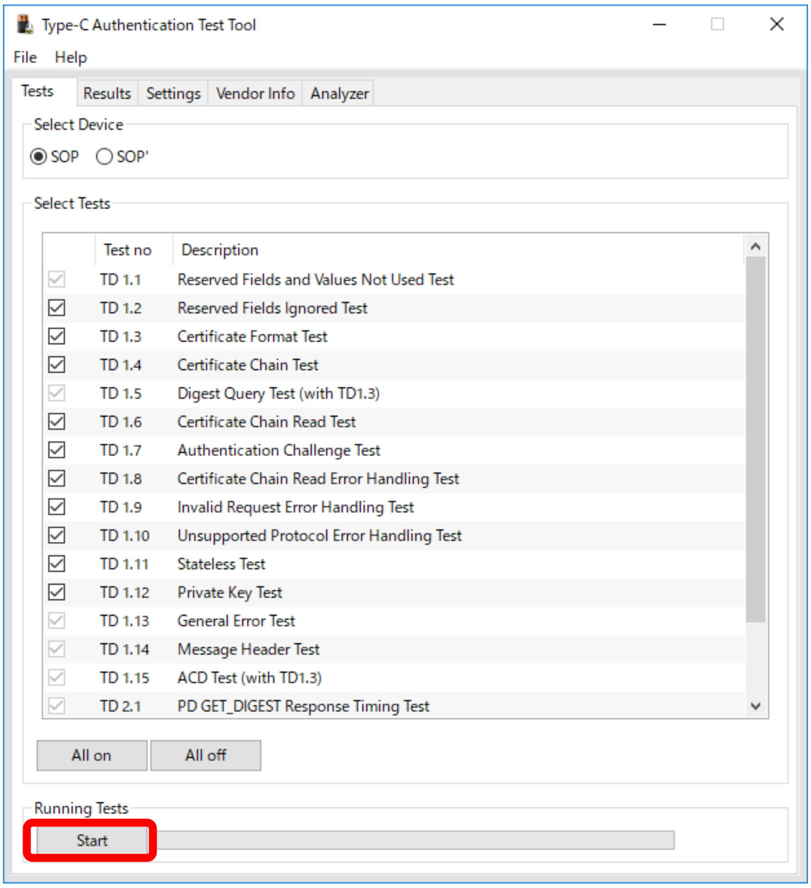


Root Certificate : C:¥Users¥a5099589¥OneDrive - Renesas Electronics Corp

Figure 4-7 Click "Calc"

7. Select “slot4”
8. Click “Browse” and set Renesas Certification
9. Click “Calc” to calculate the HASH

10. Open “Tests”
11. Click “Start”



Type-C Authentication Test Tool
File Help
Tests Results Settings Vendor Info Analyzer
Select Device

