Workgroup: RADEXT Working Group
Internet-Draft: draft-grayson-radext-rabble-01
Published: 10 July 2023
Intended Status: Standards Track
Expires: 11 January 2024
Authors: M. Grayson E. Lear
Cisco Systems Cisco Systems

RADIUS profile for Bonded Bluetooth Low Energy peripherals

Abstract

This document specifies an extension to the Remote Authentication Dial-In User Service (RADIUS) protocol that enables a Bluetooth Low Energy (BLE) peripheral device that has previously formed a bonded, secure trusted relationship with a first "home" Bluetooth Low Energy Central device to operate with a second "visited" Bluetooth Low Energy Central device.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 11 January 2024.

Table of Contents

1. Introduction

This document specifies an extension to the Remote Authentication Dial-In User Service (RADIUS) protocol [RFC2865] that enables a Bluetooth Low Energy (BLE) peripheral device that has previously formed a bonded, secure trusted relationship with a first "home" Bluetooth Low Energy Central device to operate with a second "visited" Bluetooth Low Energy Central device that is integrated with a Network Access Server.

After being successfully authenticated, a signalling link is established that enables Bluetooth messages advertised by the BLE Peripheral to be forwarded from the Visited Bluetooth Low Energy Central device to a Home MQTT Broker. For connectable BLE Peripherals, the signalling link enables the Home MQTT Broker to send BLE Requests or Commands to the Visited Bluetooth Low Energy Central device that is then responsible for forwarding to the BLE peripheral.

The extensions allow administrative entities to collaborate to enable RADIUS authentication of BLE devices onto their respective networks, without requiring the peripheral to perform a re-pairing on the visited network.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

1.2. Terminology

BLE Central Controller:

The BLE entity that implements the Bluetooth Link Layer and interacts with the Bluetooth Radio Hardware.

BLE Central Host:

A BLE entity that interacts with the BLE Central Controller to enable applications to communicate with peer BLE devices in a standard and interoperable way.

BLE Peripheral Device:

A BLE device that is configured to repeatedly send advertising messages.

BLE Security Database:

A database that stores the keying material associated with a bonded Bluetooth Connection.

Bluetooth Low Energy (BLE):

A wireless technology designed for low power operation and specified by the Bluetooth Special Interest Group.

Bonding:

A Bluetooth [BLUETOOTH] defined process that creates a relation between a Bluetooth Central device and a Bluetooth Peripheral device and which generates session keying material that is expected to be stored by both Bluetooth devices, to be used for future authentication.

Hash:

A Bluetooth [BLUETOOTH] specified 24-bit hash value which is calculated using a hash function operating on IRK and prand as its input parameters. The hash is encoded in the 24 least significant bits of a Resolvable Private Address.

Home:

A network that has access to the keying material necessary to support the pairing of a BLE peripheral and that is able to expose the keys generated as part of the BLE bonding process.

Identity Address (IA):

The 48-bit global (public) MAC address of a Bluetooth device.

Identity Resolving Key (IRK):

A Bluetooth [BLUETOOTH] specified key used in the Bluetooth privacy feature. The Resolvable Private Address hash value is calculated using a hash function of prand and the IRK.

Long-Term key (LTK):

A symmetric key which is generated during the Bluetooth bonding procedure and used to generate the session key used to encrypt a communication session between Bluetooth devices.

prand:

A 22-bit random number used by a BLE device to generate a Resolvable Private Address. The prand is encoded in the 24 most significant bits of a Resolvable Private Address.

Resolvable Private Address (RPA):

A Bluetooth [BLUETOOTH] specified private 48-bit address that can be resolved to a permanent Bluetooth Identity Address through the use of an Identity Resolving Key.

Visited:

A network that does not have access to the keying material necessary to support the pairing of a BLE peripheral, but that is able to support the RADIUS authentication of an already bonded BLE Peripheral.

2. BLE Roaming Overview

This section provides an overview of the RADIUS BLE mechanism, which is supported by the extensions described in this document. The RADIUS profile is intended to be used between a Visited BLE Central Host that is enhanced with Network Access Server (NAS) functionality which enables it to exchange messages with a RADIUS server.

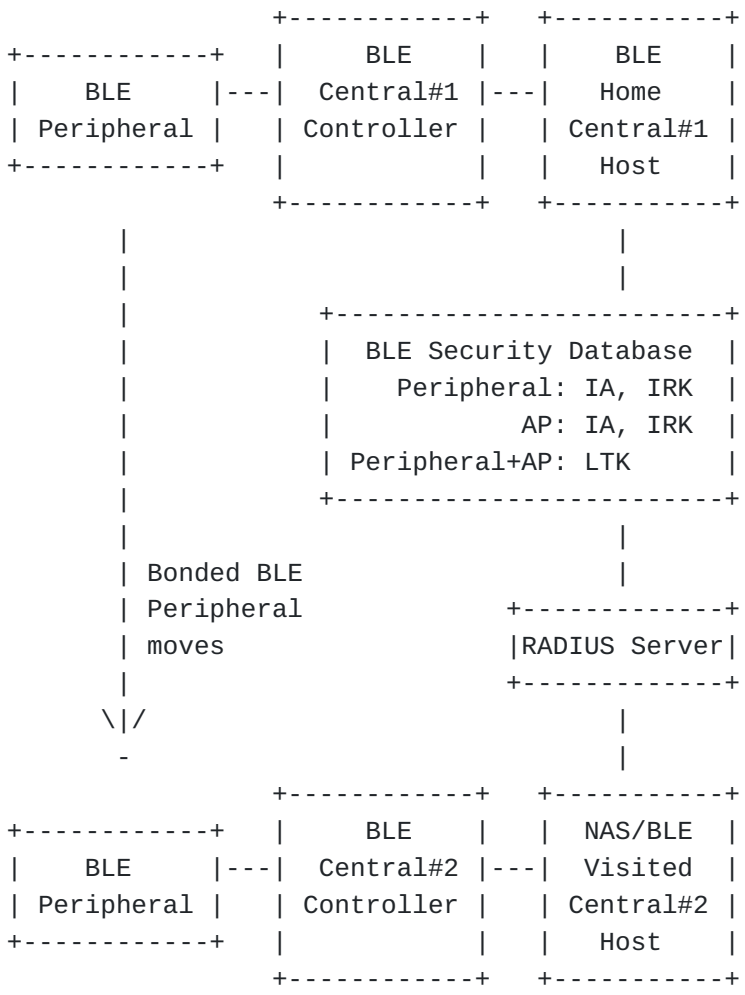

Figure 1: BLE RADIUS Authentication Overview

A BLE Peripheral is paired and bonded with the BLE Home Central Host. The pairing requires the BLE Home Central Host to have access to the keying material necessary to support the pairing of a BLE peripheral, e.g., by using techniques described in [I-D.shahzad-scim-device-model].

The bonding process generates new session specific keying material that MUST be exposed by the BLE Home Central Host to a RADIUS server, e.g., stored in a BLE Security Database which is accessible by the RADIUS server. The keying material MUST include the peripheral's IA and IRK, indicating that the BLE Peripheral has enabled the Bluetooth privacy feature and is operating with a Resolvable Private Address (RPA).

The BLE Peripheral then moves into the coverage of a second BLE Central device which comprises a second BLE Central Controller and a second BLE (Visited) Central Host which has been enhanced with Network Access Server (NAS) functionality. The BLE Peripheral MUST be configured to send low duty cycle advertising events using the

BLE Peripheral's RPA that are detected by the NAS/BLE Visited Central Host. The NAS/BLE Visited Central Host receives the Advertisement(s) sent by the BLE Peripheral and MAY use the presence and/or contents of specific Advertising Elements to decide whether to trigger a RADIUS exchange with a RADIUS Server which has access to the keying material exposed by the BLE Home Central Host.

The successful authentication of the BLE Peripheral onto the BLE Visited Central Host MUST include the signalling of the keying material exposed by the BLE Home Central Host to enable the re-establishment of the secured communication session with the BLE Peripheral. Bluetooth advertisements received from an authenticated BLE Peripheral are forwarded between the BLE Visited Central Host and a Home MQTT message broker.

If the BLE Peripheral is connectable, the Home MQTT Broker MAY send BLE Requests or Commands to the Visited Bluetooth Low Energy Central device that is then responsible for forwarding to the authenticated BLE peripheral. The Home MQTT Broker MAY be configured to forward the messages to/from a Bluetooth Application associated with the authenticated BLE Peripheral, either directly, or via the first Home Bluetooth Low Energy Central device.

