DA1469x_59x Security Integration Guide

This application note provides suggestions for the integration of Renesas Electronics Connectivity devices DA14695, DA14592 and their variants into products that must address cybersecurity concerns. The target audience is the security development team of manufacturers of such products.

The EN 18031-1:2024 and EN 18031-2:2024 standards are used as a baseline, but the mentioned approach and security integration principles can apply for other similar specifications.

Contents

Figures

Tables

1. Terms and Definitions

Bluetooth® LE	Bluetooth Low Energy
BTC	Bicycle Trip Computer
DUT	Device Under Test
JTAG	Joint Test Action Group
LE	Low Energy
MITM	Man in the Middle
OTP	One Time Programmable.
RAM	Random Access Memory
RED	Radio Equipment Directive
UART	Universal Asynchronous Receiver Transmitter

2. References

[1] DA1469x Datasheet, Renesas Electronics.

[2] DA1459x Datasheet, Renesas Electronics.

[3] SW-B-001, DA1469x SDK, Release Notes, Renesas Electronics.

[4] R18TU0006EE0120, DA1459x SDK, Release Notes, Renesas Electronics.

[5] DA1469x Software Platform Reference, https://www.renesas.com/en/document/mat/um-b-092-da1469x-software-platform-reference-manual, Manual, Renesas Electronics.

[6] DA1459x Software Platform Reference, Manual, https://www.renesas.com/en/document/mat/da1459x-software-platform-reference-manual], Renesas Electronics.

[7] DA1469x Secure Boot Tutorial, https://www.renesas.com/en/document/gde/da1469x-secure-boot-tutorial, Renesas Electronics.

[8] DA1459x Secure Boot Mechanism, https://www.renesas.com/document/gde/da1459x-tutorial-secure-boot, Renesas Electronics.

[9] CVE-2024-25076/77Advisory, https://www.renesas.com/en/document/rep/id202400001-da1469x-secure-boot-vulnerabilities, Renesas Electronics.

Note 1 References are for the latest published version, unless otherwise indicated.

3. Introduction

This guide is intended for the equipment manufacturer that wants to launch products that comply with cybersecurity regulations. Specifically, it describes the steps to be followed for assessing the security of products based on Renesas Electronics Connectivity devices like DA14695, DA14592, corresponding modules and variants.

Before proceeding, you need to understand and acknowledge the following three statements:

- Using Renesas Electronics Connectivity devices and following this guide provides no guarantee of conformity. Each end-product has specific security requirements that must be fully assessed on their own.
- Conforming to a specific standard or regulation does not guarantee the product is secure, only that it integrates protection mechanisms that at the time of the assessment were considered adequate for the specific product and its intended operating environment.
- There are other ways to protect a product which may not be described in this guide, or even in the referenced standards. Not following this guide or not adhering to the referenced standards does not mean a product does not comply with cybersecurity regulation.

3.1 Cybersecurity Regulation and the EN 18031-x Standards

There are numerous standards and regulations relating to cybersecurity. In this guide is used the EN 18031-x family of standards and specifically:

- EN 18031-1 which applies to network connected radio equipment
- EN 18031-2 which applies to network connected radio equipment, Childcare devices, Toys and Wearables

These standards have been harmonized to serve as evidence of conformity with the RED (Radio Equipment Directive) Clauses 3.3(d), and 3.3(e). A product in scope of 3.3(d) and/or 3.3(e) must conform to bear the CE mark. Consult your CE marking consultant or internal experts for more information.

Renesas Electronics tested the conformity of the mentioned devices, modules and development kits against these clauses. A product manufacturer cannot leverage Renesas Electronics declaration of conformity. Following this guide makes it easier to achieve a conforming product. But it is always the responsibility of the product manufacturer to run your own analysis and testing, and to prepare your own declaration of conformity.

3.2 How to Read this Guide

This guide uses a fictional product example and takes the reader briefly through the security analysis steps. Run such an exercise at the definition phase of a new product, so that the product architecture considers cybersecurity from the start. It is good practice to follow a secure-by-design development process. However, this document does not deal with process but only with Product security.

At various points, we refer to Recommendations and Good Practices. These are marked in bold fonts with the corresponding "Recommendation" or "Good Practice" wording, so that they can be identified faster.

3.3 Bicycle Trip Computer as an Example

This BTC is intended for bicycle riders who can use it alone or expand it with peripheral sensing and control devices (auxiliary).

