Irdeto Cloaked CA Agent VM Validator User Guide

Document Number	746893
Revision	4.0 (Approved)
Classification	Confidential
Date Issued	Nov 6, 201511/6/2015 3:00:00 PM

Documentation Feedback

Can this document be improved? If you think so, please send your comments to

CADocumentation@irdeto.com

Table of Contents

Change History

Rev.	Date Issued	Description
1.0	March 12, 2013	First release.
2.0	October 20, 2014	Updated the VM validator in Section 3.
3.0	November 07, 2014	Correct some description in Section 3.
4.0	September 21, 2015	Add some comments in Section 3.2.

Terms, Acronyms and Abbreviations

Term	Definition
FlexiFlash	A mechanism used by the Irdeto Cloaked CA Agent to upgrade its internal secure core.
Irdeto VM	The virtual machine inside the Irdeto Cloaked CA Agent for running the secure core.

Document Conventions

This document uses different text fonts, weights, and styles to signify specific meanings, as described below.

Text Convention	Definition
Bold Text	User interface elements, such as button names and menu items Example: In the **Configuration** dialog box, click **OK**.
Italic Text	Used to emphasize important words and to indicate cross-references. Example: Start server 1 *before* starting server 2.
`Monospaced Text`	Used with gray background to depict code blocks, text configuration files, screen output and other related text
`Bold Monospaced Text`	Used to depict commands that are typed in the command window and keywords

Notes, Tips, and Warnings

Notes provide additional important information that should be read, such as a brief explanation, a reinforcing comment, or offset information used to alert the reader of important information.

Tips provide additional information for advanced users, such as an alternate operation method or a keyboard shortcut.

Warnings alert the reader to possible serious consequences, such as service interruption or system failure.

1 Introduction

This document describes the Irdeto VM Validator and how device manufacturers can use it to verify VM performance.

FlexiFlash is an update mechanism used by the Irdeto Cloaked CA Agent to replace its internal secure core through EMM data. The internal secure core runs inside the Irdeto VM. The FlexiFlash upgrade method places additional performance requirements on the client device, therefore excessive ECM processing delays must be avoided. If the client device cannot meet the performance requirements, then either the device needs to be upgraded or FlexiFlash needs to be disabled.

To verify performance, Irdeto provides the VM Validator package to device manufacturers, which includes a library, test secure core file, and documents to aid the manufacturer.

1.1 Audience

This document is intended for the following audience:

- Support Engineers
- Device Manufacturers

2 Process

This verification process must be performed before beginning Irdeto Cloaked CA Agent integration, since the results of the verification is used to determine whether or not to enable FlexiFlash. Different deliverables are provided to manufacturers. The process workflow is described as below.

1. Device manufacturers provide their compiler and compile options to Irdeto.
2. Irdeto makes the Irdeto VM Validator package and sends it to manufacturers with the lab secure core file.
3. Manufacturers test the client device using the VM Validator and send the test results back to Irdeto CDI.
4. The CDI sends the test results to product groups who will determine whether FlexiFlash can be enabled on the client device.
5. Irdeto provides personalized deliverables to manufacturers for integration.

3 Irdeto Provided Package

This chapter describes the Irdeto VM Validator package and operational procedures.

3.1 Package Content

The package includes:

- IrdetoVMValidator.lib
  This library contains the testing logic needed by manufacturers for integration into their client device testing project. This library is generated by Irdeto using manufacturer provided compilers.
- SecureCore.bin
  - Must be the lab secure core
  - Provided by support engineers
  - TDES secure core or AES secure core
  - Can be loaded by the *UniversalClientSPI_File_LoadImage* SPI
- Include files
  - *irdeto_vm_validator_type.h* – The basic definition of the VM validator
  - *irdeto_vm_validator_api.h* – API declarations (currently, only Run() exists)
  - *irdeto_vm_validator_spi.h* – SPI methods which are called by *IrdetoVMValidator.lib*, The device manufacturer must implement all methods declared in this file.
- Examples

  Irdeto provides an example project (Visual studio 2010) for demonstrating how to integrate the Irdeto VM Validator for testing. Manufacturers can refer to this project when building their own projects.

For Irdeto Internal:
Irdeto support engineers can reference "./builds/vmvalidator_new/readme.txt" on TFS for helpful information about how to build the library and find other materials.

3.2 Performing the Test

When a new project is created and the IrdetoVMValidator is integrated, the application only needs to call ***Run(filename, loopCount)*** by including the *irdeto_vm_validator_api.h*.
filename*:* The name of the secure core, including the file path, such as "/usba0/securecore.bin"
loopCount: The number of times *EvaluateCWDK* and *DecryptControlWord* are run

To ensure that manufacturers have correctly integrated the validator, an example output is provided below for reference:

```
------------------------------------------------------------
Loop count: 100.
Opening bytecode file: TDESSecureCore.bin
Secure Core Version: 4.0.0
Load Time: 1170 milliseconds.
**************************************
Succeed in step 1 (EvaluateCWDK)  !
Total time: 18396 milliseconds.
Time per loop: 183 milliseconds.
**************************************
Succeed in step 2 (DecryptControlWord)  !
Total time: 14921 milliseconds.
Time per loop: 149 milliseconds.
**************************************
Test complete!
Quit.
```


The output above is interpreted as:

Loop count: 100 – The test is performed 100 times. Currently, it can be modified if required.