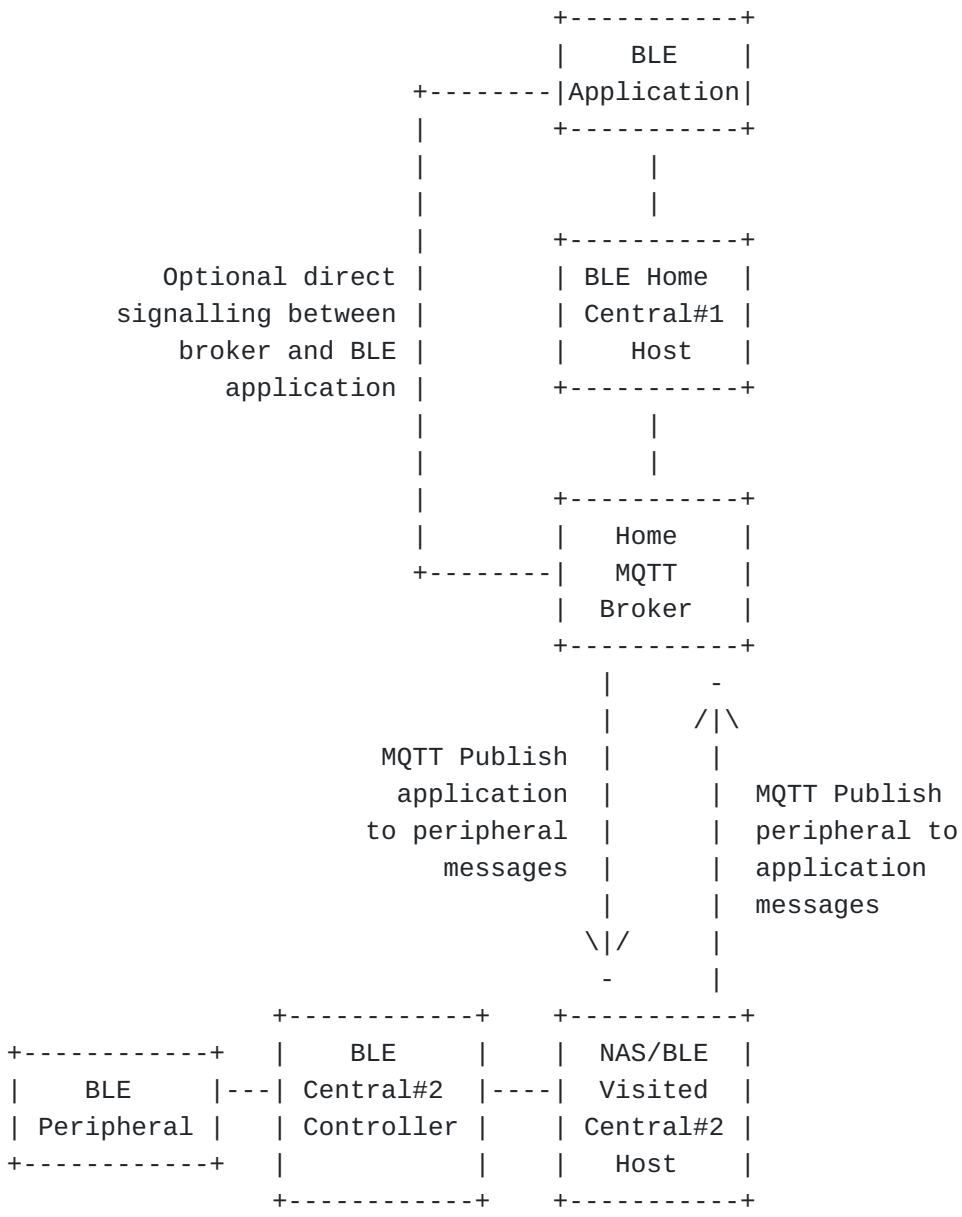

Figure 2: BLE Message Forwarding Overview

3. RADIUS Profile for BLE

3.1. User-Name

Contains a 6 character ASCII upper-case string corresponding to the hexadecimal encoding of the 22-bit prand value derived from the Bluetooth Resolvable Private Address, where the first string character represents the most significant hexadecimal digit, i.e., a prand value of 0x035fb2 is encoded as "035FB2".

3.2. NAS-IP-Address, NAS-IPv6-Address

The NAS-IP-Address contains the IPv4 address of the BLE Central Host acting as an Authenticator, and the NAS-IPv6-Address contains the IPv6 address.

3.3. NAS-Port

For use with BLE the NAS-Port will contain the port number of the BLE Central Host, if this is available.

3.4. Service-Type

For use with BLE, the Service-Type of Authenticate Only (8) is used.

3.5. State, Class, Proxy-State

These attributes are used for the same purposes as described in [RFC2865].

3.6. Vendor-Specific

Vendor-specific attributes are used for the same purposes as described in [RFC2865].

3.7. Session-Timeout

When sent in an Access-Accept without a Termination-Action attribute or with a Termination-Action attribute set to Default, the Session-Timeout attribute specifies the maximum number of seconds of service provided prior to session termination.

3.8. Idle-Timeout

The Idle-Timeout attribute indicates the maximum time that the BLE wireless device may remain idle.

3.9. Termination-Action

This attribute indicates what action should be taken when the service is completed. The value Default (0) indicates that the session should terminate.

3.10. Called-Station-Id

This attribute is used to store the public Identity Address (BD_ADDR) of the Bluetooth Access Point in ASCII formatted as specified in section 3.21 of [RFC3580].

3.11. NAS-Identifier

This attribute contains a string identifying the BLE Central Host originating the Access-Request.

3.12. NAS-Port-Type

TBA1: "Wireless - Bluetooth Low Energy"

3.13. Hashed-Password

Description

The Hashed-Password (TBA2) Attribute allows a RADIUS client to include a key and hashed password.

Type

TBA2

Length

Variable

Data Type

TLV

Value

The TLV data type is specified in section 3.13 of [RFC8044] and its value is determined by the TLV-Type field. Two TLV-Types are defined for use with the Hashed-Password Attribute.

3.13.1. Hashed-Password.Hmac-Sha256-128-Key

TLV-Type

0 (Hashed-Password.Hmac-Sha256-128-Key)

TLV-Value:

A string data type, as defined in section 3.1 of [RFC8044], encoding a sequence of octets representing a random 256-bit key. The value SHOULD satisfy the requirements of [RFC4086]. A new key value MUST be used whenever the value of Hashed-Password.Hmac-Sha256-128-Password is changed. The key MUST NOT be changed when a message is being retransmitted.

TLV-Length:

34 octets

3.13.2. Hashed-Password.Hmac-Sha256-128-Password

TLV-Type

1 (Hashed-Password.Hmac-Sha256-128-Password)

TLV-Value:

A string data type encoding a sequence of octets representing the first 128-bit (truncated) output of the HMAC-SHA-256-128 algorithm [RFC4868] where the input data corresponds to the 24-bit hash recovered from the Bluetooth Resolvable Private Address and the key corresponds to the value of the TLV-Type Hashed-Password.Hmac-Sha256-128-Key.

TLV-Length:

18 octets

3.13.3. Hashed-Password TLV-Type Usage

Two instances of the Hashed-Password Attribute MUST be included in an Access-Request packet. One instance MUST correspond to the TLV-Type 0 (Hashed-Password.Hmac-Sha256-128-Key) and one instance MUST correspond to the TLV-Type 1 (Hashed-Password.Hmac-Sha256-128-Password).

3.14. GATT-Service-Profile

Description

The GATT-Service-Profile (TBA3) Attribute allows a RADIUS client to include one or more GATT Service Profiles which are advertised by the BLE Peripheral.

Zero or more GATT-Service-Profile Attributes MAY be included in an Access-Request packet.

A summary of the GATT-Service-Profile Attribute format is shown below. The fields are transmitted from left to right.

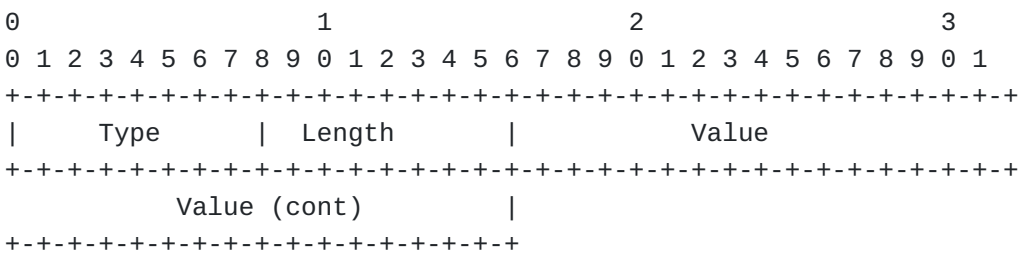

Figure 3: Encoding GATT-Service-Profile Attribute

Type

TBA3

Length

6 octet

Data Type

Integer

Value

The field is 4 octets, containing a 32-bit unsigned integer that represents a GATT Service Profile.

3.15. BLE-Keying-Material Attribute

Description

The BLE-Keying-Material (TBA3) Attribute allows the transfer of Identity Address(es) and cryptographic keying material from a RADIUS Server to the BLE Visited Central Host.

Type

TBA3

Length

Variable

Data Type

TLV

Value

The TLV data type is specified in section 3.13 of [RFC8044] and its value is determined by the TLV-Type field. Five TLV-Types are defined for use with the BLE-Keying-Material Attribute.

3.15.1. BLE-Keying-Material.Peripheral-IA

TLV-Type

0 (BLE-Keying-Material.Peripheral-IA)

TLV-Value:

A string data type encoding a sequence of octets representing the Peripheral's 6-octet Identity Address.

TLV-Length:

8 octets

3.15.2. BLE-Keying-Material.Central-IA

TLV-Type

1 (BLE-Keying-Material.Central-IA)

TLV-Value:

A string data type encoding a sequence of octets representing the Central's 6-octet Identity Address.

TLV-Length:

8 octets

3.15.3. BLE-Keying-Material.IV

TLV-Type

2 (BLE-Keying-Material.IV)

TLV-Value:

A string data type encoding a sequence of octets representing an 8-octet initial value (IV). The value MUST be as specified in section 2.2.3 of [RFC3394].

TLV-Length:

10 octets

3.15.4. BLE-Keying-Material.KEK-ID

TLV-Type

3 (BLE-Keying-Material.KEK-ID)

TLV-Value:

A string data type encoding a sequence of octets representing the identity of a Key Encryption Key (KEK). The combination of the BLE-Keying-Material.KEK-ID value and the RADIUS client and server IP addresses together uniquely identify a key shared between the RADIUS client and server. As a result, the BLE-Keying-Material.KEK-ID need not be globally unique. The BLE-Keying-Material.KEK-ID MUST refer to an encryption key for use with the AES Key Wrap with 128-bit KEK algorithm [RFC3394].
This key is used to protect the contents of the BLE-Keying-Material.KM-Data TLV (see Section 3.15.6).