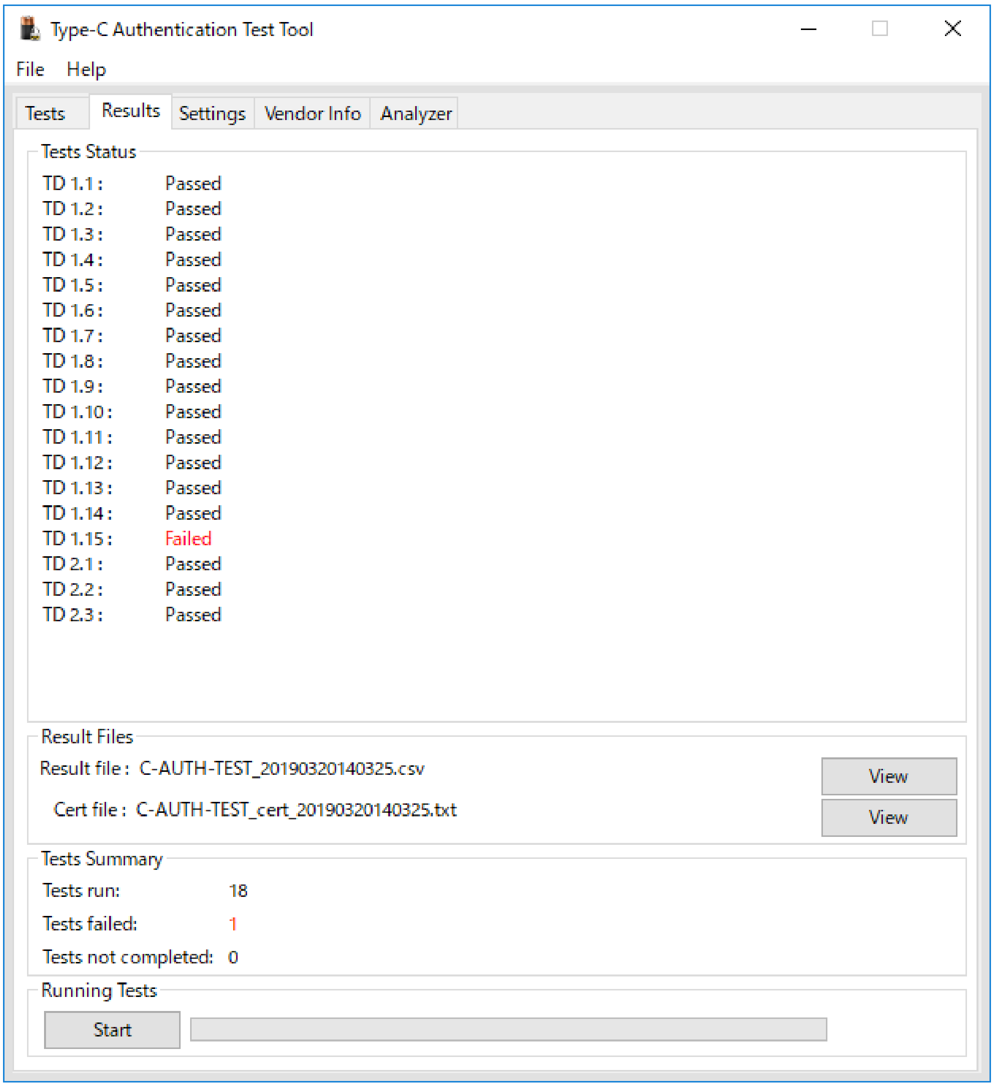
● SOP ○ SOP'

	Test no	Description
☑	TD 1.1	Reserved Fields and Values Not Used Test
☑	TD 1.2	Reserved Fields Ignored Test
☑	TD 1.3	Certificate Format Test
☑	TD 1.4	Certificate Chain Test
☑	TD 1.5	Digest Query Test (with TD1.3)
☑	TD 1.6	Certificate Chain Read Test
☑	TD 1.7	Authentication Challenge Test
☑	TD 1.8	Certificate Chain Read Error Handling Test
☑	TD 1.9	Invalid Request Error Handling Test
☑	TD 1.10	Unsupported Protocol Error Handling Test
☑	TD 1.11	Stateless Test
☑	TD 1.12	Private Key Test
☑	TD 1.13	General Error Test
☑	TD 1.14	Message Header Test
☑	TD 1.15	ACD Test (with TD1.3)
☑	TD 2.1	PD GET_DIGEST Response Timing Test

Figure 4-8 Click "Start"

4.2.4 Result

Figure 4-9 shows an example of C-Auth Test Suite result window. Test result describes in the Tests Status window. You can see csv file of the test result report if you click “View”.



Tests Status

TD 1.1 :	Passed
TD 1.2 :	Passed
TD 1.3 :	Passed
TD 1.4 :	Passed
TD 1.5 :	Passed
TD 1.6 :	Passed
TD 1.7 :	Passed
TD 1.8 :	Passed
TD 1.9 :	Passed
TD 1.10 :	Passed
TD 1.11 :	Passed
TD 1.12 :	Passed
TD 1.13 :	Passed
TD 1.14 :	Passed
TD 1.15 :	Failed
TD 2.1 :	Passed
TD 2.2 :	Passed
TD 2.3 :	Passed

Result Files

Result file : C-AUTH-TEST_20190320140325.csv

Cert file : C-AUTH-TEST_cert_20190320140325.txt

Tests Summary

Tests run:	18
Tests failed:	1
Tests not completed:	0

Running Tests

Figure 4-9 Example of C-Auth Test Suite result

Note: TD1.15 error message~
The ACD contains a Playpen TLV. slot: 0’ still remain, describes that proto type can contain Playpen information, although mass production cannot. This time we use proto type Secure MCU for the demo cable, which contain this information, and this error will be eliminated in mass production phase.

Revision History

Rev.	Date	Description	
		Page	**Summary**
1.00	Mar. 27, 2019	-	Initial revision

General Precautions in the Handling of Microprocessing Unit and Microcontroller Unit Products

The following usage notes are applicable to all Microprocessing unit and Microcontroller unit products from Renesas. For detailed usage notes on the products covered by this document, refer to the relevant sections of the document as well as any technical updates that have been issued for the products.