The BTC communicates with a tablet, a smartphone or a smartwatch through a Bluetooth Low Energy (LE) link. An authorized user can control and configure the product though the Bluetooth LE link, over a smartphone or tablet.

The BTC has an integrated display. This enables it to show information either from its own sensors or from auxiliary devices. This information can also be stored in Flash memory or can be transferred asynchronously and at slow speed through the Bluetooth interface.

Figure 1 shows a block diagram of the BTC and its connection over Bluetooth LE to a Smartphone or Tablet peer device.

The block diagram also shows the DA14695 device included in the module (DA14695MOD). If the end-product uses the bare device on the main board, similar analysis applies.

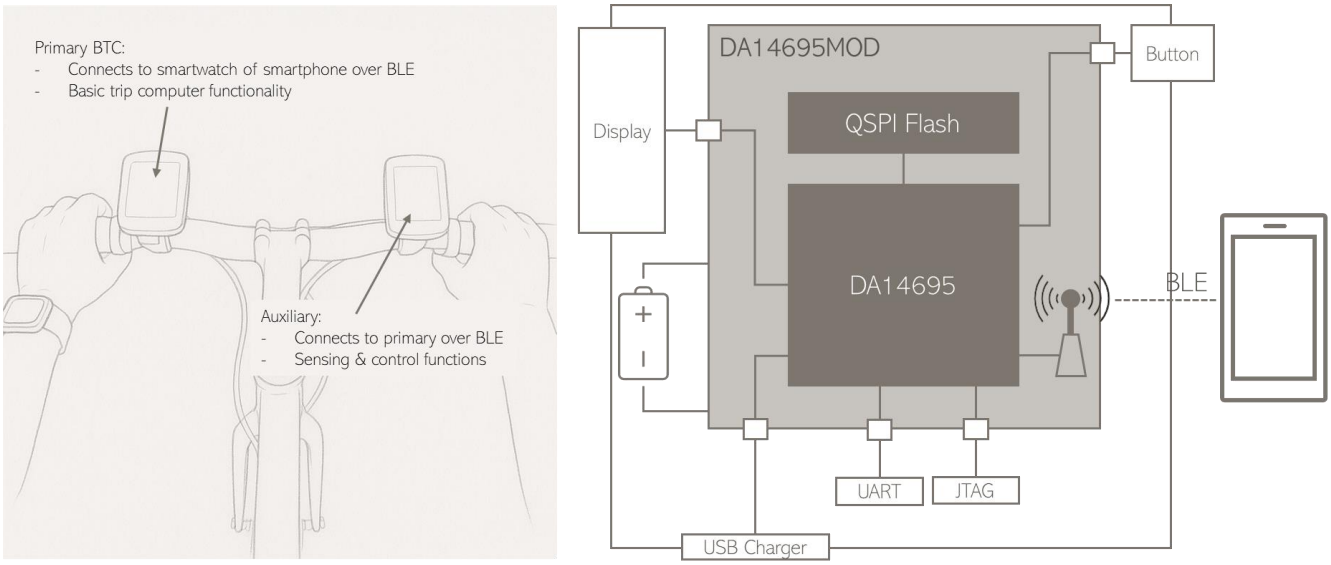

Figure 1. Example Product — A Bicycle Trip Computer (BTC)

4. Cybersecurity Analysis of the Product

When analyzing the product, it starts by identifying the interfaces that it exposes, the assets that need protection and the mechanisms that are used for protecting them. The analysis is not complete until we assess all security risks that remain in the product.

4.1 Interfaces

The interfaces can be classified in four categories:

