RTA-SWCL v3.2.0

RTA-SWCL Release Notes

Status: Release

DRIVING | EMBEDDED EXCELLENCE

Copyright

Document RTA-SWCL Release Notes v3.2.0 R01 EN - 03.2019

Contents:

1 Introduction

1.1 Definitions and Abbreviations

Term/Abbreviation	Definition
BSW	AUTOSAR Basic Software module. AUTOSAR defines a comprehensive BSW architecture consisting of OS, RTE, service, interface and driver BSW modules that provide a device independent ECU abstraction to ASW and thus promote SWC reuse and relocation. See *Product Definition* for a list of AUTOSAR BSW modules.
EHI	ETAS Help Desk International
HW	Hardware
KIR	Known Issue Report – For severe Problem Reports which occur after a release, ETAS has introduced the Known Issue Report to inform affected customer immediately. The current Known Issues of former versions can be found on the ETAS website: http://www.etas.com/kir
PR	Problem Report
SW	Software

1.2 References

1. RTA-SWCL Reference Guide, v3.2.0, ETAS GmbH

1.3 Conventions

The following typographical conventions are used in this document:

Choose **File->Open**.	Menu commands are shown in boldface.
Click **OK**.	Buttons are shown in boldface.
Press <ENTER>.	Keyboard commands are shown in angled brackets.
The ‘Open File’ dialog box is displayed.	Names of program windows, dialog boxes, fields, etc. are shown in quotation marks.
Select the file *setup.exe*	Text in drop-down lists on the screen, program code, as well as path- and file names are shown in italics.
A *distribution* is always a one-dimensional table of sample points.	General emphasis and new terms are set in italics.

1.4 User Documentation

The RTA-SWCL user documentation in PDF format can be found on the CD.

2 Product Definition

2.1 Functions at a Glance

This initial release of RTA-SWCL provides a library of software-based cryptographic functions which can be utilised in an RTA-BSW project via calls from the Rba_CryptoBCL module.

The cryptographic functions provided by the module are broadly defined by the following categories:

- Block Ciphers - elementary component of a crytographic system usually reserved for bulk data encryption.
- Hash Functions - algorithms which map arbitrarily-sized data to a fixed-size value (hash).
- Deterministic Random Bit Generators - generation of pseudo-random byte values for use in keys and other protocols.
- Message Authentication Codes - generation of short codes (tags) used to authenticate message sources and integrity.
- Non-authenticated Encryption Mechanisms - basic, less secure encryption algorithms.
- Common Public Key Cryptography Routines - algorithms for use with public-key (key pair) cryptography schemes.
- Digital Signatures - routines for signing of sent messages (generation) and verification of received messages.
- Diffie-Hellman Key Exchange - algorithms used to compute ‘shared secret’ keys between two parties.

2.2 General Description

2.2.1 System Prerequisites

The following minimum system prerequisites have to be met:

Required Hardware	• 1.9 GHz PC • 4 GB RAM • DVD-ROM drive • Network adapter • Graphics with a resolution of at least 1024 x 768, 32 MB RAM
Required Operating System	Windows® 7, 64-bit, Windows® 8.1, 64-bit
Required Free Disk Space	5 GB (not including the size for application data)

2.2.2 Software Prerequisites

ISOLAR-AB	v4.0 (with RTA-BSW v3.1.0) or v5.0.1 (with RTA-BSW v3.2.0)
RTA-BSW	v3.1.0 or v3.2.0

2.3 Delivery

The software is delivered on a CD including the RTA-SWCL software, documentation, tools, utilities, and further information. All software documentation is available in the Portable Document Format (PDF), which requires Adobe® Reader®.

2.4 Installation

To import the RTA-SWCL module source files into your RTA-BSW project, follow these steps:

1. In ‘ISOLAR-AB’, open your project and then select the ‘FileSystem Navigator’ tab.
2. In ‘Windows Explorer’, select the *RTA-SWCL* source folder and then drag it into the ‘Filesystem Navigator’ window.

You should now see the required folders created under the root folder of your project filesystem, similar to those shown in the example below.

