AN12928

Bluetooth® Low Energy Privacy and NXP QN9090

A brief review on privacy and recommended practices

Rev. 0 — September, 2020

Application Note

Contents

1 Introduction

How can someone prevent his/her smartwatch from being tracked by untrusted scanners? The ability to do so depends on the device; if it can prevent its address from being decoded by another unauthorized device, and if it can provide privacy to its user.

This Application Note discusses the means that allow Bluetooth LE devices to preserve the identity of their users and how this relates to NXP QN9090 features, limitations, and applications.

It is assumed that the reader has prior knowledge of Bluetooth LE specifications, its architecture, link layer states, and security procedures, such as pairing and bonding.

1.1 Device addresses

Each Bluetooth LE device is identified by its address. A unique 48-bit Bluetooth Device Address (called BD_ADDR) is allocated for each device. A Bluetooth LE address is equivalent to MAC address in Ethernet protocol, but the former can be modified more easily.

When advertising, a Bluetooth LE device transmits its address as part of the advertisement packet. A scanner identifies the source of the message, and may initiate a connection.

As the advertisement propagates, other untrusted devices may scan the packets and passively obtain information from it. For example, the device address, proximity, offered services, frequency of transactions, and so on.

Consider a smartwatch that advertises its unique address (public address) for connection. The following packet format in Figure 1 is defined for the Bluetooth LE Uncoded PHYs (Bluetooth LE 1M and Bluetooth LE 2M) and is used for both advertising channel packets and data channel packets.

The advertising channel PDU has a 16-bit header and a variable size payload. Among other information, the header indicates whether the advertised address AdvA is random or public, and the AdvData informs the offered services. For more information, see Core Specifications 5.0, Volume 6, Part B, sections 2.1, 2.3 and 2.3.1.1.

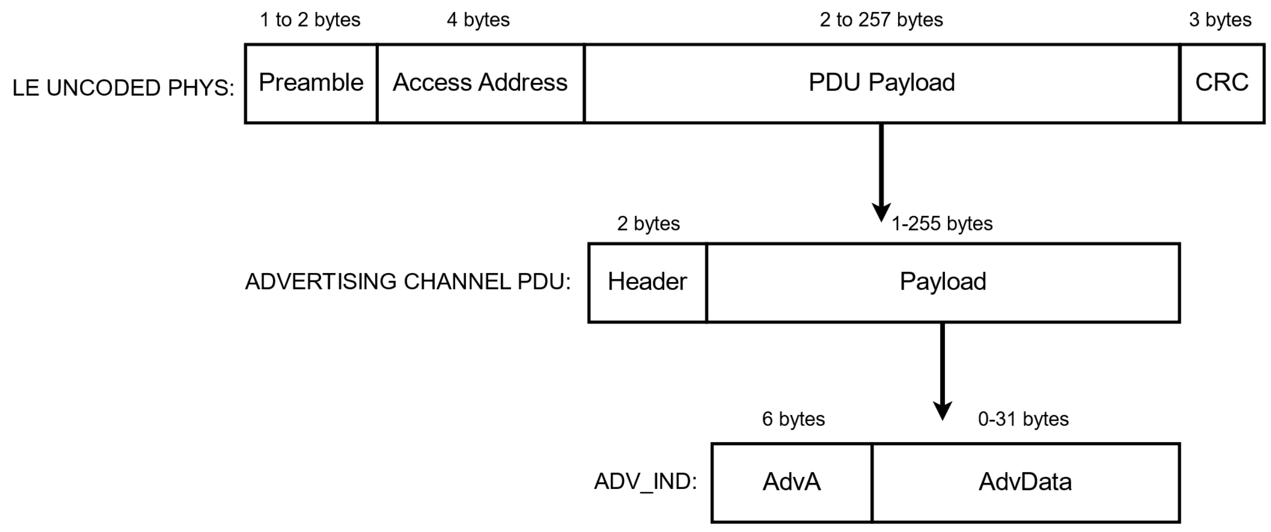

Figure 1. Bluetooth LE packet

Bluetooth LE enables privacy by changing the device's address frequently. Bluetooth LE devices have 4 types of addresses available for use. This choice of addresses allows compliance with different use cases and requirements. See Bluetooth Core Specification 5.0 Vol 1, Part A, section 5.4.5 for more information.