The BLE-Keying-Material.KEK-ID is a constant that is configured through an out-of-band mechanism. The same value is configured on both the RADIUS client and server. If no BLE-Keying-Material.KEK-ID TLV-Type is signalled, then the field is set to 0. If only a single KEK is configured for use between a given RADIUS client and server, then 0 can be used as the default value.

TLV-Length:

18 octets

3.15.5. BLE-Keying-Material.KM-Type

TLV-Type:

4 (BLE-Keying-Material.KM-Type)

TLV-Value:

An integer data type identifying the type of keying material included in the BLE-Keying-Material.KM-Data TLV.
This allows for multiple keys for different purposes to be present in the same attribute. This document defines three values for the The BLE-Keying-Material.KM-Type

0 The BLE-Keying-Material.KM-Data TLV contains the 16-octet Peripheral IRK encrypted using the AES key wrapping process with 128-bit KEK defined in [RFC3394]. The Peripheral IRK is passed as input P1 and P2, with the plaintext P1 corresponding to octet 0 through to octet 7 of

the IRK and plaintext P2 corresponding to octet 8 through to octet 15 of the IRK.

1 The BLE-Keying-Material.KM-Data TLV contains the encrypted 16-octet Peripheral IRK and the 16-octet LTK generated during an LE Secure Connection bonding procedure using the AES key wrapping process with 128-bit KEK defined in [RFC3394]. The Peripheral IRK is passed as the plaintext input P1 and P2, with P1 corresponding to octet 0 through to octet 7 of the IRK and P2 corresponding to octet 8 through to octet 15 of the IRK. The LTK is passed as the plaintext input P3 and P4, with P3 corresponding to octet 0 through to octet 7 of the LTK and P4 corresponding to octet 8 through to octet 15 of the LTK.

2 The BLE-Keying-Material.KM-Data TLV contains the encrypted 16-octet Peripheral IRK, the 16-octet LTK generated during an LE Secure Connection bonding procedure and the 16-octet Central IRK using the AES key wrapping process with 128-bit KEK defined in [RFC3394]. The Peripheral IRK is passed as the plaintext input P1 and P2, with P1 corresponding to octet 0 through to octet 7 of the IRK and P2 corresponding to octet 8 through to octet 15 of the IRK. The LTK is passed as the plaintext input P3 and P4, with P3 corresponding to octet 0 through to octet 7 of the LTK and P4 corresponding to octet 8 through to octet 15 of the LTK. The Central IRK is passed as plaintext input P5 and P6, with P5 corresponding to octet 0 through to octet 7 of the Central IRK and P6 corresponding to octet 8 through to octet 15 of the Central IRK.

TLV-Length:

6 octets

3.15.6. BLE-Keying-Material.KM-Data

TLV-Type:

5 (BLE-Keying-Material.KM-Data)

TLV-Value:

A string data type encoding a sequence of octets representing the actual encrypted keying material as identified using the BLE-Keying-Material.KM-Type.

TLV-Length:

Variable

3.15.7. BLE-Keying-Material TLV-Type Usage

At least four instances of the BLE-Keying-Material Attribute MUST be included in an Access-Accept packet, that include the following TLV-Types:

*TLV-Type 0 (BLE-Keying-Material.Peripheral-IA)

*TLV-Type 2 (BLE-Keying-Material.IV)

*TLV-Type 4 (BLE-Keying-Material.KM-Type)

*TLV-Type 5 (BLE-Keying-Material.KM-Data)

If a KEK is configured, then in addition the Access-Accept packet MUST include the BLE-Keying-Material Attribute with an instance of TLV-Type 3 (BLE-Keying-Material.KEK-ID). When not present, the NAS MUST use a default value of 0 for the KEK-ID.

If the BLE Peripheral is connectable and the RADIUS Server authorizes connections, then in addition the Access-Accept message MUST include the BLE-Keying-Material Attribute with an instance of TLV-Type 1 (BLE-Keying-Material.Central-IA).

3.16. Forwarding Bluetooth Messages

RADIUS attributes described in this section are used to exchange information to allow non-IP Bluetooth messages to be transferred between the BLE Visited Central Host and a Home MQTT Broker.

3.16.1. MQTT-Broker-URI

Description

The MQTT-Broker-URI (TBA5) Attribute allows a RADIUS server to specify the URI of the MQTT Broker. A single MQTT-Broker-URI Attributes MAY be included in an Access-Accept packet.

If the RADIUS server operates with NAS/BLE Visited Hosts that are deployed behind firewalls or NAT gateways, MQTT Messages SHOULD be transported using WebSocket [RFC6455] as a network transport as defined in MQTT [MQTT] and the the attribute SHOULD specify the URI of a WebSocket server that supports the 'mqtt' Sec-WebSocket-Protocol.

A summary of the MQTT-Broker-URI Attribute format is shown below. The fields are transmitted from left to right.

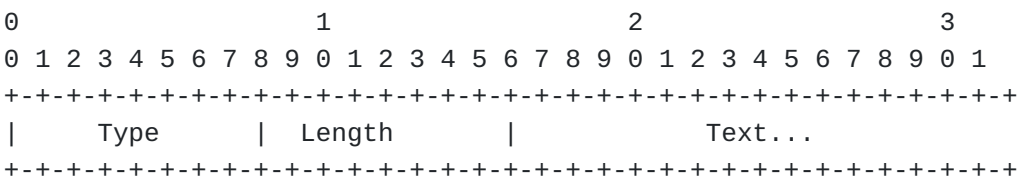

Figure 4: Encoding MQTT-Broker-URI Attribute

Type

TBA5

Length

>=3 octet

Data Type

Text

Value

The text field encodes a URI where the MQTT service can be accessed, e.g., "wss://broker.example.com:443".

3.16.2. MQTT-Token

Description

The MQTT-Token (TBA6) Attribute allows a RADIUS server to signal a token for use by an MQTT client in an MQTT CONNECT packet [MQTT]. The token can be used by an MQTT Broker to associate an MQTT Connection from an MQTT Client with a Network Access Server.

A MQTT-Token Attributes MAY be included in an Access-Accept packet.

A summary of the MQTT-Token Attribute format is shown below. The fields are transmitted from left to right.

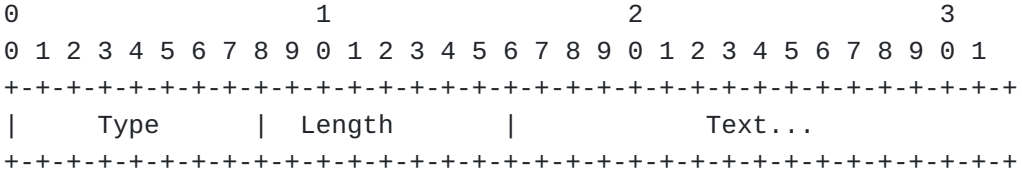

Figure 5: Encoding MQTT-Token Attribute

Type

TBA6

Length

>=3 octet

Data Type

Text

Value

The text field contains a token for use with an MQTT CONNECT packet.

3.17. RADIUS Accounting Attributes

With a few exceptions, the RADIUS accounting attributes defined in [RFC2866] have the same meaning within BLE sessions as they do in dialup sessions and therefore no additional commentary is needed.

3.17.1. Acct-Input-Octets and Acct-Output-Octets

These attributes are not not used by BLE Authenticators.

3.17.2. Acct-Input-Packets

This attribute is used to indicate how many MQTT messages that include the Peripheral Identity Address signalled in the BLE-Keying-Material attribute have been sent by the BLE Central Host.

3.17.3. Acct-Output-Packets

This attribute is used to indicate how many MQTT messages that include the Peripheral Identity Address signalled in the BLE-Keying-Material attribute have been received by the BLE Central Host.

3.17.4. Acct-Terminate-Cause

This attribute indicates how the session was terminated, as described in [RFC2866]. When the idle-timeout attribute is used by the NAS/BLE Visited Host to terminate a RADIUS Accounting session, it MUST set the Acct-Terminate-Cause set to Lost Carrier (2).

4. BLE RADIUS Exchange

The BLE Peripheral uses techniques defined in Bluetooth Core Specifications [BLUETOOTH] to establish a bonded, secure, trusted relationship with a BLE Home Central device in the network. The bonding procedure generates session specific keying material. The BLE Peripheral sends low duty cycle advertising events.

The BLE Peripheral moves into coverage of a second BLE Central device that is integrated with a NAS.

The BLE Peripheral sends Advertisements using its Resolvable Public Address. The contents of the Advertisements are signalled to a BLE Visited Central Host associated with the second BLE Central device. The received Advertisements sent by the BLE Peripheral are used by the BLE Visited Central Host to decide whether to trigger a RADIUS exchange, e.g., using the presence and/or contents of specific Advertising Elements.

The NAS associated with the BLE Visited Central Host is configured with the identity of the RADIUS server. The NAS/BLE Visited Host MAY be statically configured with the identity of a RADIUS Server. Alternatively, the NAS/BLE Visited Host MAY use the contents of an Advertisement Element received from the BLE Peripheral to derive an FQDN of the RADIUS sever and use RFC 7585 [RFC7585] to dynamically resolve the address of the RADIUS server. For example, the peripheral can use the Bluetooth URI data type Advertisement Element (0x24) to encode the Bluetooth defined 'empty scheme' name tag together with a hostname that identifies the network which operates the BLE Home Central Host associated with the peripheral. Alternatively, a federation of operators of BLE Visited Centrals and RADIUS Servers can define the use of the Bluetooth defined Manufacturer Specific Advertisement Data Element (0xFF) together with a Company Identifier that identifies the federation to signal a federation defined sub-type that encodes information that enables the BLE Visited Central Host to derive an FQDN of the RADIUS sever associated with the advertising peripheral.

The NAS/BLE Host generates a RADIUS Access-Request message using the prand from the RPA as the User-Name attribute and the hash from the RPA to generate the TLV-Type Hashed-Password.Hmac-Sha256-128-Password. The NAS-Port-Type is set to "Wireless - Bluetooth Low Energy".