- Network interfaces
  - In the example product, there is only one network interface; the wireless interface which uses the Bluetooth® LE protocol for communication to a peer device (like a smartphone, tablet or smartwatch).
- User interfaces
  - In the example product, there is one user interface on the product itself and another user interface that connects to the system through the Bluetooth LE Network Interface.
    - Display: this is an output interface that can show information collected by various sensors or auxiliary devices.
    - Button: this is a Yes/No input interface. It is not used for normal operation of the product but only at configuration by the authorized user. To protect from unauthorized access, it is not readily available on the BTC but can only be accessed by unscrewing and opening the battery department. **It is a good practice to mechanically protect user interfaces that can be used for configuring the device by authorized users, especially if the product is intended to be normally used by non-authorized users.**
    - Smartphone Application UI: this is an elaborate user interface that allows a user to control and interact with the BTC. It also provides advanced features for configuration of the BTC from the authorized user. **It is strongly recommended that applications on peer devices implement different user privileges for generic users and authorized users (especially in Toys and Childcare devices), that can be accessed only by using strong passwords.**
- Machine interfaces
  - A machine interface is used when another device directly connects to the product. In the example product we might consider the connected smartphone as another device, and the Bluetooth LE connection as a machine interface. However, we are already considering this for our security analysis as a "network interface". Therefore, there is only one machine interface:
    - Data coming from auxiliary interfaces. This is an interface that feeds sensing and control data in the product for storage or for transfer over the Bluetooth LE network interface. The stored data may contain private information and should therefore be protected from unauthorized access. For example, a GPS auxiliary device could provide the geographical location of the bicycle and the rider**. It is good practice to treat all data that is stored on the device as private.**
- Physical interfaces, including the ones used for debugging
  - The above-mentioned user interfaces rely on physical connections and are considered there for our security analysis.
  - In the example, there are two more physical interfaces:
    - The JTAG interfaces. These are debug interfaces and are exclusively used during product development and testing. Before the product reaches the market, the JTAG interfaces are disabled. **It is strongly recommended that both JTAG interfaces are always disabled by setting the corresponding OTP flags of Renesas Electronics device at the end of the production cycle and before the product leaves the factory floor.**
    - The UART Interface. This is used on the factory floor during production. Renesas Electronics Connectivity devices have a feature called UART-boot which allows you to download special firmware in RAM. We program such firmware so that UART behaves as a debug interface allowing program/read Flash and OTP. Downloading this special firmware is not allowed after the product leaves the factory floor, by disabling UART-boot in the OTP settings. **It is strongly recommended to disable UART-boot at the end of the production cycle and before the product leaves the factory floor.**

4.2 Assets

The interfaces may provide access to various keys, data, code or other information which should be protected. These assets can be classified as:

- Network Assets
  - The Bluetooth Stack, including the information and data that it communicates. In the example product, the Bluetooth stack is used in two configurations:
    - Paired, when the authorized user needs access to the device for configuration or update.
    - Public, when a non-authorized user (a child) uses a bicycle equipped with the BTC. In this analysis we assume that while riding, no privacy or security related information can be accessed.
- Privacy Assets
  - User data that is collected and stored or communicated. In the example product, such data might be sensor readings, usage patterns, GPS location, and so on.
    - When an unauthorized user (a child) is riding, such data may be stored but cannot be retrieved or communicated. One must be an authorized user (or the child's parent) to access it.
    - It is good practice to treat all data that is stored on the device as private.
- Security Assets
  - The application firmware — allows to read the application firmware is not a security concern, although it is still necessary to protect the IP. But protecting it from manipulation is critical, as through the application firmware someone can access all other interfaces and assets.
  - The user application — although not part of the product itself, the user application that runs on the smartphone is considered an associated service that runs on a peer device. If our example product, the user application supports two modes:
    - Authorized (adult) user — allows configuration of the BTC, software updates, Readout of stored data, Factory reset and so on.
    - Child — allows only temporary interaction with the BTC, and so on, selection of displayed data.
  - Stored keys that are used by the various protection mechanisms. In the example product these are:
    - Bluetooth bonding parameters, including encryption keys
    - Keys to encrypt the application image
    - Keys used to sign and check the signature of the application image
    - Keys to encrypt storage of private data

4.3 Protection Mechanisms

Each interface and each asset that is accessible through the interfaces may need to be protected from manipulation or information leakage. The product must provide mechanisms for implementing security-related system functionality.

4.3.1 Mechanisms to Control Access to Assets and Interfaces

Access to the assets and the interfaces must be controlled, to ensure that an attacker cannot modify or read them if that impacts the security of the system. The physical or logical mechanisms to control access must be documented. In the example product:

- The wireless interface of the BTC can only be accessed through the Bluetooth Stack. The Bluetooth stack is only accessible through function calls from the product's firmware and debug interfaces before production.
- The user interface on the BTC (display) connects to an output port of the Renesas Electronics Connectivity device. It is accessible through function calls from the product's firmware. The user can access it physically when using the product, by looking at the screen.
- The button interface is not accessible by unauthorized users. Access is physically controlled because the button is located within the battery compartment. This means that someone must physically get hold of the BTC to unscrew the cover of the battery compartment and access the button. **It is good practice to mechanically protect user interfaces that can be used for configuring the device by authorized users, especially if the product is intended to be normally used by non-authorized users.**
  The user application interface is accessible from all users. Access to individual functions is controlled by the

configuration of the user application. Security and privacy related functions are only available to the authorized user.

