

18 Intrinsic ID B.V. – all rights reserved. Information contained herein is proprietary to Intrinsic ID B.V. ipt of this document does not imply any license under any intellectual property rights of Intrinsic ID.

DemoKey 2.4

Demonstrator Quickstart Guide

Version2.0DateSeptember 6, 2018StatusApprovedReferenceDemonstrator Quickstart Guide

www.intrinsic-id.com



Copyright in this document rests with Intrinsic ID B.V. Reproduction or publication in any medium of this document, in whole or in part, is expressly prohibited without the prior written permission of Intrinsic ID. Intrinsic ID reserves the right to make any changes to this document without prior notice. The contents of this document is provided AS-IS and without any warranties or guarantees as to accuracy or completeness. Receipt or possession of this document conveys no license under any patent or other intellectual property right of Intrinsic ID.

Intrinsic ID®, QuiddiKey®, QuiddiCard®, BroadKey™, DemoKey™, Citadel™, Spartan™, Confidentio™, Fuzzy ID™ and other designated brands included herein are trademarks of Intrinsic ID B.V. All other trademarks are the property of their respective owners.

This product contains code which is copyright 2014 Kenneth MacKay and licensed under the BSD license:

Copyright (c) 2014, Kenneth MacKay All rights reserved.

Redistribution and use in source and binary forms, with or without modification,

are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Demonstrator Quickstart Guide



History Information

Version	Date	Change Description	Modified by:	Reviewed by:
1.0	2017-09-21	First release.	PB	OH, SG, TA, ML
	20			
2.0	2018-08-07	New Product Naming Update.	DA	BO



Table of Contents

History Information	3
Table of Contents	4
 Introduction Introduction Purpose Definitions, Acronyms and Abbreviations Overview 	5 5 5 6
2. Prerequisites2.1. Required Software and Tools2.2. Dip Switch Settings	7 7 7
 Running the Demonstrator Building the Demonstrator Image Running and Debugging the Demonstrator 	8 8 10
 4. Functional Overview 4.1. Demonstrator Flow 4.1.1. Enrollment Procedure 4.1.2. Reconstruction Procedure 	12 12 13 14



1. Introduction

1.1. Purpose

The purpose of the demonstrator is to show how unclonable keys can be generated from the unique physical properties of the underlying hardware using Intrinsic ID's DemoKey. This product is based on the concept of SRAM Physical Unclonable Functions (PUFs), where the underlying SRAM is used as a silicon fingerprint from which device-unique keys can be derived. The demonstrator shows the derivation of an ECC 256 bit private key from the SRAM PUF. In addition, it proves that the same key will be reconstructed each time, even after power cycles.

The public key corresponding to the derived ECC 256 bit private key can be computed to create an ECC keypair. This keypair in turn can be used for creating device certificates or authenticating the hardware.

DemoKey is a simulation version mimicking the behavior and functionality of the Intrinsic ID's production version BroadKey. In order to allow developers to effortlessly migrate from DemoKey to BroadKey, the API's are compatible.

After going through this Quickstart Guide, before adding the DemoKey software in a userdefined project, it is highly recommended to read the *IID-DK2-4-DS.pdf* and IID-DK2-4-IG.*pdf*.

Disclaimer: DemoKey is a simulation version of the commercial BroadKey product, intended explicitly for demonstration and evaluation purposes only.

1.2. Definitions, Acronyms and Abbreviations

AC	Activation Code
API	Application Programming Interface
bk_	BroadKey (as prefix in function/variable names)
IP	Intellectual Property
NVM	Non-Volatile Memory
PUF	Physical Unclonable Function
SD	Start-up Data (of uninitialized SRAM)
SRAM	Static Random Access Memory



1.3. Overview

This document is organized as follows:

- Section 2 contains the prerequisites needed to run the demonstrator.
- Section 3 contains practical details for running and debugging the demonstrator.
- Section 4 contains a functional overview of the demonstrator's execution flow.

© 2018 Intrinsic ID B.V. – all rights reserved. The information contained herein is proprietary to Intrinsic ID B.V. Receipt of this document does not imply any license under any intellectual property rights of Intrinsic ID.