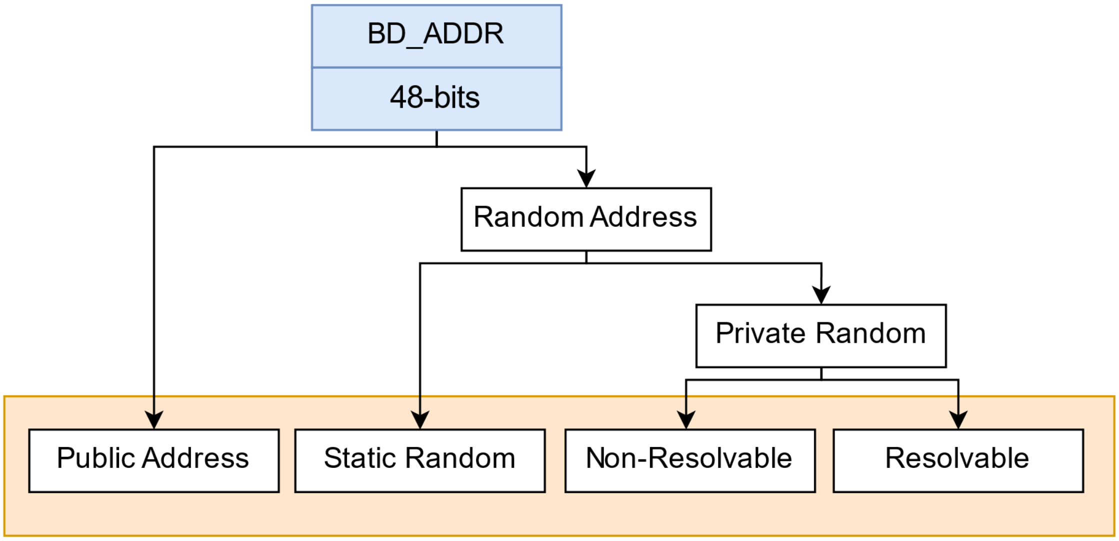

Figure 2. Bluetooth LE address types

The public address consists of two 24-bit long values, defined by the company ID and a company assigned ID. The public address is not changeable.

As the name suggests, the random address is randomly generated and it can be either a static random address or private random address.

Static random addresses do not change in one power cycle, whereas private random addresses may be changed at each connection. The two most significant bits of static random addresses are equal to 1.

Resolvable Private Address (RPA) is a random address, generated and resolved by the use of a key, called the Identity Resolving Key (IRK). Devices share this key during pairing procedure and store it when bonding. In addition to the IRK, the devices also share their identity address which is a random static or public address. The final information of the peer device is called device identity. The device identity consists of the peer's identity address and a local and peer's IRK pair. RPA is the foundation for privacy in Bluetooth LE.

The scanner resolves the incoming advertising address using the IRKs available in its memory. In case the resolution is successful with one of the stored IRKs, the identity address of the advertiser is known to the scanner. If a device uses RPAs and changes its identity frequently, non-peer scanners are unable to track it based on its address. Peer devices, on the contrary, may identify it using the Address Resolution procedure. The two most significant bits of RPA are 1 and 0.

Non-Resolvable Private Address (NRPA) is a random address that cannot be decoded and does not relate to an IRK known to the peer device. For NRPAs, the two most significant bits of the address are equal to 0.

1.2 Address resolution procedure

Consider the initial use case. A smartwatch is an advertiser and a cell phone is a scanner, both use RPAs in the first connection. Using Bluetooth LE Secure Connections, they encrypt the link and exchange security data, including their identity address (static random or public address) and IRK. See Core Specifications 5.0, Vol. 3, Part H, section 3.6.1 for more information.

Before advertising, the smartwatch generates a random number, called *prand*, and uses it with its own IRK, as input to the hash function. The output is a hash value. The hash value and the *prand* are juxtaposed and added to the advertising packet as the address of the smartwatch. The two most significant bits of *prand* are equal to 1 and 0. See Core Specifications 5.0, Vol 6, Part B, section 1 for more information.