- The Renesas Electronics Connectivity devices have two debug interfaces (JTAG, UART). Access to these interfaces would compromise the security of the product, therefore it is controlled by two mechanisms:
  - Physical restriction: these interfaces are not exposed (they are not on the product surface).
  - Logical disabling: these interfaces are blocked by OTP flags in the production line.
- User data is stored on flash memory, inside the BTC and cannot be externally read or modified. It can only be accessed by the application firmware through function calls. As an extra mechanism of protection, such data is also stored in an encrypted format. See Section 4.3.4.
- The application firmware is stored in the flash and execution by the on-chip MCU on the fly. There are two mechanisms to control access to it. Physically, someone would have to open the product to get access to the flash and the firmware. But even if one did, the firmware is stored with a signature that confirms its integrity. DA1469x and DA1459x utilize a ROM-based secure bootloader. This bootloader checks the firmware image signature and only uses it if the signature is valid. **It is strongly recommended to use the secure bootloader features.**
  - The firmware image can also be accessed outside the device during software update. Besides the mechanisms provided by the Bluetooth stack, having the firmware image signed prevents someone from altering it during transfer.
  - As an extra method of protection, the application firmware is stored in an encrypted format (DA1469x family only).
- The user application on the smartphone or tablet is accessible to all users. As explained before, only authorized user access needs to be controlled. This can be achieved with two mechanisms that may coexist:
  - Using a password to get access to the privileged functions of the application. This guide focuses on the product itself (the BTC), so it does not elaborate more on this mechanism. It is up to the user application designer to provide an implementation of this mechanism.
  - Enabling the privileged functions only if the specific peer device (and its user) is paired (in Bluetooth terms) with the BTC. See Section 4.3.5.
  - **It is recommended that any application which provides functionality that influences product security, is designed, developed and tested so that it controls access and allows only authorized users to perform such functionality.**
- Access to the stored keys must be restricted only to the functions of the application firmware that use them. As an extra mechanism to ensure the keys cannot be altered or retrieved, the keys are stored in a protected area within the device. See Section 4.3.4.

Table 1 shows a summary of access control mechanisms.

Table 1. Access control overview

Asset or Interface	Type of access control mechanism
Wireless Interface	Logical - from the stack functions
Bluetooth Stack	Physical - resides in encrypted flash Logical - from application firmware
Display User Interface	Logical - from application firmware
Auxiliary device interface	Logical - from the stack functions
Button interface	Physical - in the battery compartment. Logical - from application firmware
Debug interfaces (JTAG, UART)	Physical - not exposed on the product Logical - disabled at production
Stored User Data	Physical - not exposed on the product Logical - from application firmware Secured - stored in encrypted format
Application Firmware	Physical - not exposed on the product Secured - encrypted during transfer and storage

Asset or Interface	Type of access control mechanism
	Secured - signed during transfer and storage
Functions of the user application	Logical - password based privileged access Secured - only over paired Bluetooth connection
Stored Keys	Physical - not exposed on the product Logical - from application firmware Secured - stored in protected area

4.3.2 Mechanisms to Support and Enforce Authentication of Users and/or Peer Devices

In some cases, you need to have access to assets and interfaces. To ensure that this access does not pose a security threat, a mechanism to authenticate the user is required and must be documented.

In connected devices, users also interact through a peer device like a smartphone or tablet. Connecting to such peer devices - when used to access security or privacy related assets and interfaces - needs an authentication mechanism that must be documented.

There two types of users in the example product:

- Authorized (adult) users: they need to have access to the BTC's security and privacy assets.
- Children: they only use the BTC while riding the bicycle. Their access is limited to non-private and non-secure assets and interfaces.

Both users interact over the Wireless interface through functions of the user application. The application uses the mechanisms of the Bluetooth stack to get read and/or modify access to individual characteristics in BTC.

When the accessed characteristics are related to privacy or security, the Bluetooth Stack is configured by the Application Firmware to block access if the peer device is not paired.

The Bluetooth pairing mechanism ensures that only authorized users can connect.

