IAR SYSTEMS SECURE THINGZ

RX Ecosystem Partner Solution

Compliance Suite for Renesas RX

1.Solution Summary

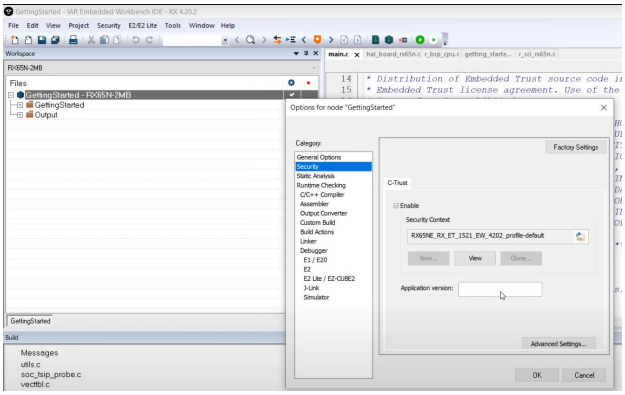
Shrink-wrapped security solution

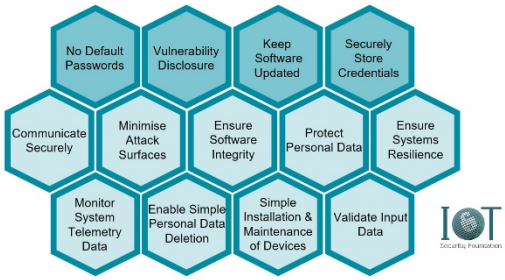
Compliance Suite for Renesas RX includes security development tools and practical guidance, delivering a shrink-wrapped solution for organizations to ensure security legislation compliance in IoT applications based on Renesas RX microcontrollers.

2. Features/Benefits

- Preconfigured Security Context – Ensuring all necessary security and encryption are automatically included in your application
- Secure Boot Manager – Securing the overall boot process to protect the device
- C-Trust – Extension to IAR Embedded Workbench for RX enabling secure, encrypted code
- C-STAT – Static code analysis tool ensuring code quality
- Practical guidance – Package of courses with hands-on guides led by Secure Thingz' in-house security experts, covering the topics *Introduction to Security, Secure Development Workflow, Legislation and Compliance Requirements, Meeting the IoTSF Compliance Framework*

3. Diagrams/Graphics





4. Target Markets and Applications

- Industrial automation
- Automotive
- Consumer electronics
- Medical technology and wearables
- Smart metering

www.iar.com/renesas

2021.07

Ensure legislation compliance for your application

With new legislation for IoT security and privacy rapidly being introduced globally, compliance according to these regulations is a challenge for organizations and developers working with embedded applications. For your existing or new application, this means that it has to meet a new set of baseline standards. The good news is that we can help you to comply with the new regulations. Compliance Suite for Renesas RX is specifically designed for applications based on the Renesas RX family of microcontrollers (MCUs) and delivers a shrink-wrapped security solution including:

- Preconfigured Security Context
- Secure Boot Manager
- Practical guidance
- C-Trust extension to IAR Embedded Workbench for RX
- C-STAT static code analysis tool

Evolving IoT security legislation

The Consumer IoT Security Standard EN 303 645, based on the 13 Best Practices Guidelines evolved by the IoT Security Foundation and UK Government, is widely regarded as the security benchmark for Consumer IoT. Both the standard and the guidelines contain core requirements for applications, which developers should achieve.

The Preconfigured Security Context included with Compliance Suite targets a broad set of the Best Practice requirements. A Preconfigured Security Context includes all the necessary security and encryption settings for protecting an application against security threats such as IP theft, malware injection, illegal access, copying or counterfeiting. This innovative technology ensures that you remain in control of your application.

What are the 13 IoT Security Best Practices?

- Defined by the IoT Security Foundation
- Adopted by the UK Government
- Adopted by the EU in ETSI EN 303 645
- Supported by US Cybersecurity Improvement Act

IoT Security Foundation

The IoT Security Foundation is a non-profit organization dedicated to driving security excellence. It is a collaborative, vendor-neutral, international initiative aspiring to be the expert resource for sharing knowledge, best practice and advice. As a founding member of the IoT Security Foundation, Secure Thingz has been involved in the creation of best practices, compliance and vulnerability disclosure for over 5 years.

www.iar.com/renesas