On receiving the RADIUS Access-Request message, the RADIUS Server uses the keying material exposed by the BLE Home Central Host and attempts to resolve the User-Name and the TLV-Type Hashed-Password.Hmac-Sha256-128-Password to a known BLE Identity Address (IA). If the RADIUS Server cannot resolve the User-Name and TLV-Type

Hashed-Password.Hmac-Sha256-128-Password to a known BLE Identity Address, the RADIUS server MUST reject the Access-Request.

If the RADIUS Server resolves the User-Name and TLV-Type Hashed-Password.Hmac-Sha256-128-Password to a known BLE Identity Address, and the BLE Identity Address is authorized to access via the BLE Visited Host, the RADIUS server recovers the session specific keying material exposed by the BLE Home Central Host.

If the BLE Peripheral is not connectable or connections are not authorized, the RADIUS server signals the Peripheral Identity Address in the TLV-type BLE-Keying-Material.Peripheral-IA, sets the value of TLV-Type BLE-Keying-Material.KM-Type to 0 and encodes the Peripheral Identity Resolving Key in the TLV-Type BLE-Keying-Material.KM-Data. If the BLE Peripheral is connectable and connections are authorized via the BLE Visited Host, the RADIUS server additionally includes the Central Identity Address in the TLV-type BLE-Keying-Material.Central-IA, sets the value of TLV-Type BLE-Keying-Material.KM-Type to 1 and encodes the Peripheral Identity Resolving Key and the 16-octet Long Term Key in the TLV-Type BLE-Keying-Material.KM-Data. Finally, if the BLE Peripheral is connectable and connections are authorized via the BLE Visited Host and the security database indicates that the BLE Home Central Host operates using Bluetooth privacy, then the RADIUS server sets the value of TLV-Type BLE-Keying-Material.KM-Type to 2 and encodes the Peripheral Identity Resolving Key, the 16-octet Long Term Key and the 16-octet Central Identity Resolving Key in the TLV-Type BLE-Keying-Material.KM-Data.

The RADIUS Server SHOULD include the MQTT-Broker-URI attribute and MAY include the MQTT-Token attribute by which an MQTT client associated with the BLE Visited Host can establish an MQTT connection with a Home MQTT Broker for forwarding messages received to/from the BLE peripheral.

On receiving the Access-Accept, the NAS/BLE Visited Host recovers the keying material, including the BLE Peripheral's Identity Address and then establishes an MQTT Connection with the Home MQTT Broker. The NAS/BLE Visited Host SHOULD include its NAS-Id in the User Name field of the MQTT CONNECT message and MAY include an Operator Name, if for example the NAS has been configured with the operator-name attribute (#126) as specified in section 4.1 of RFC5580 [RFC5580].

If the advertisement that triggered the RADIUS exchange corresponds to an ADV_IND then the NAS/BLE Visited Host can subsequently establish a secure connection with the BLE Peripheral.

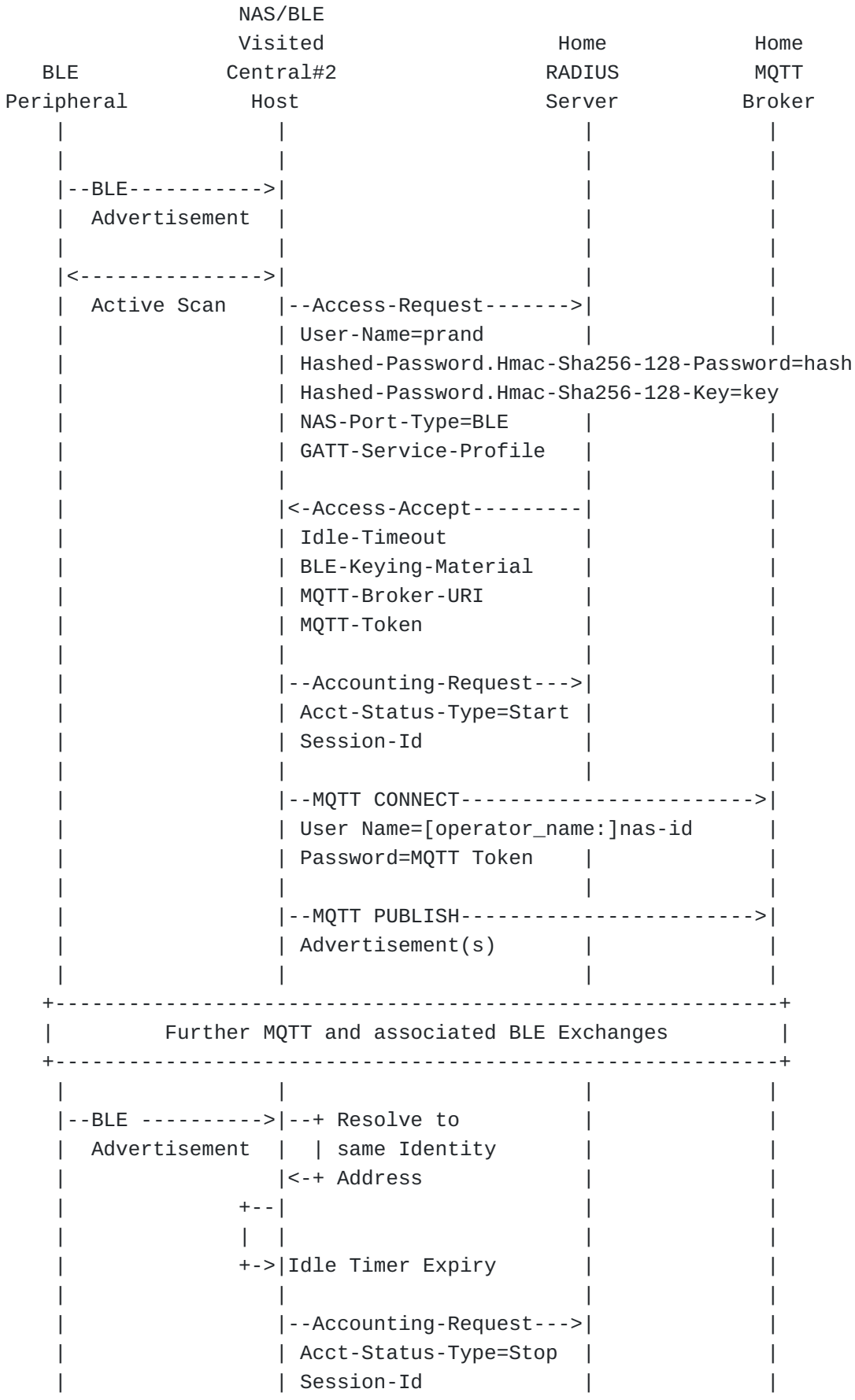
NAS/BLE
Visited
Central#2
Host
Home
RADIUS
Server
Home
MQTT
Broker
BLE
Peripheral
--BLE----------->|
Advertisement
<----------->|
Active Scan
--Access-Request------->|
User-Name=prand
Hashed-Password.Hmac-Sha256-128-Password=hash
Hashed-Password.Hmac-Sha256-128-Key=key
NAS-Port-Type=BLE
GATT-Service-Profile
<-Access-Accept---------|
Idle-Timeout
BLE-Keying-Material
MQTT-Broker-URI
MQTT-Token
--Accounting-Request--->|
Acct-Status-Type=Start
Session-Id
--MQTT CONNECT----------->|
User Name=[operator_name:]nas-id
Password=MQTT Token
--MQTT PUBLISH----------->|
Advertisement(s)
Further MQTT and associated BLE Exchanges
--BLE ---------->|--+ Resolve to
Advertisement
<-+ Address
+--|
+->|Idle Timer Expiry
--Accounting-Request--->|
Acct-Status-Type=Stop
Session-Id

Figure 6: BLE RADIUS Exchange

5. Table of Attributes

The following table provides a guide to which of the attribute defined may be found in which kinds of packets, and in what quantity.

Request	Accept	Reject	Challenge	Acct-Request	#	Attribute
1+	0	0	0	0	TBA2	Hashed-Password
0+	0	0	0	0	TBA3	GATT-Service-Profile
0	1+	0	0	0	TBA4	BLE-Keying-Material
0	0-1	0	0	0	TBA5	MQTT-Broker-URI
0	0-1	0	0	0	TBA6	MQTT-Token

Table 1: Table of Attributes

The following table defines the meaning of the above table entries.

Entry	Meaning
0	This attribute MUST NOT be present in packet.
0+	Zero or more instances of this attribute MAY be present in packet.
0-1	Zero or one instance of this attribute MAY be present in packet.
1	One instance of this attribute MUST be present in packet.

Table 2: Table of Attributes Entry Definition

6. Security Considerations

Use of this RADIUS profile for BLE can be between a NAS/BLE Visited Host and a RADIUS Server inside a secure network, or between a NAS/BLE Visited Host and RADIUS server operated in different administrative domains which are connected over the Internet. All implementations MUST follow [I-D.draft-dekok-radext-deprecating-radius].

The RADIUS profile for BLE devices is designed to operate when BLE devices operate their physical links with BLE Secure Connections [BLUETOOTH]. This approach uses a secure exchange of data over the Bluetooth connection, together with Elliptic Curve Diffie-Hellman (ECDH) public key cryptography, to create the session specific symmetric Long Term Key (LTK) which is then exchanged using the BLE-Keying-Material attribute in the RADIUS Access-Accept message.

Bluetooth [BLUETOOTH] specifies how an IRK can be generated from an Identity Root (IR) key. Removing the Bluetooth bond in a device will typically trigger the generation of a new IRK key for the device.