Renesas Electronics Connectivity devices support Bluetooth pairing and more specifically the "Secure Connections" standards feature which provides enhanced protection from security threats. In our example product, we use Secure Connections with the "Numeric Comparison" pairing mechanism. As described in Ref. [5], to support this method, the device should be equipped with a "display" that presents a 6-digit number on the display for the user. The same number should match the digits shown on the smartphone application, and the user must confirm the match to complete pairing.

This procedure is quite tedious to repeat every time a user wants to access the device. This is why used another standard Bluetooth mechanism: Bonding. Bonding allows to store the connection parameters after pairing, so that the two devices (BTC and Authorized user's phone) are reconnected securely every time.

It is recommended to use Bluetooth Secure Connections for Pairing and Bonding.

If the device has some means of providing the 6-digit number to the user, it is recommended to use the Numeric Comparison pairing method.

4.3.3 Mechanisms to Securely Update Product's Software

The application firmware that runs within the device must be updatable. Through software updates, the manufacturer can deploy new versions of the application firmware, in the case that some security vulnerability is found and fixed. But making the device software updatable is also a risk, because an attacker might exploit this to load malicious code. Therefore, it is critical that any software update mechanism is secure and does not allow running other firmware besides the one intentionally pushed by the device manufacturer.

The mentioned Renesas Connectivity devices can support secure updates by using the secure bootloader. This bootloader is available in ROM. **It is strongly recommended to use the secure bootloader features.**

The secure bootloader ensures that only images that are signed can be loaded on the device. Image signature is performed using advanced asymmetric encryption, with the public key stored in the device OTP and the private key maintained at the manufacturer. The private key is a secret and measures at the manufacturer's premises must be taken to prevent it from leaking. In case of leaking, there is a key revocation feature in the secure bootloader. However, there is always a time window where devices on the field might be exposed (from the

moment the private key leaks, to the moment a key revocation update is deployed). It is therefore strongly recommended that the private key remains secret, and any leakage is detected as soon as possible.

4.3.4 Mechanisms to Securely Store and Delete Security-related and Private Information

Some information that is stored on the device must be protected from readout and from manipulation. This includes at least:

- Security-related information (connection keys)
- Sensitive personal information of the end user.

When the device is initialized and used on the field, such information cannot be modified or read, unless by the authorized user. Other entities or unauthorized users should not have any access.

When the device is returned to the manufacturer, handed over to a different end-user or disposed, this information should be deleted, to protect them from more elaborate (physical) attacks.

It is strongly recommended to employ secure storage and deletion for all network and privacy assets of the product.

The latest SDKs of DA1469x and DA1459x come with functions that support encrypted storage. Using this set of functions, the application can also delete the security-related and the private information when needed. The keys used by this mechanism are created at runtime by the application image and are unique per device. **It is strongly recommended to use unique per device keys for encrypted storage, to prevent scalable attacks.**

In the BTC example, the application firmware utilizes these secure storage and deletion mechanisms for network keys (bonding parameters) and for any user data.

4.3.5 Mechanisms of Secure Communication

The communication channels may carry information that is critical for device security or the user privacy. When such information is transferred, the protocol must provide mechanisms for encryption. The Bluetooth Low Energy protocol provides a variety of security mechanisms, depending on the user interface capabilities of the devices that communicate.

When possible, it is strongly recommended to use the Bluetooth Secure Connections mechanism with Numeric Comparison. This mechanism provides very strong keys for encrypting the channel and are immune to a variety of attacks including MITM.

4.3.6 Key Management and Cryptography

Many of the protection mechanisms explained here utilize cryptography functions. When a cryptography function is used — it must use best practice implementations that correspond to the protection needed for each of the supported assets and interfaces. Where these functions use keys, these keys must be generated, managed and securely stored.

In DA1469x, DA1459x and corresponding SDKs, Renesas Electronics provides cryptography functions and key generation tools. Specifically:

- To generate the asymmetric keys for firmware image signing
- To generate the symmetric key for image encryption
- To generate keys for Bluetooth communication
- To derive a unique per device key for secure storage

It is strongly recommended to use the methods provided (or equivalent ones) for key generation and management.

4.3.7 Generic Provisions

There are some generic provisions that the end-product must support. Most of these are described in previous sections, but we provide here a table that organizes them as per the 18031-x section 5.10.