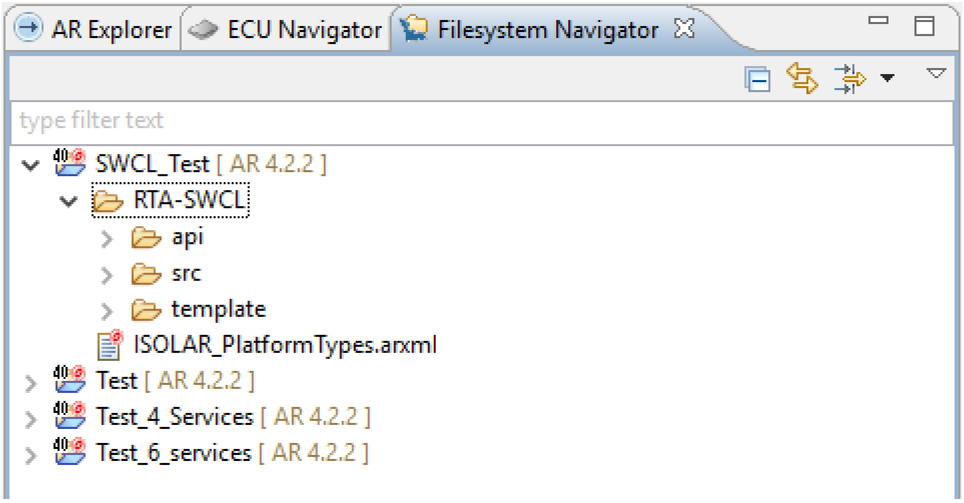

Fig. 2.1: Example Project Folder Structure

2.5 Licensing

You will need the RTA-SEC license with RTA-BSW to use the code that calls into RTA-SWCL.

The RTA-BSW Getting Started Guide describes how to obtain and activate licenses.

2.6 Compatibility

RTA-SWCL v3.2.0 ensures compatibility with the following other ETAS products and product versions.

Product	Version
ISOLAR-AB	v4.0, v5.0.1
RTA-RTE	v6.5.0
RTA-OS	v5.5.11
RTA-BSW	v3.1.0, v3.2.0

3 Changes and Defects Fixed

3.1 RTA-SWCL v3.2.0

3.1.1 New Features

The supported version for this release is AUTOSAR v4.3.0

This is the first release of the RTA-SWCL module. It provides an API containing the function definitions required to support cryptographic operations through the AUTOSAR Cryptographic Abstraction Library. For details on which cryptographic methods are provided, please refer to the RTA-SWCL Reference Guide.

3.1.2 Known Issues Resolved

There are no known issues resolved in this release of the module.

4 Known Issues

4.1 Arithmetic Shifts in DH Curve 25519

The Diffie-Hellman Curve25519 algorithm implemented in the module uses left and right bit-shift operations. The behaviour of these operations is expected to be as follows:

- Left-shift operations behave in a similar way for both signed and unsigned integers.
- Right-shift operations are assumed to perform an arithmetic-right shift which fills the vacant positions with the most significant bit.

This behaviour is defined in the ANSI C standard. Most compilers will conform to this standard, however you should be aware that non-standard compilers may produce object code with different behaviour for bit-shift operations which may produce unintended results when using this cryptographic algorithm.

5 Hotfix Information

No hotfixes for RTA-SWCL are available at this time.

6 Contact, Support and Problem Reporting

6.1 ETAS HQ

ETAS GmbH Borsigstraße 24 70469 Stuttgart Germany	Phone:	+49 711 3423-0
	Fax:	+49 711 3423-2106
	WWW:	www.etas.com

6.2 ETAS Subsidiaries and Technical Support

For details of your local sales office as well as your local technical support team and product hotlines, take a look at the ETAS website:

ETAS subsidiaries	WWW:	www.etas.com/en/contact.php
ETAS technical support	WWW:	www.etas.com/en/hotlines.php

6.2.1 RTA Hotline

The RTA hotline is available to all RTA users with a valid support contract.

- rta.hotline.uk@etas.com
- +44 (0)1904 562624. (0900-1730 GMT/BST)

Please provide support with the following information:

- Your support contract number.
- Your AUTOSAR XML and/or OS configuration files.
- Reproduction steps that result in an error message.
- The version of the ETAS tools you are using.