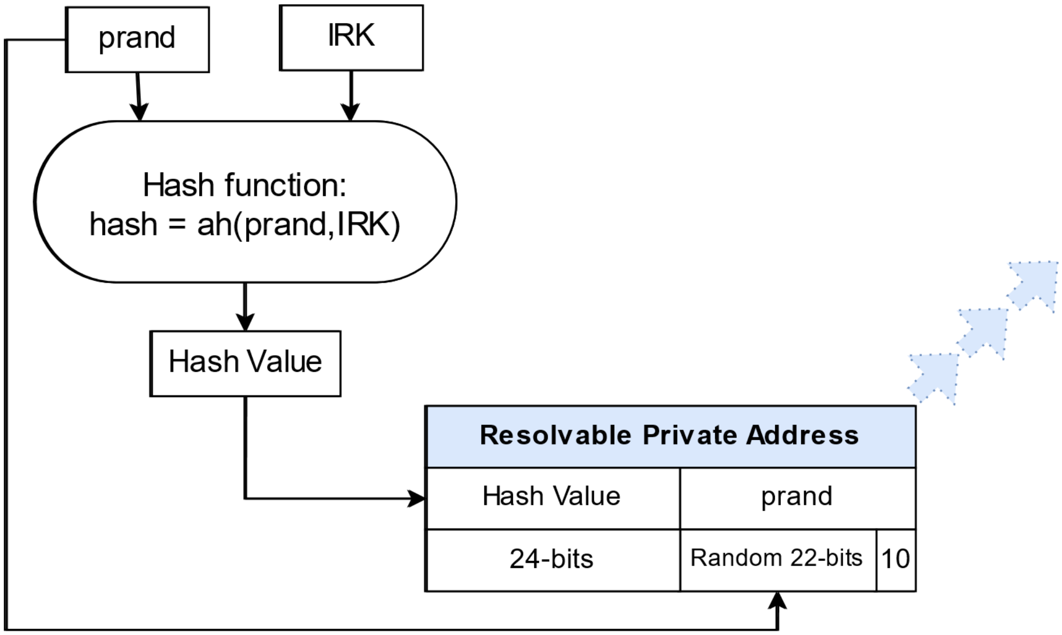

Figure 3. RPA generation diagram

The cell phone receives the advertising packet from the smartwatch and resolves the RPA. It uses the received 22-bit *prand* and stored IRKs to generate local hash values. It has the IRK of its peer smartwatch stored, as well as the Identity Address. Therefore, one of the generated local hash values matches with the received hash value, and the advertiser is identified. It is important to highlight that this operation is both time and power consuming, therefore, resolving lists are limited in size.