Provision	Recommendation
Up-to-date software, without known vulnerabilities	Before product launch, check public vulnerability databases of any software library used in the SDK or used in additional application

Provision	Recommendation
	code. Also check specifically for any mention of the relevant Renesas Electronics device. Periodically check, and - if something is found - roll out a software update on the field with the appropriate mitigation.
Limit Exposure of services	In the BTC example, the only services that are exposed at the factory default state are the Bluetooth LE services needed to connect and configure the device so that the authorized user can configure the product.
Configure Optional Services	
Document exposed interfaces	The user documentation (manual) of the example BTC product must describe that the product must be configured by the authorized user and must provide step by step easy to follow instructions of how to configure it, how to access personal data and how to perform software updates through the companion smartphone application.
No unnecessary interfaces	The example product exposes the minimal set of interfaces needed for operation. Any other interfaces are internally disabled and not exposed on the device enclosure.
Document sensing capabilities	The user documentation (manual) of the example product must describe that the product built in sensors and that it interfaces to auxiliary devices and that any recorded data is stored in a way that only the authorized user can access it
Input Validation	Input validation through the Bluetooth interface is provided by the implementation of the protocol in DA1469x and DA1459x.

4.3.8 Application-specific Mechanisms 18031-2

The mechanisms described here are application specific. DA1469x and SDK 10.0.16 APIs (or same APIs on the DA1459x SDK) can be utilized to implement such mechanisms but there is no generic implementation.

Logging

The equipment shall provide a mechanism to log internal activities that are relevant for the protection of events, unless the logging of Events is done by other means outside the equipment. In the example BTC product, the events that can be logged are:

- Software updates and whether they are successful or not.
- Pairing attempts and whether they are successful or not.

This information can be logged in the flash. If the product has flash size restrictions, the designer may consider logging by the smartphone application, but a risk analysis should be performed against the specific use case.

User Notification

The device should notify the user when a change that affects security or privacy occurs. In the example BTC product, such notifications are delivered over the user interface of the smartphone application and relate to:

- Software Updated
- Pairing and Bonding
- Secure Data Deletion ("Factory Reset")

It is strongly recommended that the application firmware implements the logging of security events and generates appropriate user notifications.

4.3.9 Application-specific Mechanisms 18031-1

The mechanisms described here are application specific. DA1469x and SDK 10.0.16 APIs (or same APIs of DA1459x) can be utilized to implement such mechanisms but there is no generic implementation.

Resilience

The Bluetooth LE protocol includes mechanisms that are inherently resilient to DOS attacks. However, as with all wireless protocols, there is always the chance that an attacker fully blocks the available RF spectrum. The application designer must assess if such an attack would compromise the security of the product and if yes,

develop countermeasures. In the example BTC project such an attack would not allow any security or privacy compromise, although it could impact user experience.

Network Monitoring

If the device is used to connect other devices to the network, it must implement network monitoring mechanisms, including at least monitoring for DOS attacks. In the example of the BTC product, this is not needed.

Traffic Control

If the device is used to connect other devices to the network, it must implement traffic control mechanisms. In the example of the BTC product, this is not needed.

Depending on the actual product, the manufacturer must consider implementing (in the application firmware) network monitoring and traffic control mechanisms.

4.4 Risks

Even with all the implemented security mechanisms, a product may not be 100% secure. For example, if an attacker gets physical access to the product or finds out the value of shared secrets, you are able to prepare elaborate attacks that compromise the system. An analysis of these risks must be carried out and documented. A simple table should be created.

At the time of preparing this guide, there are two vulnerabilities reported for DA14695 on the public vulnerability databases (CVE-2024-25077, CVE-2024-25076). Both these vulnerabilities would allow an attacker with physical access to the product's flash memory to compromise secure boot. It is therefore strongly recommended to prevent access to the flash device by enclosure, encapsulation or coating.

NOTE
Any published vulnerabilities at the time of product launch must be added to a Risk Table and the risk must be adequately assessed and accepted or mitigated.

In the example BTC product, the risk table entry corresponding to CVE-2024-25077/25076 could as in Table 2.

Table 2. Cybersecurity risks example

Risk ID	Affected Asset or Interface	Severity of the attack	Method of the attack	Risk assessment
R01	Image loaded by Secure Booter as explained in CVE-2024-25077 and CVE-2024-25076	Medium	Cannot be performed. On the DUT, any physical access to the flash memory is blocked by encapsulation in the module as recommended in Renesas Electronics' advisory for CVE-2024-25077/25076.	Low

4.5 Mapping to EN 18031-x Provisions

The following table provides a proposed mapping of the above sections with the provisions of the EN 18031-1 and 18031-2 standards.