The RADIUS profile for BLE devices is designed to operate when BLE devices are configured to operate with Bluetooth Privacy Mode enabled [BLUETOOTH]. The BLE device defines the policy of how often it should generate a new Resolvable Private Address. This can be configured to be between every second and every hour, with a default value of every 15 minutes [BLUETOOTH]. This mode mitigates risks associated with a malicious third-party scanning for and collecting Bluetooth addresses over time and using such to build a picture of the movements of BLE devices and, by inference, the human users of those devices.

The Home MQTT broker can observe the Bluetooth messages exchanged with the BLE Peripheral. The Bluetooth GATT attributes SHOULD be cryptographically protected at the application-layer. The Home MQTT Broker MUST be configured with access control lists so that a NAS cannot subscribe to a topic that is intended for another NAS.

The WebSocket connection MUST operate using a WebSocket Secure connection. If the entropy of the MQTT-Token is known to be low, the WebSocket Secure TLS connection SHOULD be secured with certificate-based mutual TLS.

7. IANA Considerations

This document defines a new value of TBA1 for RADIUS Attribute Type #61 (NAS-Port-Type) defined in https://www.iana.org/assignments/radius-types/radius-types.xhtml#radius-types-13

Value	Description	Reference
TBA1	"Wireless - Bluetooth Low Energy"	Section 3.12

Table 3: New NAS-Port-Type value defined in this document

This document defines new RADIUS attributes, (see section Section 3), and assigns values of TBA2, TBA3, TBA4, TBA5 and TBA6 from the RADIUS Attribute Type space https://www.iana.org/assignments/radius-types.

Tag	Attribute	Reference
TBA2	Hashed-Password	Section 3.13
TBA3	GATT-Service-Profile	Section 3.14
TBA4	BLE-Keying-Material	Section 3.15
TBA5	MQTT-Broker-URI	Section 3.16.1

Tag	Attribute	Reference
TBA6	MQTT-Token	Section 3.16.2

Table 4: New RADIUS attributes defined in this document

8. References

8.1. Normative References

[I-D.draft-dekok-radext-deprecating-radius]
DeKok, A., "Deprecating RADIUS/UDP and RADIUS/TCP", Work in Progress, Internet-Draft, draft-dekok-radext-deprecating-radius-01, 3 March 2023, <https://datatracker.ietf.org/doc/html/draft-dekok-radext-deprecating-radius-01>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, DOI 10.17487/RFC2865, June 2000, <https://www.rfc-editor.org/info/rfc2865>.

[RFC4086] Eastlake 3rd, D., Schiller, J., and S. Crocker, "Randomness Requirements for Security", BCP 106, RFC 4086, DOI 10.17487/RFC4086, June 2005, <https://www.rfc-editor.org/info/rfc4086>.

[RFC4868] Kelly, S. and S. Frankel, "Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec", RFC 4868, DOI 10.17487/RFC4868, May 2007, <https://www.rfc-editor.org/info/rfc4868>.

[RFC5580] Tschofenig, H., Ed., Adrangi, F., Jones, M., Lior, A., and B. Aboba, "Carrying Location Objects in RADIUS and

Diameter", RFC 5580, DOI 10.17487/RFC5580, August 2009, <https://www.rfc-editor.org/info/rfc5580>.

[RFC6455] Fette, I. and A. Melnikov, "The WebSocket Protocol", RFC 6455, DOI 10.17487/RFC6455, December 2011, <https://www.rfc-editor.org/info/rfc6455>.

[RFC8044] DeKok, A., "Data Types in RADIUS", RFC 8044, DOI 10.17487/RFC8044, January 2017, <https://www.rfc-editor.org/info/rfc8044>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

8.2. Informative References

[BLUETOOTH] Bluetooth Core Specification Working Group, "BLUETOOTH CORE SPECIFICATION v5.3", 13 July 2021, <https://www.bluetooth.com/specifications/bluetooth-core-specification/>.

[I-D.shahzad-scim-device-model] Shahzad, M., Hassan, H., and E. Lear, "Device Schema Extensions to the SCIM model", Work in Progress, Internet-Draft, draft-shahzad-scim-device-model-05, 2 June 2023, <https://datatracker.ietf.org/doc/html/draft-shahzad-scim-device-model-05>.

[MQTT] OASIS, "MQTT Version 5.0", 7 March 2019, <https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.html>.

[RFC2866] Rigney, C., "RADIUS Accounting", RFC 2866, DOI 10.17487/RFC2866, June 2000, <https://www.rfc-editor.org/info/rfc2866>.

[RFC3394] Schaad, J. and R. Housley, "Advanced Encryption Standard (AES) Key Wrap Algorithm", RFC 3394, DOI 10.17487/RFC3394, September 2002, <https://www.rfc-editor.org/info/rfc3394>.

[RFC3580] Congdon, P., Aboba, B., Smith, A., Zorn, G., and J. Roese, "IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines", RFC 3580, DOI 10.17487/RFC3580, September 2003, <https://www.rfc-editor.org/info/rfc3580>.

[RFC7585] Winter, S. and M. McCauley, "Dynamic Peer Discovery for RADIUS/TLS and RADIUS/DTLS Based on the Network Access Identifier (NAI)", RFC 7585, DOI 10.17487/RFC7585, October 2015, <https://www.rfc-editor.org/info/rfc7585>.

Appendix A. MQTT Interworking

This section describes how a NAS/BLE Visited Host supporting the BLE RADIUS profile can interwork with a Home MQTT Message Broker in order to use MQTT topics to deliver Bluetooth messages to/from a BLE Peripheral. It is intended to move this material to another document - but is included here to describe, at a high level, the MQTT interworking established by the RADIUS exchange.

A.1. Establishing a Session to a MQTT-Broker-URI

If the NAS/BLE Visited Host is signalled a MQTT-Broker-URI in an Access-Accept with which it does not have an established MQTT connection, then it MUST establish an MQTT connection. It the NAS/BLE Visited Host is behind a firewall or NAT gateway it MUST use WebSocket transport for the MQTT connection. The user name in the MQTT CONNECT message SHOULD include the NAS-ID and MAY include the name of the operator of the NAS/BLE Visited Host.

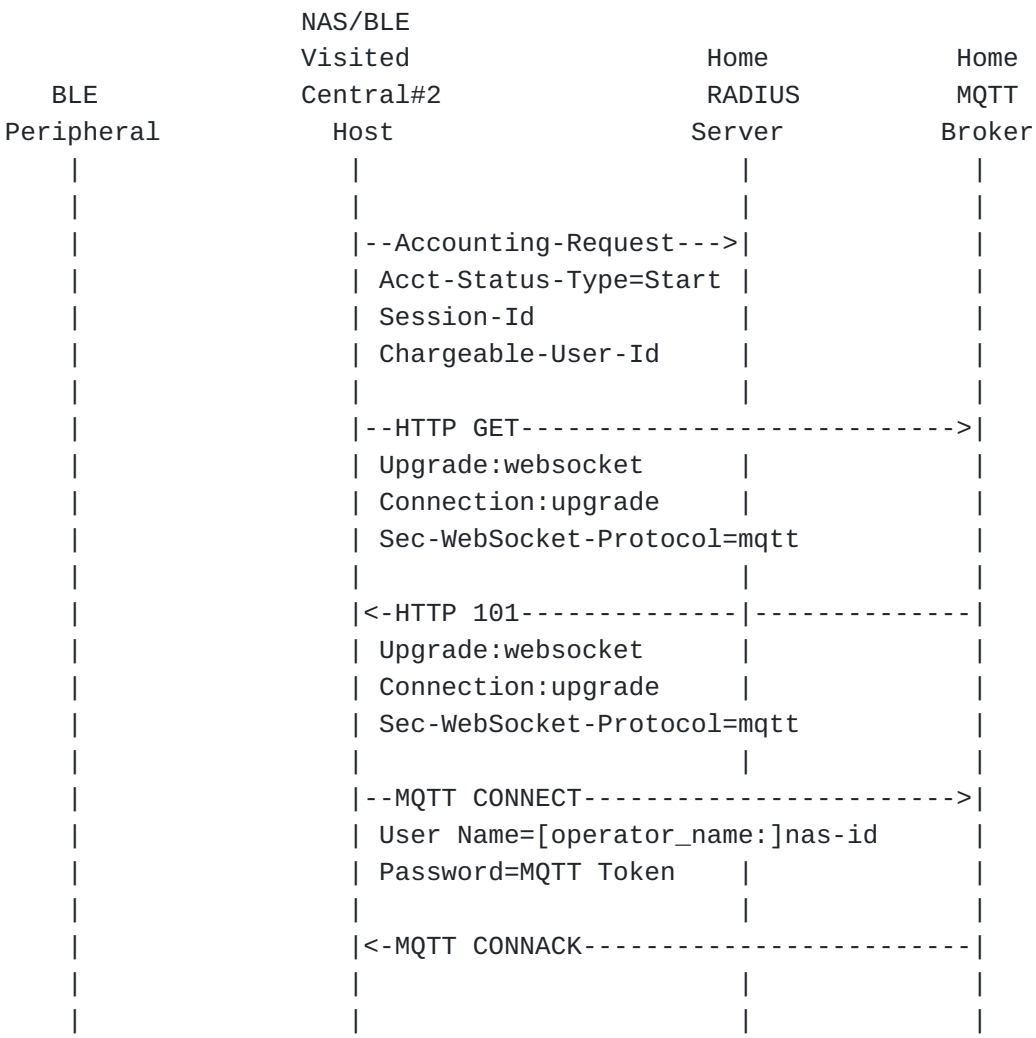

Figure 7: Establishing an MQTT connection to a Home Broker using WebSocket transport

A.2. MQTT topics

The following topic is used by the MQTT client of the BLE Visited Host to signal active and passive scan advertisements received from BLE Peripherals to the home MQTT Broker.