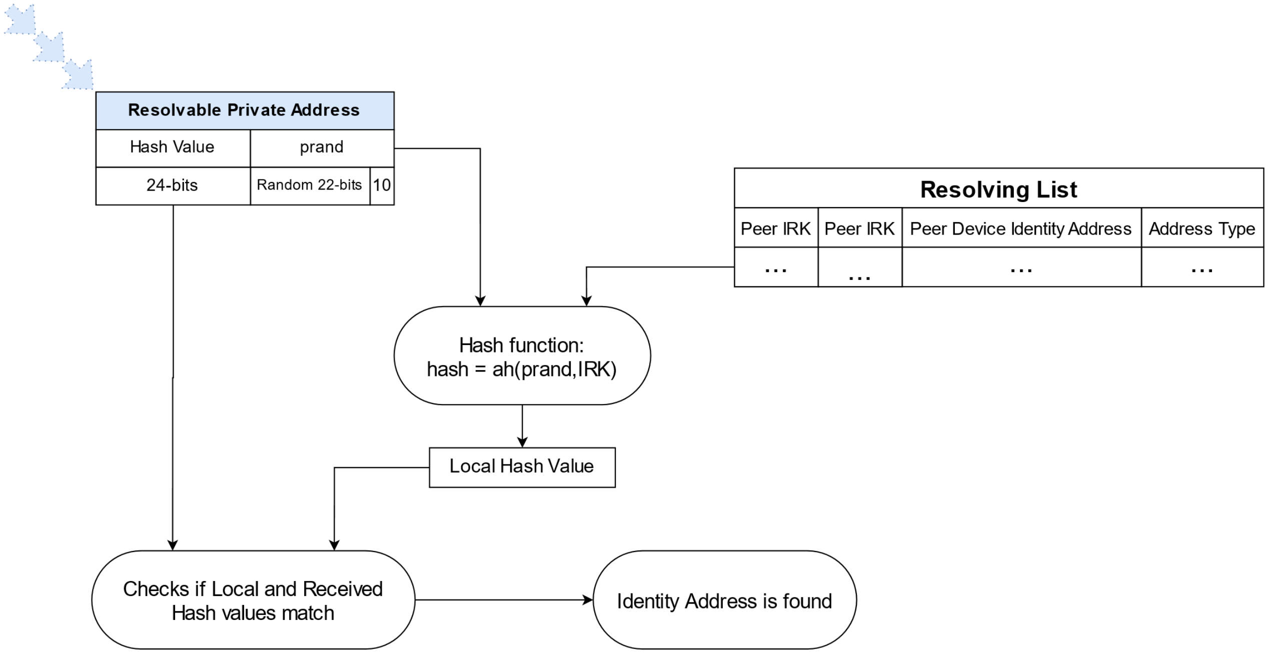

Figure 4. RPA resolution diagram

By the Identity Resolution procedure, two peer devices identify each other and communicate using RPAs. The RPA can be resolved and reveals the true identity of the transmitter, while for other scanners around, the RPA is just another random address.

2 Bluetooth LE host and controller privacy

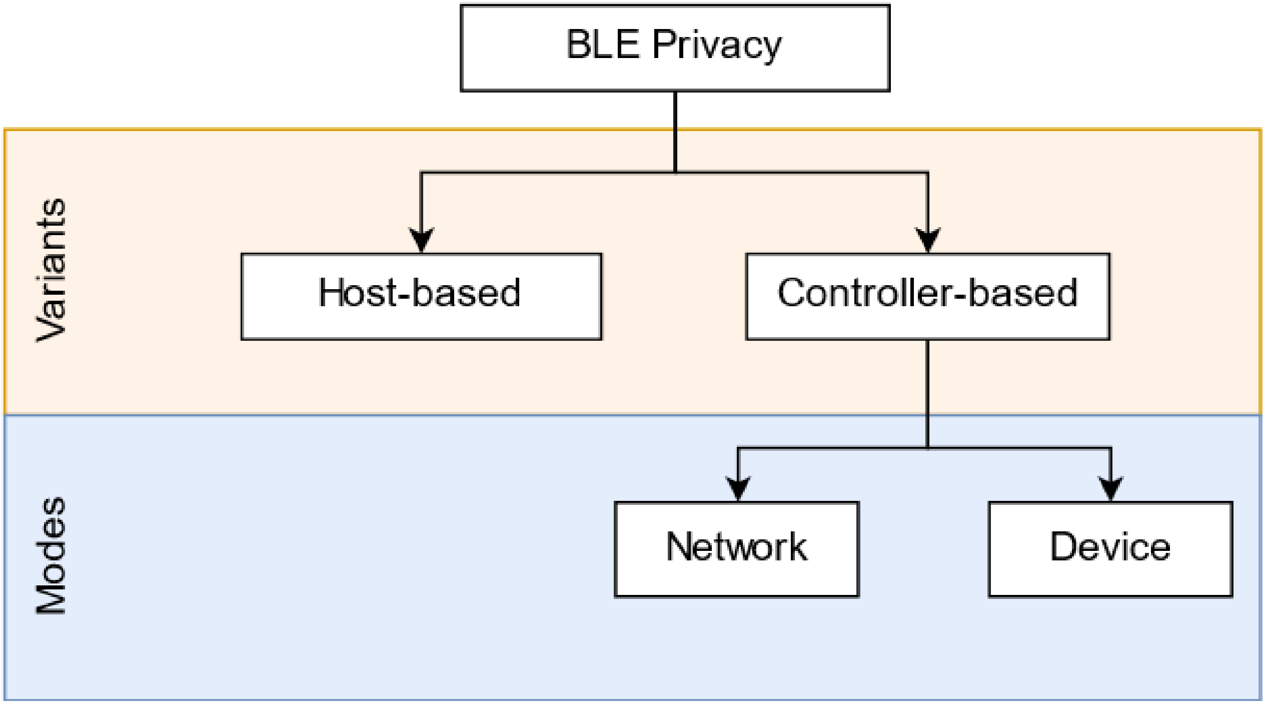

Figure 5. Bluetooth privacy configurations

2.1 Variants

There are two variants of the privacy feature: Host and Controller-based.

Host-based: In this first variant, private addresses are resolved and generated by the Host. Peer device identities are accessed by the Host during resolution.

Controller-based: In this second variant, private addresses are resolved and generated by the Controller after the Host provides its own identity as well as those of peer devices to the Controller. The Host is still responsible for maintaining a resolving list by adding and removing device identities whenever needed. In addition, when using the second variant, the Host may provide an extended resolving list, in case the Controller cannot store all the device identity resolving keys necessary for bonded devices.