2. Prerequisites

2.1. Required Software and Tools

- e² studio Integrated Solution Development Environment (ISDE)
- Synergy Software Package (SSP), Release 1.4.1 •
- DK-S7G2 Development Kit •

Please read Development Toolbox Setup Guide.pdf to learn how to install the ISDE and SSP package and how to set up and connect the DK-S7G2 kit.

2.2. Dip Switch Settings

In order to be able to run the demonstrator, the S5 DIP switches on the main board must be configured as indicated below:



DIP switch name	Setting
BOOT	Off
EXP	Off
JTAG	On
PBs	On^1
PMOD	Off
ENET1	Off^1
QSPI	On^1
DRAM	On

© 2018 Intrinsic ID B.V. – all rights reserved. The information contradient breating into the contraction ID B.V. Resection for the occument does not imply any litense under any initelectual property rights of intrinsic ID.

¹ Switch setting differs from the setting as seen in the Development Toolbox Setup Guide.



3. Running the Demonstrator

3.1. Building the Demonstrator Image

The first step is building the demonstrator project into an executable image that can be flashed and run on the board.

The project, named IID_DemoKey_DKS7G2, must be imported in an e² studio workspace. In the menu click on **File** and select **Import...**

e²	C/C++ - e2 studio		el Import	□ ×
File	Edit Source Refactor Navigate New Open File	Search Project Renesas Alt+Shift+N >	Select Create new projects from an archive file or directory.	Ľ
	Close	Ctrl+W	Select an import source: type filter text	
	Close All Save Save As Save All	Ctrl+Shift+W Ctrl+S Ctrl+Shift+S	✓	^
	Revert Move Rename	F2	 Existing Projects into Workspace File System HEW Project Import KPIT GNUARM Project to GCC ARM Embedded Preferences 	
£)	Refresh Convert Line Delimiters To	F5 >	 Rename & Import Existing C/C++ Project into Workspace Renesas CA78K0R Project Renesas Common Project File 	
	Print Switch Workspace Restart	Ctrl+P) 🕑 UU++	~
	Import Export		() < Back Next > Einish	Cancel

In the **Import** dialog from the **General** category select **Existing Projects into Workspace**. Press **Next** to go to the **Import Projects** dialog.

Browse to the directory containing the **IID_DemoKey_DKS7G2** project and make sure that the **Copy projects into workspace** option is enabled. Check that the project is selected and press **Finish**.



mport Projects Select a directory to sear	ch for existing Eclipse projects.		Ê
Select root directory:	C:\iid\iid_demokey\e2Studio_Project	~	B <u>r</u> owse
○ Select <u>a</u> rchive file: <u>P</u> rojects:		_	Browse
IID_DEMOKEY_D	KS7G2 (C:\iid\iid_demokey\e2Studio_Projec	ct\IID_I	<u>S</u> elect All
		[Deselect All
		Ŧ	Pefrech
<		>	Ngiresii
 Options Search for nested previous for projects into w ☐ Hide projects that all 	ojects orkspace ready exist in the workspace	>	Ngirean
Coptions Search for nested prive Copy projects into w ☐ Hide projects that all Working sets	ojects orkspace ready exist in the workspace	>	Ngirean
< Options Search for nested pro Copy projects into w Hide projects that al Working sets Add project to work	ojects orkspace ready exist in the workspace	>	rgreat
< Options Search for nested pro Copy projects into w Hide projects that al Working sets Add project to work Working sets:	ojects orkspace ready exist in the workspace	•	Sglect

Now that the project is included in the Project Explorer, expand the project and double click on the **configuration.xml** file located in the project's root directory and wait for the file to be parsed and opened in the editor. Click on **Generate Project Content**, which will place all drivers for the board from the SSP package and place these in the project.

0
Generate Project Content

In order to build the imported project, right click on the project name and select **Build Project**. This will build the demonstrator firmware that can be programmed on the DK-S7G2 board.



3.2. Running and Debugging the Demonstrator

Before programming the firmware, confirm all cables are connected between the board and the PC running e^2 studio.

Verify the IID_DemoKey_DKS7G2 demonstrator project is selected in the **Project Explorer**, otherwise select it now. Click on the **Debug** button in the menu, select **Debug** from the **Run** menu or press **F11**.

Run	Window Help	
T	TraceX	>
Q,	Run	Ctrl+F11
to	Debug	F11
	Run History	>
	Run As	>
	Run Configurations	
	Debug History	>
	Debug As	>
	Debug Configurations	
	Toggle Breaknoint	Ctrl+Shift+B

The demonstrator firmware will now be flashed onto the board and the debug process will start.