*{peripheral_identity_address}/advertisement/gatt-ind

If the BLE Peripheral is connectable, the MQTT client of the BLE Visited Host SHOULD subscribe to the following message topics to be able to receive GATT requests from the Home MQTT Broker:

1. {peripheral_identity_address}/connect/gatt-req : when publishing a message on the {peripheral_identity_address}/connect/gatt-req topic, an MQTT client SHOULD include the following as a response topic {peripheral_identity_address}/connect/gatt-res.

2. {peripheral_identity_address}/disconnect/gatt-req : when publishing a message on the {peripheral_identity_address}/disconnect/gatt-req topic, an MQTT client SHOULD include the following as a response topic {peripheral_identity_address}/disconnect/gatt-res.

3. {peripheral_identity_address}/read/gatt-req : when publishing a message on the {peripheral_identity_address}/read/gatt-req topic, an MQTT client SHOULD include the following as a response topic {peripheral_identity_address}/read/gatt-res.

4. {peripheral_identity_address}/write/gatt-req : when publishing a message on the {peripheral_identity_address}/write/gatt-req topic, an MQTT client SHOULD include the following as a response topic {peripheral_identity_address}/write/gatt-res.

5. {peripheral_identity_address}/service-discovery/gatt-req : when publishing a message on the {peripheral_identity_address}/service-discovery/gatt-req topic, an MQTT client SHOULD include the following as a response topic {peripheral_identity_address}/service-discovery/gatt-res.

6. {peripheral_identity_address}/notification/gatt-ind-res : when sending indications, the MQTT client of the NAS/BLE Visited Host SHOULD publish the message using the topic: {peripheral_identity_address}/notification/gatt-ind-req indication and SHOULD include the following as a response topic {peripheral_identity_address}/notification/gatt-ind-res.

A.3. MQTT Exchange for Non-Connectable BLE Peripherals

If the BLE Peripheral indicates in its scan that it is not connectable, the NAS/BLE Visited Host is responsible for publishing the received advertisements received from the authenticated BLE Peripheral.

On idle-timeout the NAS/BLE Visited Host MUST send an Accounting-Request message with Acct-Status-Type set to STOP and Acct-Terminate-Cause set to Lost Carrier (2).

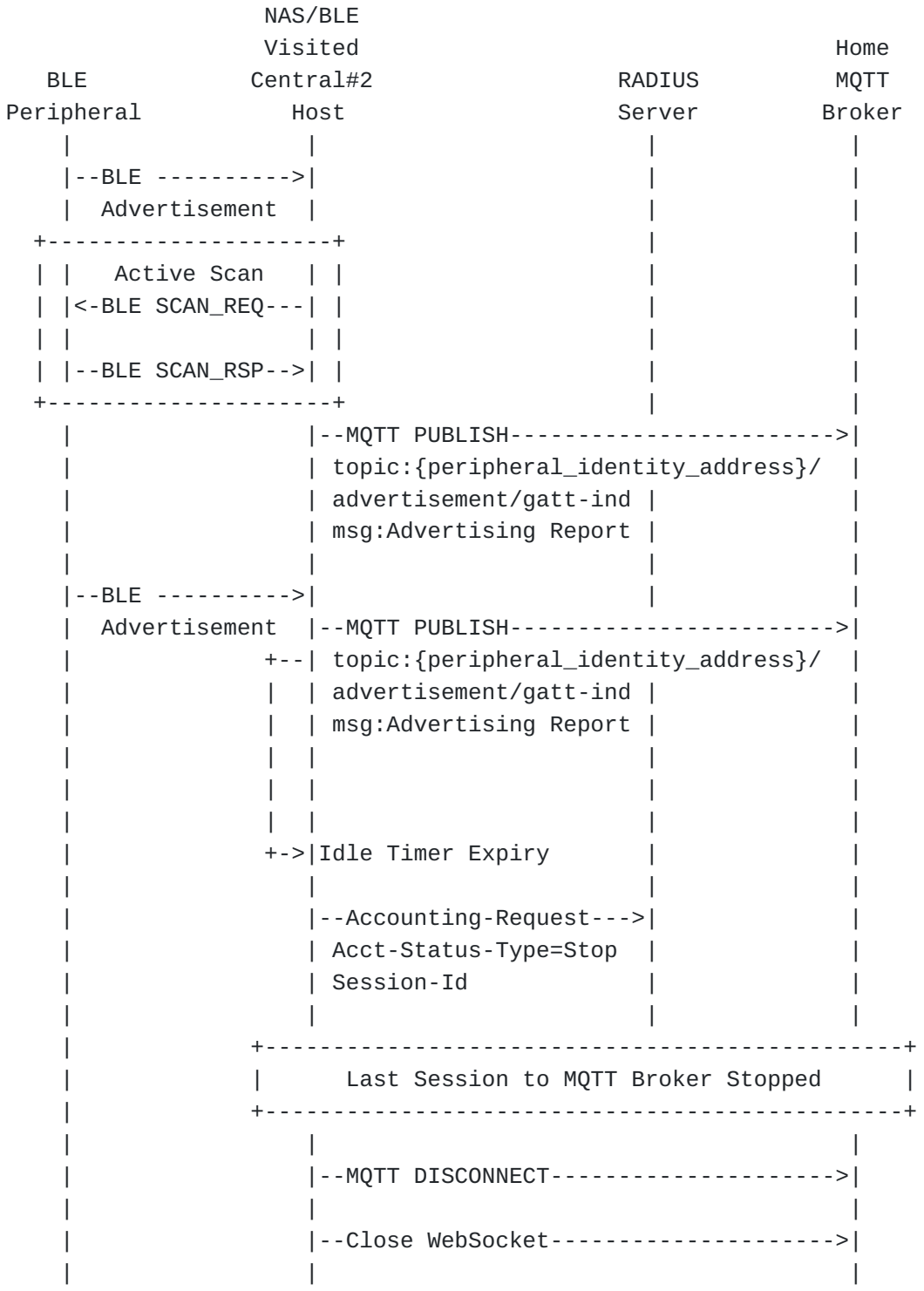

Figure 8: MQTT Exchange for Non-Connectable BLE Peripherals

A.4. Initial MQTT Exchange for Connectable BLE Peripherals

If the BLE Peripheral indicates in its scan that it is connectable, the NAS/BLE Visited Host is responsible for publishing the received advertisements received from the authenticated BLE Peripheral and to

subscribing to the GATT requests published for the BLE Peripheral's Identity Address.


NAS/BLE
Visited
Central#2
Host
Home
MQTT
Broker
BLE
Peripheral
--BLE----------->
Advertisement
---MQTT PUBLISH----------->
topic:{peripheral_identity_address}/
advertisement/gatt-ind
msg:Advertising Report
GATT Subscription
---MQTT SUBSCRIBE---------->
topic:{peripheral_identity_address}/
+/gatt-req
topic:{peripheral_identity_address}/
+/gatt-ind-res
GATT Connection and Service Discovery
<--MQTT PUBLISH----------
topic:{peripheral_identity_address}/
connect/gatt-req
response topic:
{peripheral_identity_address}/
connect/gatt-res
correlation data:{binary_data}
msg:
<-BLE PDU------->
Exchange
---MQTT PUBLISH----------->
topic:{peripheral_identity_address}/
connect/gatt-res
correlation data:{binary data}
msg: connect-id or error
<--MQTT PUBLISH----------
topic:{peripheral_identity_address}/
service-discovery/gatt-req
response topic:
{peripheral_identity_address}/
service-discovery/gatt-res
correlation data:{binary_data}
msg: connect-id, optional UUID

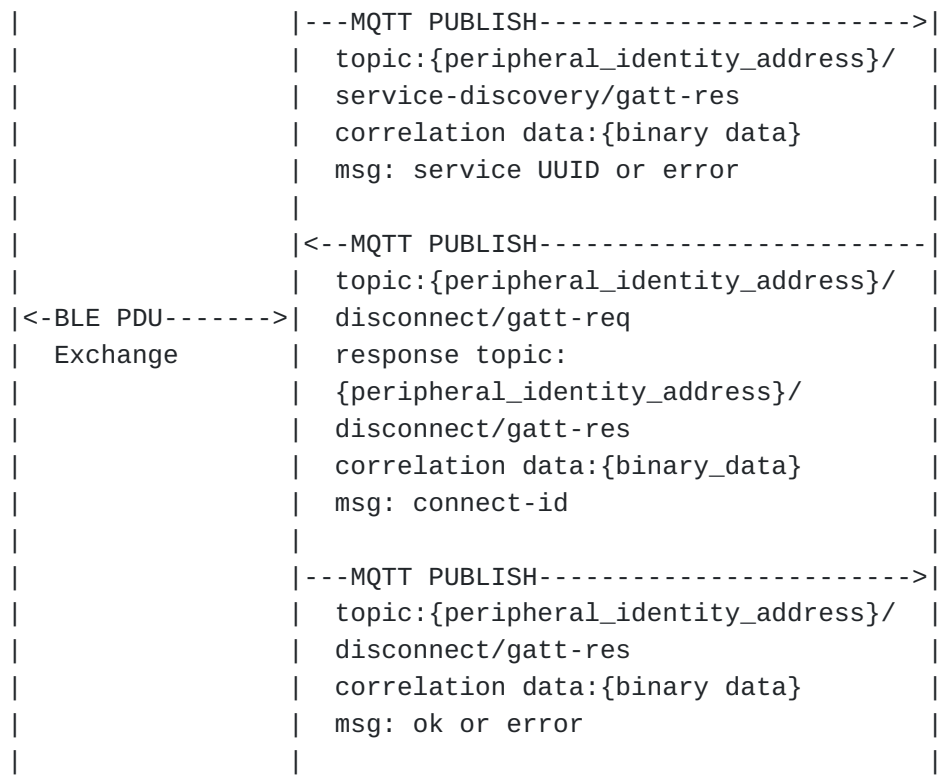
|---MQTT PUBLISH----------->|
| topic:{peripheral_identity_address}/ |
| service-discovery/gatt-res |
| correlation data:{binary data} |
| msg: service UUID or error |
|<--MQTT PUBLISH------------|
| topic:{peripheral_identity_address}/ |
|<-BLE PDU------->| disconnect/gatt-req |
| Exchange | response topic: |
| {peripheral_identity_address}/ |
| disconnect/gatt-res |
| correlation data:{binary_data} |
| msg: connect-id |
|---MQTT PUBLISH----------->|
| topic:{peripheral_identity_address}/ |
| disconnect/gatt-res |
| correlation data:{binary data} |
| msg: ok or error |

Figure 9: MQTT Exchange for GATT Service Discovery

A.5. MQTT Exchange for Reading a GATT Attribute

If the BLE Peripheral is connectable, a Bluetooth Application can read GATT attributes.