If the Controller cannot resolve the peer's device identity address in an advertisement, it passes the event to the Host for resolution. In case the peer's device address has been resolved by the Controller, all incoming events from the Controller to the Host use the peer's device identity.

NOTE

As described in Bluetooth Core Specifications (5.0 Vol.6, Part B, section 4.3) the Link Layer may perform device filtering based on the address of peer devices. This procedure allows the Link Layer to minimize the number of devices to which it responds. The set of devices that the Link Layer uses for device filtering is called the White List. Device filtering is directly related to the privacy variant in use as well. When using Controller-based privacy, an incoming RPA is resolved by the Scanner's Controller, and the device identity is verified in the White List, also located in the Controller. In case the received identity is found in the White List, it is passed to the Host for further connection processing. Otherwise it is simply ignored, even if it is a peer device.

Device filtering becomes possible when address resolution is performed in the Controller because the peer's device identity address can be resolved prior to checking whether it is in the White List.

2.2 Modes

There are two modes of privacy: device privacy and network privacy. These modes determine how a privacy-enabled device handles connection creation with its peer devices.

A device in device privacy mode is only concerned about its own privacy and accepts advertising packets from peer devices that contain their identity address as well as ones that contain a random private address, even if the peer device has distributed its IRK in the past.

In network privacy mode, it is mandatory that all devices use random addresses. In this mode, a device only accepts advertising packets from peer devices that contain private addresses. Network privacy is the default behavior for Controller-based privacy.

For example, assume a smartwatch and a phone are bonded devices.

In the phone's resolving list, the smartwatch identity information is set as *device privacy mode*. When the smartwatch advertises with its own Identity Address in the advertisement payload (Static Random or Public Address, instead of an RPA), the phone accepts the advertisement packet and establishes the connection link. The phone is not concerned about the fact that the smartwatch is revealing its own identity.

In the second situation, in the phone's resolving list, the smartwatch Identity Info is set as *network privacy mode*. When the smartwatch advertises with its own Identity Address in the advertisement payload (Static Random or Public Address, instead of an RPA), the phone does not accept the advertisement packet and the connection link is not possible. The phone, in this case, is indeed concerned about the fact that the smartwatch is revealing its own identity.

3 NXP QN9090

3.1 Available variants and mode

The QN9090 MCU supports both Host and Controller-based privacy variants. Only Network Mode is available for Controller-based privacy. The difference between supporting a feature and being Bluetooth SIG qualified to use that same feature must be noted. QN9090 supports Controller-based privacy, Network Mode only, but it is not qualified for use as a Bluetooth LE 5 subsystem. The reason for this is that Bluetooth SIG now requires Device Privacy Mode support for Bluetooth LE 5 products to use Controller-based Privacy. For Bluetooth LE 4.2, Bluetooth SIG does not require Device Privacy Mode support. In this case, devices may support Controller-based privacy in Network Mode only, and qualify for using it. See Privacy and Bluetooth project qualification for more information on how variants and modes available in QN9090 relate to Bluetooth SIG qualification process. Device Privacy Mode is not supported.

A scanner that enables Controller-based privacy ignores advertising packets from a peer device if the latter advertises using its Identity Address. Only RPAs are accepted from peer devices while Controller-based privacy is enabled in Network Mode.

In the same way, an advertiser that enables Controller-based privacy in Network Mode ignores connection requests from a peer device that is using its identity address. Only RPAs are accepted from peer devices while Controller-based privacy is enabled in Network Mode.

NOTE

All privacy-enabled SDK projects implement Host-based privacy.

3.2 Host and controller privacy

As described in the Bluetooth® Low Energy Application Developer's Guide, the capabilities of each privacy variant are summarized as follows.

3.2.1 Host-based Privacy

Random address generation - Periodically regenerating a random address (resolvable or on-resolvable private address) inside the Host and the applying it into the Controller.

Random address resolution - Try to resolve incoming RPAs using the IRKs stored in the bonded devices list. The address resolution is performed when a connection is established with a device or for the autoconnect scan. The advertising packets that have an RPA are not resolved automatically due to the high MCU processing required. Each of the use cases is detailed in the following sections. The random address resolution is performed by default by the Host whenever the Controller is unable to resolve an RPA. The random address generation is performed by the Host only when Host Privacy is requested to be enabled.

3.2.2 Controller-based Privacy

Controller Privacy, introduced by Bluetooth LE 4.2, consists of writing the local IRK in the Controller, together with all known peer IRKs, and letting the Controller perform hardware, fully automatic RPA generation and resolution.