1. Precaution against Electrostatic Discharge (ESD)

   A strong electrical field, when exposed to a CMOS device, can cause destruction of the gate oxide and ultimately degrade the device operation. Steps must be taken to stop the generation of static electricity as much as possible, and quickly dissipate it when it occurs. Environmental control must be adequate. When it is dry, a humidifier should be used. This is recommended to avoid using insulators that can easily build up static electricity. Semiconductor devices must be stored and transported in an anti-static container, static shielding bag or conductive material. All test and measurement tools including work benches and floors must be grounded. The operator must also be grounded using a wrist strap. Semiconductor devices must not be touched with bare hands. Similar precautions must be taken for printed circuit boards with mounted semiconductor devices.
2. Processing at power-on

   The state of the product is undefined at the time when power is supplied. The states of internal circuits in the LSI are indeterminate and the states of register settings and pins are undefined at the time when power is supplied. In a finished product where the reset signal is applied to the external reset pin, the states of pins are not guaranteed from the time when power is supplied until the reset process is completed. In a similar way, the states of pins in a product that is reset by an on-chip power-on reset function are not guaranteed from the time when power is supplied until the power reaches the level at which resetting is specified.
3. Input of signal during power-off state

   Do not input signals or an I/O pull-up power supply while the device is powered off. The current injection that results from input of such a signal or I/O pull-up power supply may cause malfunction and the abnormal current that passes in the device at this time may cause degradation of internal elements. Follow the guideline for input signal during power-off state as described in your product documentation.
4. Handling of unused pins

   Handle unused pins in accordance with the directions given under handling of unused pins in the manual. The input pins of CMOS products are generally in the high-impedance state. In operation with an unused pin in the open-circuit state, extra electromagnetic noise is induced in the vicinity of the LSI, an associated shoot-through current flows internally, and malfunctions occur due to the false recognition of the pin state as an input signal become possible.
5. Clock signals

   After applying a reset, only release the reset line after the operating clock signal becomes stable. When switching the clock signal during program execution, wait until the target clock signal is stabilized. When the clock signal is generated with an external resonator or from an external oscillator during a reset, ensure that the reset line is only released after full stabilization of the clock signal. Additionally, when switching to a clock signal produced with an external resonator or by an external oscillator while program execution is in progress, wait until the target clock signal is stable.
6. Voltage application waveform at input pin

   Waveform distortion due to input noise or a reflected wave may cause malfunction. If the input of the CMOS device stays in the area between V_{IL} (Max.) and V_{IH} (Min.) due to noise, for example, the device may malfunction. Take care to prevent chattering noise from entering the device when the input level is fixed, and also in the transition period when the input level passes through the area between V_{IL} (Max.) and V_{IH} (Min.).
7. Prohibition of access to reserved addresses

   Access to reserved addresses is prohibited. The reserved addresses are provided for possible future expansion of functions. Do not access these addresses as the correct operation of the LSI is not guaranteed.
8. Differences between products

   Before changing from one product to another, for example to a product with a different part number, confirm that the change will not lead to problems. The characteristics of a microprocessing unit or microcontroller unit products in the same group but having a different part number might differ in terms of internal memory capacity, layout pattern, and other factors, which can affect the ranges of electrical characteristics, such as characteristic values, operating margins, immunity to noise, and amount of radiated noise. When changing to a product with a different part number, implement a system-evaluation test for the given product.

Notice

1. Descriptions of circuits, software and other related information in this document are provided only to illustrate the operation of semiconductor products and application examples. You are fully responsible for the incorporation or any other use of the circuits, software, and information in the design of your product or system. Renesas Electronics disclaims any and all liability for any losses and damages incurred by you or third parties arising from the use of these circuits, software, or information.
2. Renesas Electronics hereby expressly disclaims any warranties against and liability for infringement or any other claims involving patents, copyrights, or other intellectual property rights of third parties, by or arising from the use of Renesas Electronics products or technical information described in this document, including but not limited to, the product data, drawings, charts, programs, algorithms, and application examples.
3. No license, express, implied or otherwise, is granted hereby under any patents, copyrights or other intellectual property rights of Renesas Electronics or others.
4. You shall not alter, modify, copy, or reverse engineer any Renesas Electronics product, whether in whole or in part. Renesas Electronics disclaims any and all liability for any losses or damages incurred by you or third parties arising from such alteration, modification, copying or reverse engineering.
5. Renesas Electronics products are classified according to the following two quality grades: “Standard” and “High Quality”. The intended applications for each Renesas Electronics product depends on the product’s quality grade, as indicated below.