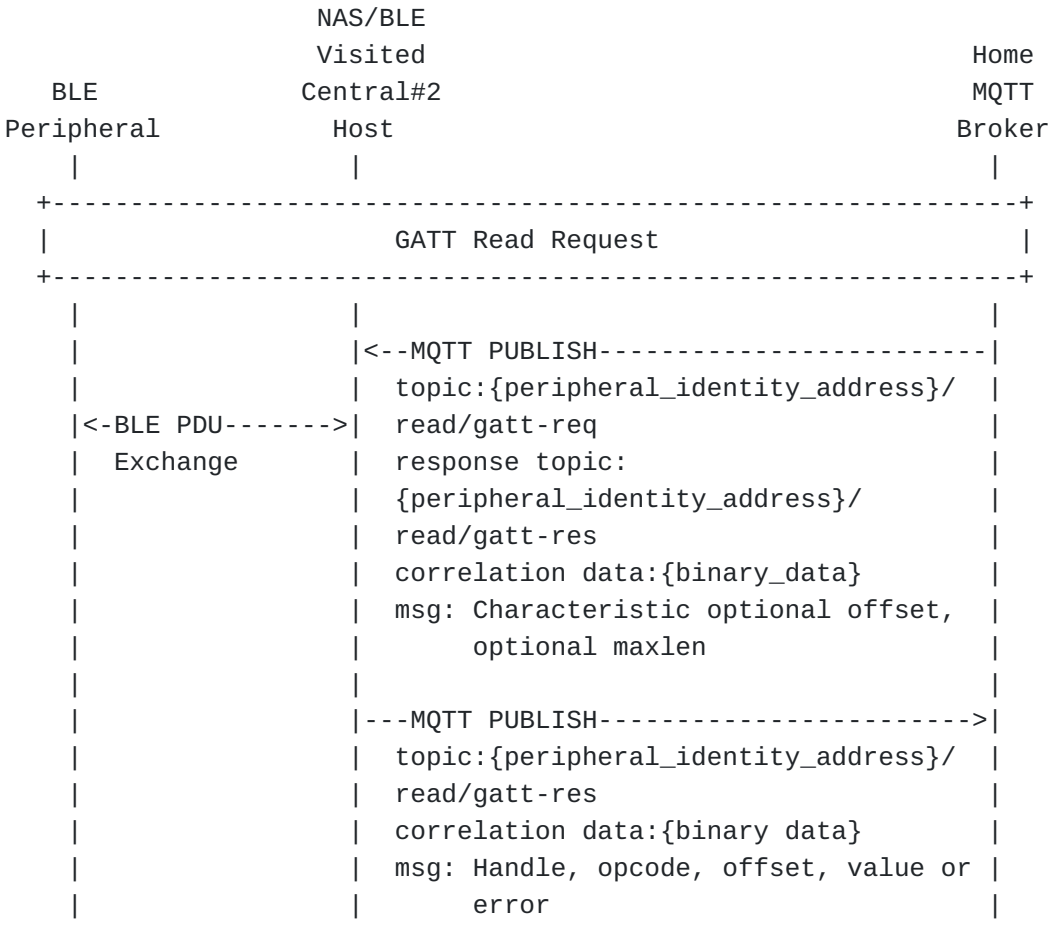

Figure 10: MQTT Exchange for GATT Read Attribute

A.6. MQTT Exchange for Writing a GATT Attribute

If the BLE Peripheral is connectable, a Bluetooth Application can write GATT attributes.

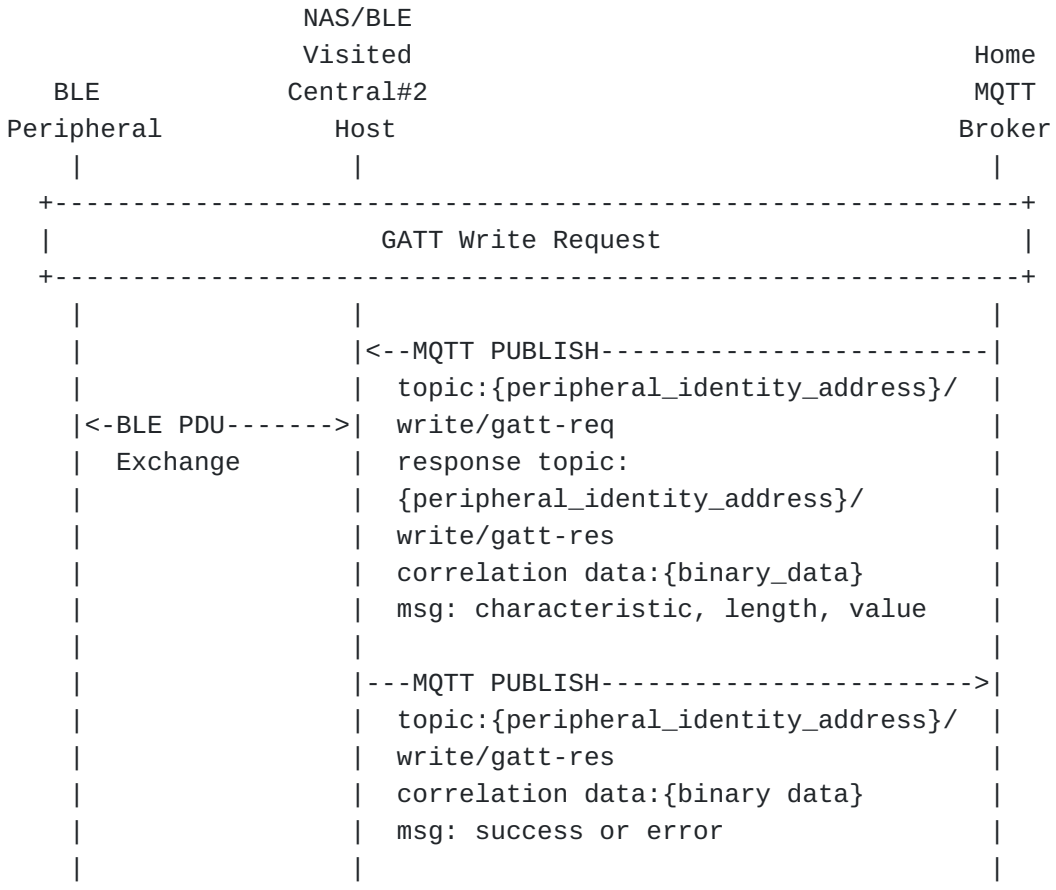

Figure 11: MQTT Exchange for GATT Write Attribute

A.7. MQTT Exchange for BLE Peripheral initiated Notifications

A Bluetooth Application can subscribe to receive Bluetooth notifications sent by the BLE Peripheral.