The Controller uses a resolving list to store these entries and the size of the list is platform-dependent, given by gMaxResolvingListSize_c. In QN9090, the maximum number of devices in the resolving list is 6 and in the white list is 16. For RPA resolution, the entries that do not fit in this list are processed by the Host to be resolved using the IRKs from the bonded devices list.

The recommended way of using privacy is the Controller Privacy. However, enabling Controller Privacy requires at least a pair of local IRK and peer IRK. This can only be enabled after a pairing is performed with a peer and the IRKs are exchanged during the key distribution phase. When a device starts and privacy is required, the workflow is as follows:

1. Enable Host Privacy using the local IRK.
2. Connect to a peer and perform pairing and bonding to exchange IRKs.
3. Disable Host Privacy.
4. Enable Controller Privacy using the local IRK and the peer IRK and peer identity address.

3.3 Privacy and Bluetooth project qualification

Bluetooth SIG Qualification Program Reference Document refers to the qualification procedure of a specific design of Bluetooth wireless technology by an individual member. To be qualified by Bluetooth SIG, a product needs to go through the qualification and declaration processes. Two Bluetooth SIG reference documents for qualifying and declaring conformity are the Test Case Reference List (TCRL) and the Implementation Conformance Statement (ICS).

The TCRL is the list of all available Bluetooth Test Cases and is the basis for generation of the test plan. TCRL categorizes test cases, as well as introduces new ones and removes others, and is periodically updated. The ICS is a document completed by the member specifying all the implemented Bluetooth capabilities in detail, which consequently relates to the TCRL as well.

There are two ways to qualify a new Bluetooth LE compliant product. The architecture of the system determines the qualification procedure. It will fit into one of the cases below:

1. The product is a single or a combination of qualified Bluetooth Subsystem Products and/or qualified Bluetooth End Products. For such projects, provided no design changes were made during the combination, no testing is required during qualification process. They inherit the reports of their qualified subsystems.
2. The product is a single or a combination of systems that involve qualified subsystems and tested or untested components or that include changes or additions to Bluetooth LE capabilities. For such projects, testing is required during qualification process, since any ICS change shall be treated like a new design. See Bluetooth SIG PRD for more information.

The QN9090 is a Bluetooth LE 5 qualified subsystem. It does not support Device Mode privacy, therefore, QN9090 is not qualified for using Controller-based privacy as a Bluetooth LE 5 device. It is qualified for using Host-based Privacy only. This qualification status doesn’t expire and can be used for new products that comply with the first case.

For qualifying a new product based on the QN9090, the designer should consider the system’s architecture.

In case the architecture is of type 1, described above, no retesting of subsystems is required and it is be qualified as Bluetooth LE 5, while using QN9090.

In case of type 2 above, retesting subsystems under the latest TCRL is usually required.

A product based on QN9090 can still use Controller-based Privacy without featuring Device Privacy mode, by qualifying as Bluetooth LE 4.2 device. TCRL 2019-2 does not define Device Privacy mode as mandatory for Bluetooth LE 4.2 devices. It is also important to consider that Bluetooth LE 4.2 devices do not support LL PHY 2M.

4 Enabling privacy on the QN9090

To enable or disable Host Privacy, the following API is used:

```
bleResult_t Gap_EnableHostPrivacy
(
    bool_t enable,
    const uint8_t * aIrk
);
```

See the Bluetooth® Low Energy Application Developer’s Guide available in SDK documentation for more information about NXP Bluetooth LE Stack.

5 Bluetooth SIG best privacy practices

Bluetooth SIG has released a guide to help developers understand and apply security and privacy measures into their projects. Bluetooth® Security and Privacy Best Practices Guide.

6 Application perspective: comparing variants

For the following comparison, consider the temperature collector and sensor use case. These projects are available in the QN9090 SDK. Note that this section is based on SDK projects for the purpose of comprehending privacy features available in QN9090. Low power modes that would optimize idle state current consumption were not added to the projects and the tests were executed for one master to one slave connection. Considerations for different use cases can be found in Conclusions.

The collector scans advertising packets from the sensor, connects, receives the instant value of the environment temperature, and disconnects. Both devices have previously paired and bonded.

For comparing privacy variants, this routine was executed for different privacy combinations in both devices. The sensor alternates between Public and Private addresses in its advertising packets using Host-based Privacy.