Table 3. Mapping to EN 18031-x provisions

Section	18031-1	18031-2	Comment
Section 4.3.1	5.1 [ACM]	5.1 [ACM]	18031-2 has more [ACM] provisions than 18031-1, specifically targeting Toys and Childcare devices.
Section 4.3.2	5.2 [AUM]	5.2 [AUM]	Similar provisions on both standards
Section 4.3.3	5.3 [SUM]	5.3 [SUM]	Similar provisions on both standards
Section 4.3.4	5.4 [SSM]	5.4 [SSM] 5.7 [DLM]	Similar provisions on both standards. 18031-2 also needs a deletion mechanism.
Section 4.3.5	5.5 [SCM]	5.5 [SCM]	Similar provisions on both standards
Section 4.3.6	5.9 [CCK] 5.11 [CRY]	5.9 [CCK] 5.11 [CRY]	Similar provisions on both standards
Section 4.3.7	5.10 [GEC]	5.10 [GEC]	Similar provisions on both standards
Section 4.3.8	-	5.6 [LGM] 5.8 [UNM]	Applies only to 18031-2
Section 4.3.9	5.6 [RLM] 5.7 [NNM] 5.8 [TCM]	-	Applies only to 18031-1

Note 1 This guide does not reference EN 18031-3. Although the provisions are very similar to those of 18031-1 and 18031-2, it does not target the use cases of EN 18031-3 with DA1469x or DA1459x.

5. Documenting Conformity

Conformity assessment and declaration are the responsibility of the end-product manufacturer. Renesas Electronics recommends working with a specialized expert. Working with a notified body and a competent test house is also beneficial, especially if the provisions of the EN 18031-1 and 18031-2 standards are not fully met, or if one of the restrictions mentioned in the implementing act applies to the product.

Below is a simple list of work products that should be prepared and maintained by the manufacturer. The list is non-exhaustive, and Renesas Electronics cannot provide any guarantee that something else is not required.

Conformity Dossier:

- Documentation of Conformity
  - A list of all assets, interfaces and protection mechanisms.
  - Description of how each provision of the 18031-x standards is fulfilled by the corresponding mechanisms.
  - Path through all applicable decision flows in the 18031-x standards
  - List of risks and vulnerabilities (if any, see Section 4.4).
- Test Report
  - Either from test house if externally performed or from internal testing
  - Include at least pass/fail and test description
  - Including test evidence records is optional but recommended
- Device information
  - Model, Commercial Name, Origin
  - Hardware Design, Bill of Materials
  - Software Version used for the testing
  - Photos of the product showing all interfaces
- Physical storage of the hardware and the software used for the tests
- Test instructions so that the tests can be repeated if needed

6. Conclusions

This guide used an example fictional product (a Bicycle Trip Computer) to provide suggestions on how a product can address cybersecurity requirements coming from RED articles 3.3 d. The target audience is the security development team of manufacturers of such products.

Be aware that Renesas Electronics provides no guarantee that following this guide results in conformity with these standards or any other security specification. It is the responsibility of the product manufacturer to ensure the product conforms.

Appendix A Recommendations and Best Practices

In this appendix, we list all recommendations and best practices mentioned above and (if applicable) we point to corresponding locations in the referenced user documentation.