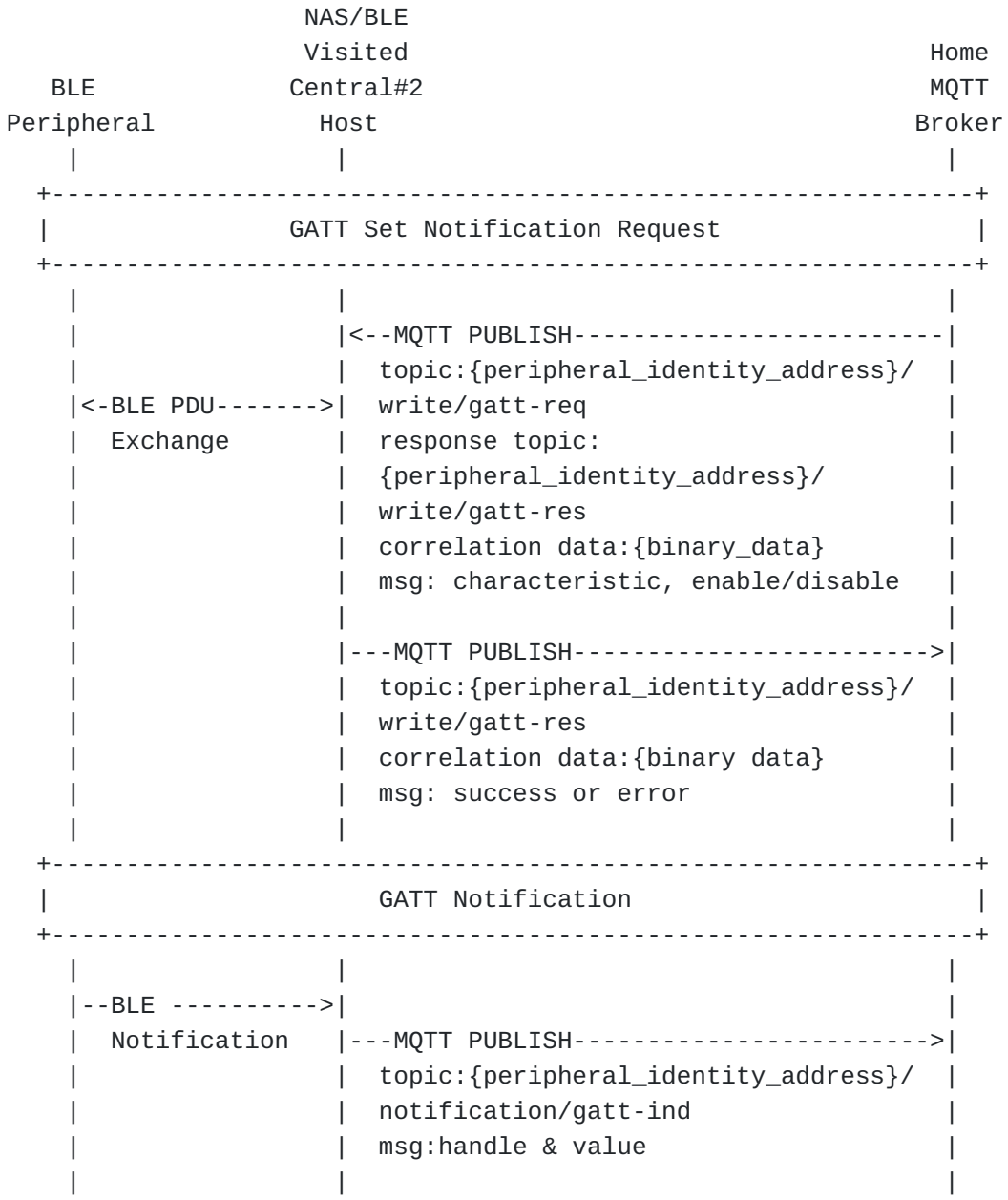

Figure 12: MQTT Exchange for BLE Peripheral Notifications

A.8. MQTT Exchange for BLE Peripheral initiated Indications

A Bluetooth Application can subscribe to receive Bluetooth indications sent by the BLE Peripheral.

Figure 13: MQTT Exchange for BLE Peripheral Indications

A.9. MQTT Exchange for dealing with NAS Mobility


NAS/BLE Visited Central#2 Host
NAS/BLE Visited Central#3 Host
Home MQTT Broker
BLE Peripheral
Initial Authentication With Central#2
--MQTT SUBSCRIBE ---------->
topic:{periperal_identity_address}/
+/gatt-req
NAS Mobility to Central#3 without MQTT unsubscription
--MQTT SUBSCRIBE---------->
topic:
{peripheral_identity_address}/
+/gatt-req
Example GATT Connection Request with NAS Mobility
<-MQTT PUBLISH----------
topic:{peripheral_identity_address}/
connect/gatt-req
response topic:
{peripheral_identity_address}/
connect/gatt-res
correlation data:{binary_data}
msg:
<--MQTT PUBLISH----------
topic:
{peripheral_identity_address}/
connect/gatt-req
response topic:
{peripheral_identity_address}/
connect/gatt-res
correlation data:{binary_data}
msg:
---MQTT PUBLISH---------->
topic:
{peripheral_identity_address}/
connect/gatt-res
<-BLE----
PDU Exchange
Central#2

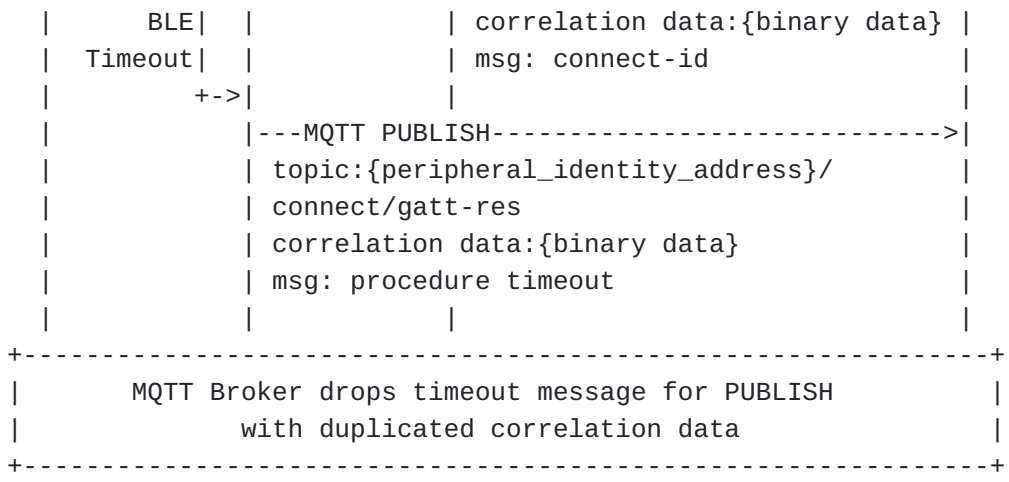
BLE|
Timeout|
+->|
correlation data:{binary data}
msg: connect-id
---MQTT PUBLISH---------->|
topic:{peripheral_identity_address}/
connect/gatt-res
correlation data:{binary data}
msg: procedure timeout
MQTT Broker drops timeout message for PUBLISH
with duplicated correlation data

Figure 14: MQTT Exchange for Inter-NAS Mobility without MQTT Unsubscription

A.10. MQTT Exchange for ending a session for a connected BLE Peripheral

On idle-timeout the NAS/BLE Visited Host MUST un-subscribe from any subscribed to topics and send an Accounting-Request message with Acct-Status-Type set to STOP and Acct-Terminate-Cause set to Lost Carrier (2).

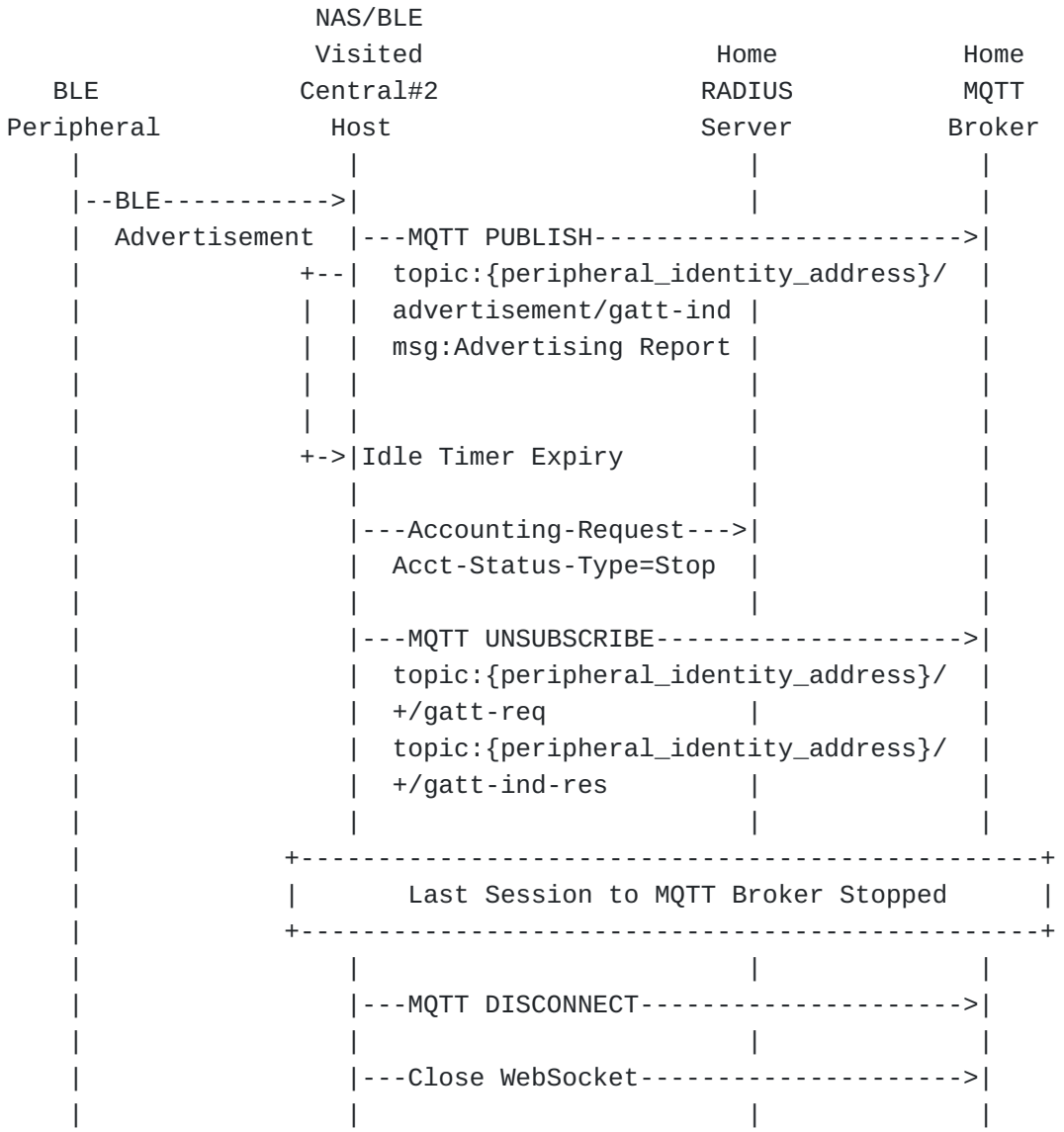

Figure 15: MQTT Exchange when disconnecting from a connected BLE Peripheral

Appendix B. History of Changes

Note: This appendix will be deleted in the final version of the document.

From version 00 -> 01:

* switched from User-Password to new Hashed-Password attribute using SHA256

* switched to TLV-encoding of BLE-Keying-Material

* re-ordered MQTT topic definitions

* removed redundant attribute sections

Acknowledgements

Thanks to Oleg Pekar and Eric Vyncke for their review comments.

Authors' Addresses

Mark Grayson
Cisco Systems
10 New Square Park
Feltham
TW14 8HA
United Kingdom

Email: mgrayson@cisco.com

Eliot Lear
Cisco Systems
Glatt-com
CH- CH-8301 Glattzentrum, Zurich
Switzerland

Email: elear@cisco.com