The collector is configured to three cases of privacy: disabled, host-based, and controller-based. The average value of 100 measurements was calculated and is shown. Connection interval was set to 7.5 ms and advertising interval to 20 ms.

The timing for a temperature collector to connect to a peer sensor device is acquired. Time is measured using CTIMER at 48 MHz timestamping, from the moment the collector starts scanning to the moment it connects to the sensor.

Table 1. Time for connecting while using different privacy configurations

Collector Privacy Variant	Disabled (Public)			Host-based (RPA)			Controller-based (RPA)		
Sensor address type	Public	RPA	**RPA**	Public	RPA	RPA	**Public**	RPA	RPA
Average time to connect (ms)	50.95	57.12	**N/A**	50.12	58.88	57.70	**N/A**	51.29	51.27

NOTE

The cases highlighted in bold in the table above indicate that a device that enables Controller-based privacy does not connect to another that uses no privacy.

The time difference between the Host-based and Controller-based privacy RPA resolution can be visualized by the instant current consumption. The plot shows the full routine of the temperature SDK project. An average filter was used to smooth curves. The final plot overlapped both cases. The horizontal axis expresses time in milliseconds (ms). The vertical axis expresses the instant current in milliamperes (mA).

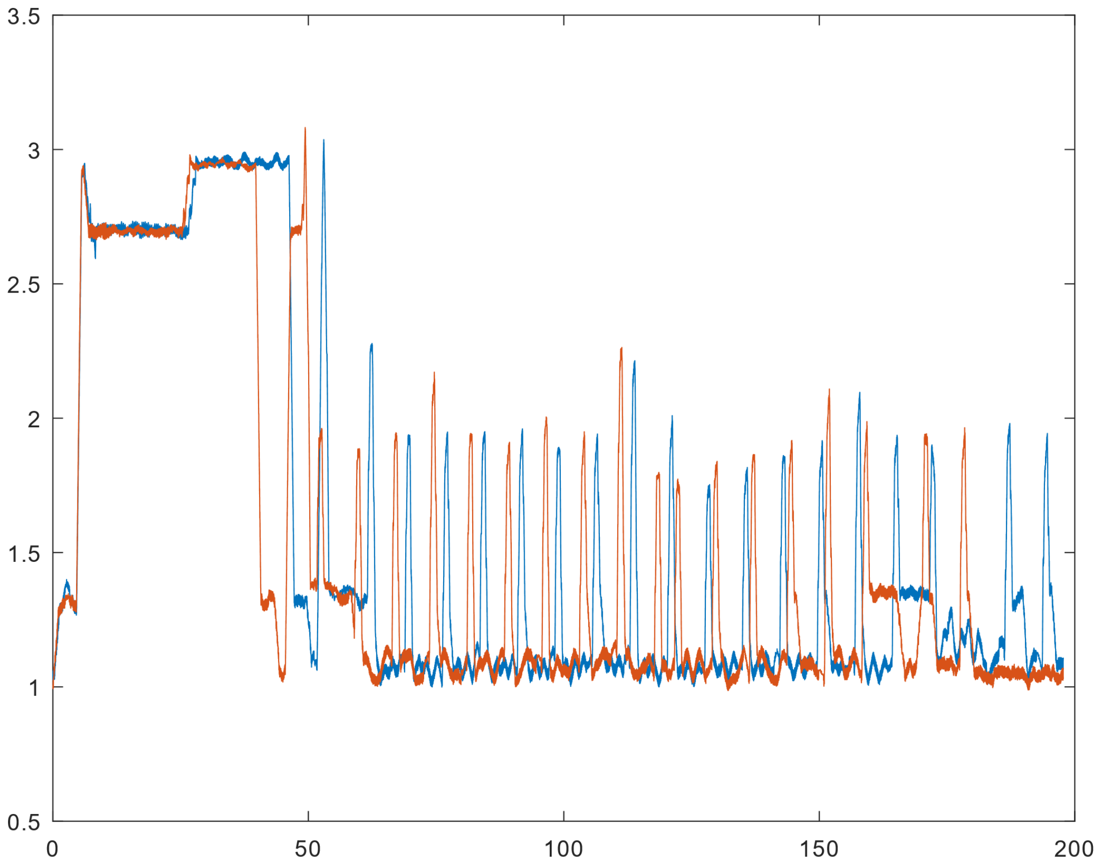

Figure 6. Instant current consumption obtained with MCUXpresso

It is possible to verify that, when using Controller-based privacy, the routine was executed in less time. The acquisition routine was performed 10 times for each case, controller and host-based. The average current for the execution was calculated.