   "Standard": Computers; office equipment; communications equipment; test and measurement equipment; audio and visual equipment; home electronic appliances; machine tools; personal electronic equipment; industrial robots; etc.

   "High Quality": Transportation equipment (automobiles, trains, ships, etc.); traffic control (traffic lights); large-scale communication equipment; key financial terminal systems; safety control equipment; etc.

   Unless expressly designated as a high reliability product or a product for harsh environments in a Renesas Electronics data sheet or other Renesas Electronics document, Renesas Electronics products are not intended or authorized for use in products or systems that may pose a direct threat to human life or bodily injury (artificial life support devices or systems; surgical implantations; etc.), or may cause serious property damage (space system; undersea repeaters; nuclear power control systems; aircraft control systems; key plant systems; military equipment; etc.). Renesas Electronics disclaims any and all liability for any damages or losses incurred by you or any third parties arising from the use of any Renesas Electronics product that is inconsistent with any Renesas Electronics data sheet, user’s manual or other Renesas Electronics document.
6. When using Renesas Electronics products, refer to the latest product information (data sheets, user’s manuals, application notes, “General Notes for Handling and Using Semiconductor Devices” in the reliability handbook, etc.), and ensure that usage conditions are within the ranges specified by Renesas Electronics with respect to maximum ratings, operating power supply voltage range, heat dissipation characteristics, installation, etc. Renesas Electronics disclaims any and all liability for any malfunctions, failure or accident arising out of the use of Renesas Electronics products outside of such specified ranges.
7. Although Renesas Electronics endeavors to improve the quality and reliability of Renesas Electronics products, semiconductor products have specific characteristics, such as the occurrence of failure at a certain rate and malfunctions under certain use conditions. Unless designated as a high reliability product or a product for harsh environments in a Renesas Electronics data sheet or other Renesas Electronics document, Renesas Electronics products are not subject to radiation resistance design. You are responsible for implementing safety measures to guard against the possibility of bodily injury, injury or damage caused by fire, and/or danger to the public in the event of a failure or malfunction of Renesas Electronics products, such as safety design for hardware and software, including but not limited to redundancy, fire control and malfunction prevention, appropriate treatment for aging degradation or any other appropriate measures. Because the evaluation of microcomputer software alone is very difficult and impractical, you are responsible for evaluating the safety of the final products or systems manufactured by you.
8. Please contact a Renesas Electronics sales office for details as to environmental matters such as the environmental compatibility of each Renesas Electronics product. You are responsible for carefully and sufficiently investigating applicable laws and regulations that regulate the inclusion or use of controlled substances, including without limitation, the EU RoHS Directive, and using Renesas Electronics products in compliance with all these applicable laws and regulations. Renesas Electronics disclaims any and all liability for damages or losses occurring as a result of your noncompliance with applicable laws and regulations.
9. Renesas Electronics products and technologies shall not be used for or incorporated into any products or systems whose manufacture, use, or sale is prohibited under any applicable domestic or foreign laws or regulations. You shall comply with any applicable export control laws and regulations promulgated and administered by the governments of any countries asserting jurisdiction over the parties or transactions.
10. It is the responsibility of the buyer or distributor of Renesas Electronics products, or any other party who distributes, disposes of, or otherwise sells or transfers the product to a third party, to notify such third party in advance of the contents and conditions set forth in this document.
11. This document shall not be reprinted, reproduced or duplicated in any form, in whole or in part, without prior written consent of Renesas Electronics.
12. Please contact a Renesas Electronics sales office if you have any questions regarding the information contained in this document or Renesas Electronics products.

(Note1) “Renesas Electronics” as used in this document means Renesas Electronics Corporation and also includes its directly or indirectly controlled subsidiaries.

(Note2) “Renesas Electronics product(s)” means any product developed or manufactured by or for Renesas Electronics.

(Rev.4.0-1 November 2017)

Corporate Headquarters

TOYOSU FORESIA, 3-2-24 Toyosu,
Koto-ku, Tokyo 135-0061, Japan
www.renesas.com

Trademarks

USB Type-C™ and USB-C™ are trademarks of USB Implementers Forum. Renesas and the Renesas logo are trademarks of Renesas Electronics Corporation. All trademarks and registered trademarks are the property of their respective owners.

Contact information

For further information on a product, technology, the most up-to-date version of a document, or your nearest sales office, please visit: www.renesas.com/contact/.