Recommendation/Best practice	Pointers to documentation (where applicable)
It is good practice to treat all data that is stored on the device as private.	
It is good practice to mechanically protect user interfaces that can be used for configuring the device by authorized users, especially if the product is intended to be normally used by non-authorized users.	
It is strongly recommended that applications on peer devices implement different user privileges for generic users and authorized users (especially in Toys and Childcare devices), that can be accessed only by using strong passwords.	
It is strongly recommended that both JTAG interface are always disabled by setting the corresponding OTP flags of Renesas Electronics device at the end of the production cycle and before the product exists the factory floor.	See Ref. [2] Section 5.12.3 (Secure Access)
It is strongly recommended to disable UART-boot at the end of the production cycle and before the product exits the factory floor.	See Ref. [1] Section 6.5.2 (Configuration Script), Table 70, Entry #5. See Ref. [2] Section 5.6 (Configuration Script), Table 66, Entry #5.
It is recommended that any application which provides functionality that influences product security is designed, developed and tested so that it controls access and allows only authorized users to perform such functionality.	
It is strongly recommended to use Bluetooth Secure Connections for Pairing and Bonding.	See Ref. [5] Section 5.1.10.1 (LE Secure) See Ref. [6] Section 5.1.9.1 (LE Secure)
If the device has some means of providing the 6-digit number to the user, it is recommended to use the Numeric Comparison pairing method.	See Ref. [5] Section 5.1.10.1 (LE Secure) See Ref. [6] Section 5.1.9.1 (LE Secure)
It is strongly recommended to use the secure bootloader features.	See Ref. [1] Section 6.11.2 (Secure Boot) See Ref. [2] Section 5.12.2 (Secure Boot)
If the secure bootloader cannot be used for any reason, it is strongly recommended that the security risks are analyzed and other mechanisms to protect the user and the network are employed.	
It is strongly recommended that the private key remains secret, and any leakage is detected as soon as possible.	
It is strongly recommended to employ secure storage and deletion for all network and privacy assets of the product.	See Ref. [5] Section 5.1.2 (User Data Secure Store) See Ref. [6] Section 5.1.1.1 (User Data Secure Store)
It is strongly recommended to use unique per device keys for encrypted storage, to prevent scalable attacks.	See Ref. [5] Section 5.1.2 (User Data Secure Store) See Ref. [6] Section 5.1.1.1 (User Data Secure Store)
it is strongly recommended to use the Bluetooth Secure Connections mechanism with Numeric Comparison	See Ref. [5] Section 5.1.10.1 (LE Secure) See Ref. [6] Section 5.1.9.1 (LE Secure)
It is strongly recommended to use the methods provided by DA1469x, DA1459x and corresponding SDKs for key generation and management: ▪ To generate the asymmetric keys for firmware image signing ▪ To generate the symmetric key for image encryption ▪ To generate keys for Bluetooth communication ▪ To derive a unique per device key for secure storage	See Ref. [7] and Ref. [8] DA1459x/69x Secure Boot Mechanism
Any published vulnerabilities at the time of product launch must be added in the Risk Table and the risk must be adequately assessed and accepted or mitigated.	See Ref. [9]
On DA1469x, it is strongly recommended to prevent access to the flash device by enclosure, encapsulation or coating. This does not apply on DA1459x because the flash is embedded in the device.	
It is strongly recommended that the application firmware implements the logging of security events and generates appropriate user notifications.	

Recommendation/Best practice	Pointers to documentation (where applicable)
Depending on the actual product, the manufacturer must consider implementing network monitoring and traffic control mechanisms in the application firmware network monitoring and traffic control mechanisms.	

7. Revision History

Revision	Date	Description
1.00	Aug 28, 2025	Initial Release

STATUS DEFINITIONS

Status	Definition
DRAFT	The content of this document is under review and subject to formal approval, which may result in modifications or additions.
APPROVED or unmarked	The content of this document has been approved for publication.

ROHS COMPLIANCE

Renesas Electronics' suppliers certify that its products are in compliance with the requirements of Directive 2011/65/EU of the European Parliament on the restriction of the use of certain hazardous substances in electrical and electronic equipment. RoHS certificates from our suppliers are available on request.

IMPORTANT NOTICE AND DISCLAIMER

RENESAS ELECTRONICS CORPORATION AND ITS SUBSIDIARIES (“RENESAS”) PROVIDES TECHNICAL SPECIFICATIONS AND RELIABILITY DATA (INCLUDING DATASHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT OF THIRD-PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for developers who are designing with Renesas products. You are solely responsible for (1) selecting the appropriate products for your application, (2) designing, validating, and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, or other requirements. These resources are subject to change without notice. Renesas grants you permission to use these resources only to develop an application that uses Renesas products. Other reproduction or use of these resources is strictly prohibited. No license is granted to any other Renesas intellectual property or to any third-party intellectual property. Renesas disclaims responsibility for, and you will fully indemnify Renesas and its representatives against, any claims, damages, costs, losses, or liabilities arising from your use of these resources. Renesas' products are provided only subject to Renesas' Terms and Conditions of Sale or other applicable terms agreed to in writing. No use of any Renesas resources expands or otherwise alters any applicable warranties or warranty disclaimers for these products.

(Disclaimer Rev.1.1 Jan 2024)

Corporate Headquarters

TOYOSU FORESIA, 3-2-24 Toyosu
Koto-ku, Tokyo 135-0061, Japan

www.renesas.com

Trademarks

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-us/