Table 2. Time for connecting and current consumption for one routine execution

Collector Privacy Variant	Host-based	Controller-based
Average time to connect (ms)	58.29	51.28
Average current of a single routine execution (mA)	1.5904	1.5356

6.1 Estimating battery autonomy

To further understand the impacts at the application level, consider two periodic collectors based on the same SDK projects:

- One-Second Temperature Collector: updates the temperature value at each second
- One-Minute Temperature Collector: updates the temperature value at each minute

They scan the advertising sensor, resolve its address, connect, receive the temperature value, disconnect, and go to idle state with different time periods. A 230 mAh coin cell was considered as the power supply, and current consumption in idle state was taken as 1.0317 mA.

NOTE

Low power measures were not implemented for this example.

Table 3. One-second temperature collector

Collector Privacy Variant	Host-based	Controller-based
Average Current Consumption (mA)	1.1720	1.1595
Coin Cell Autonomy	**196.25 hours**	**198.36 hours**

Table 4. One-minute temperature collector

Collector Privacy Variant	Host-based	Controller-based
Average Current Consumption (mA)	1.0340	1.0338
Coin Cell Autonomy	**222.43 hours**	**222.47 hours**

7 Conclusions

The use of non-predictable private addressing modes is an important and recommended privacy measure, as in Bluetooth® Security and Privacy Best Practices Guide reference LE-9. QN9090 complies with this practice by featuring a true random number generator and Host and Controller-based privacy.

It is important to note that the benefits from using Controller-based privacy depend on the use case and system requirements. Applications that disconnect and reconnect more frequently execute RPA resolution more often. Therefore, these applications achieve greater performance by using Controller-based privacy.

Device filtering by white listing requires the use of Controller-based privacy and also provide better performance (time and current consumption) when compared to device filtering executed in the Host by software. Applications that use low power modes and operate in dense advertising environments also obtain greater advantage by resolving addresses in the Controller.

QN9090 supports and is qualified for using Host-based privacy as a Bluetooth LE 5 subsystem. All privacy-enabled QN9090 SDK projects are implemented with Host-based privacy. QN9090 supports Controller-based Privacy, Network Mode only, but it is not qualified for using it as a Bluetooth LE 5 subsystem. It is fully capable of enabling privacy using the Host layer. In case of qualifying QN9090 as a Bluetooth LE 4.2 device, Bluetooth SIG does not require Device Privacy Mode support. In this case, devices may support Controller-based Privacy in Network Mode only, and qualify for using it.

8 References

1. Bluetooth SIG. Bluetooth® Security and Privacy Best Practices Guide. Revision: 1.0. Revision Date: 15 April 2020.
2. Bluetooth SIG. Qualification Program Reference Document (PRD). Revision: 2.3. Date: 01 May 2014.
3. NXP Bluetooth® Low Energy Application Developer's Guide. Revision 1.1. Date: 19 December 2019.

How To Reach Us

Home Page:

nxp.com

Web Support:

nxp.com/support

Information in this document is provided solely to enable system and software implementers to use NXP products. There are no express or implied copyright licenses granted hereunder to design or fabricate any integrated circuits based on the information in this document. NXP reserves the right to make changes without further notice to any products herein.

NXP makes no warranty, representation, or guarantee regarding the suitability of its products for any particular purpose, nor does NXP assume any liability arising out of the application or use of any product or circuit, and specifically disclaims any and all liability, including without limitation consequential or incidental damages. “Typical” parameters that may be provided in NXP data sheets and/or specifications can and do vary in different applications, and actual performance may vary over time. All operating parameters, including “typicals,” must be validated for each customer application by customer's technical experts. NXP does not convey any license under its patent rights nor the rights of others. NXP sells products pursuant to standard terms and conditions of sale, which can be found at the following address: nxp.com/SalesTermsandConditions.

While NXP has implemented advanced security features, all products may be subject to unidentified vulnerabilities. Customers are responsible for the design and operation of their applications and products to reduce the effect of these vulnerabilities on customer’s applications and products, and NXP accepts no liability for any vulnerability that is discovered. Customers should implement appropriate design and operating safeguards to minimize the risks associated with their applications and products.

For more information, please visit: http://www.nxp.com
For sales office addresses, please send an email to: salesaddresses@nxp.com

Date of release: September, 2020
Document identifier: AN12928