Opening bytecode file: TDESSecureCore.bin – This is the file name of the loaded secure core.

If loading the secure core file failed, then the "**Error: Failed to open bytecode file: TDESSecureCore.bin**" is displayed and the information below is now displayed.

Secure Core Version: 4.0.0 – This is the file version of the loaded secure core.

Load Time – This the time used to load the secure core byte code into the VM.

Succeed in step 1 (EvaluateCWDK) ! – This indicates that the first test step was successful. If failed, the "**EvaluateDecisionBlock execution failed!!!!!!!.**" is displayed.

If [Loop count] is set to 100, wait several minutes until the success message or failure message of step 1 appears.

Total time: 18396 milliseconds. – This is the total duration of step 1.

Time per loop: 183 milliseconds. – This is the running time of each EvaluateCWDK.

Succeed in step 2 (DecryptControlWord) ! − This indicates that the second test step was successful. If failed, the "**DecryptControlWord execution failed!!!!!!!.**" is displayed.

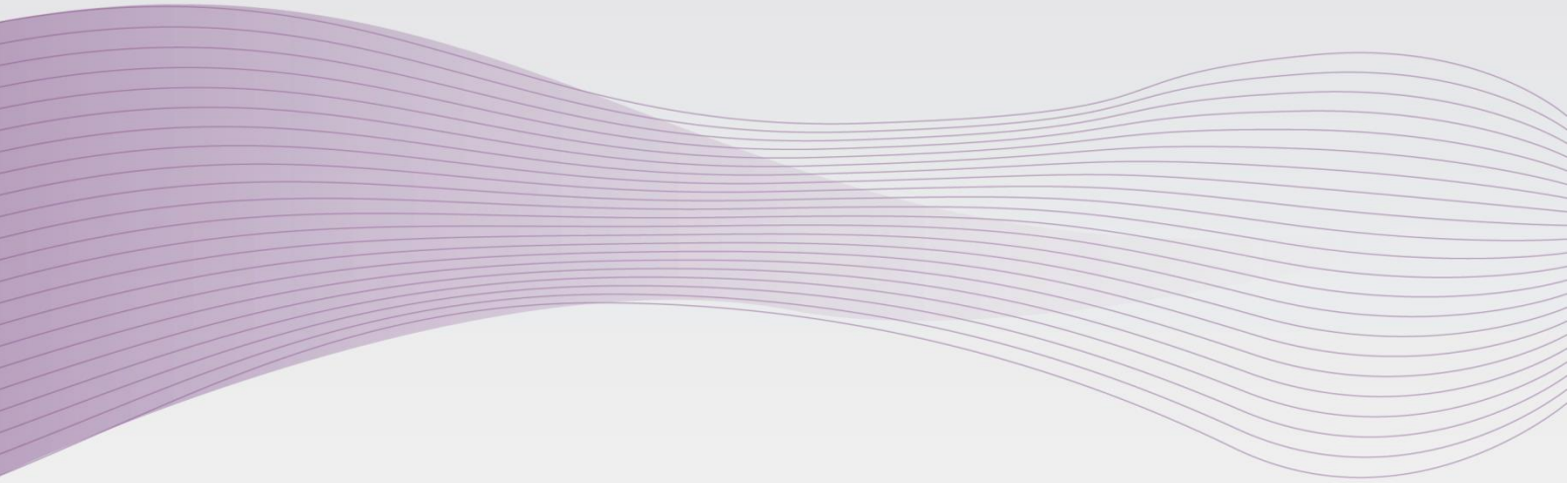
If [Loop count] is set to 100, wait several minutes until the success message or failure message of step 2 appears.

Total time: 14921 milliseconds – This is the total duration of step 2.

Time per loop: 149 milliseconds. – This is the running time of each DecryptControlWord.

Analysis of the results:

The final test result must be sent back to Irdeto without any manual changes. Irdeto determines whether the device needs to be improved to pass the test.



The Netherlands
Taurus Avenue 105
2132 LS Hoofddorp
Phone: +31 23 556 2222
Fax: +31 23 556 2240

China
F3/6, Sunflower Tower
37 Maizidian Street
Chaoyang District
Beijing 100125, P.R.C
Phone: +86 10 8527 6460
Fax: +86 10 8527 5685

Canada
2500 Solandt Road
Suite 300
Ottawa, ON K2K 3G5
Phone: +1 613 271 9446
Fax: +1 613 271 9447

U.S.A.
1741 Technology Drive
Suite 130
San Jose, CA 95110
Phone: +1 408 492 8500
Fax: +1 408 436 8335

www.irdeto.com