If by any chance e² studio flashes the wrong program, it is possible to force the debugger to use the demonstrator by selecting **Debug Configurations** from the **Run** menu. This will open the **Debug Configurations** dialog. In this dialog under the section **Renesas GDB Hardware Debugging**, select the demonstrator project and press **Debug**.

••••

reate, manage, and run configurations	
ype filter text C C/C++ Application C C/C++ Application C C/C++ Remote Application C C/C++ Remote Application C C/C++ Remote Application C GDB Ardware Debugging C GDB Simulator Debugging C GDB Simulator Debugging (SH, RH850) G GHS Applet Java Applet Java Application L aunch Group	Name: IID_DEMOKEY_DKS7G2 Debug Main % Debugger Main % Debugger Debug hardware: 1-Link ARM Target Device: R7FS7G27H GDB Settings Connection Settings GDB Connection Settings Debug Tool Settings GDB Connection Settings Host name or IP address: O Connect to remote GDB server GDB port number: GDB port number: 61234 ADM port number: 61236
Remote Application Remote Debugger Remote Java Application © Renesas GDB Hardware Debugging [©] *ID_DEMOKEV_DKS7G2 Debug [local] [©] Renesas Linux Application [©] Renesas Linux Application [©] Target Communication Framework	GDB Command: S{eclipse_home}/DebugComp/arm-none-eabi-gdb Browse Variables Enable verbose mode Additional GDB Server Arguments
lter matched 19 of 21 items	< > Reyert Apply.

© 2018 Intrinsic ID B.V. – all rights reserved. The information contained herein is proprietary to Intrinsic ID B.V. Receipt of this document does not imply any license under any intellectual property rights of Intrinsic ID.

The debugger first halts the program at the entry point of the **Reset_Handler** function. Press the **Resume** button from the menu or press **F8** to continue. The debugger now halts at the **main** function. Again, press the **Resume** button or **F8**.

The demonstrator is now started and the user can interact with the demo.

Note: Since at this point the board is already flashed with the application, the demonstrator can be run without e^2 studio or the debugger.



© 2018 Intrinsic ID B.V. – all rights reserved. The information contradient breating into the contraction ID B.V. Resection for the occument does not imply any litense under any initelectual property rights of intrinsic ID.

4. Functional Overview

4.1. Demonstrator Flow

The software demonstrator includes both **Enrollment** (initial key derivation -S1 below) and **Reconstruction** (upon restart, re-deriving the same key -S2 below).

Steps of both procedures are shown on the display included in the Renesas *Synergy DK-S7G2* kit. The following flow chart depicts the general flow of the demo.



Figure 1 Demo execution flow

Note: The private key is written to flash as part of the **Enrollment** (S1) only for the purpose of comparing the key with the one derived in the **Reconstruction** (S2) step. In normal operation, the private (secret) key should never be stored in flash, since it will be reconstructed by DemoKey as part of the reconstruction (S2) process.

12 / 14



4.1.1. Enrollment Procedure

The first time the demo is started after (re)flashing the firmware, the user can only select enrollment. This is done by pressing the **S1** button on the board.

The iid_enrollment_procedure, as depicted in Figure 1, is executed. The result of the enrollment procdured can be seen on the display of the board, depicted in the figure below. The activation code created during enrollment is also used in the reconstruction and is therefore written to flash, this is described in more detail in the *Product Specification*.

INTRINSIC ID	
DemcKey v.2.4.0 initialized Press S1 for enrollment procedure Enrollment successfully executed!	
BK ECC CURVE NIST P256 Private Key valué (truncated): ef298dffee288cfeed2b8ffdec2a8efceb2d89fb	
Activation Code and Private Key written to Flash!	



4.1.2. Reconstruction Procedure

In order to test and view the reconstruction procedure (or run the enrollment procedure again), reset the board by pressing the **Reset** button on the board or by unplugging and re-inserting the power to the board.



The reconstruction procedure is only selectable when the enrollment procedure has been executed at least once. The reconstruction procedure can be started by pressing the S2 button on the board.

The iid_reconstruction_procedure, as depicted in Figure 1, is executed. The result of the enrollment procdure can be seen on the display of the board, depicted in the figure below.

