Cookware Profile

Bluetooth® Profile Specification

- **Revision:** v1.0
- **Revision Date:** 2025-11-03
- **Prepared By:** Automation Working Group

Abstract:

This Bluetooth® Profile enables cooking appliances and smart devices to connect and interact with a cookware device such as a temperature probe, a pot, or a pan to automate and optimize the cooking process.

Version History

Version Number	Date (yyyy-mm-dd)	Comments
v1.0	2025-11-03	Adopted by the Bluetooth SIG Board of Directors.

Acknowledgments

Name	Company
Victor Zhodzishsky	Infineon Technologies AG
Jordi Alvarez Raventos	E.G.O. Elektro-Gerätebau GmbH
Peter Favrholdt	Ztove ApS
Eduardo Velez Pellicer	Robert Bosch GmbH
Holger Henke	Cuciniale GmbH

Contents

1 Introduction

The Cookware Profile (CWP) is a part of the Sensor-Assisted Cooking System which supports use cases in which communication links exist between a smart device, a kitchen appliance (such as an oven or a cooktop), and a smart Cookware Device (CWD) such as a pot, a pan, or a cooking temperature probe. This system can improve the consistency of cooking, reduce power consumption, and improve the user experience during cooking by automating the process.

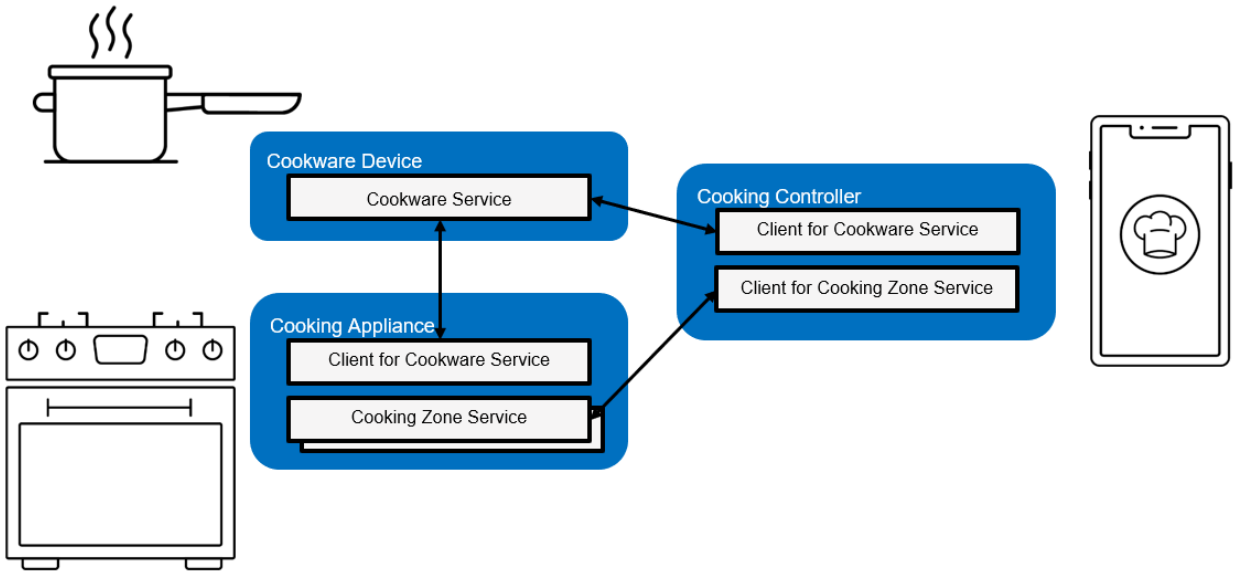

Figure 1.1: Sensor-Assisted Cooking System

This CWP defines the communications between a CWD and a Client of the Cookware Service (CWS). A Cookware Client (CWC) can be either a Cooking Controller or a Cooking Appliance. The CWP allows two main use cases:

- The Cookware Client executes the control loop (i.e., the Cookware Client collects sensor data, such as temperature readings) from the CWD and adjusts the cooking condition (e.g., the power) to be applied to the CWD.
- The Cookware Client sends the recipe to the CWD. The CWD executes the control loop and instructs the Cookware Client to change the cooking conditions according to the recipe parameters.

1.1 Language

1.1.1 Language conventions

In the development of a specification, the Bluetooth SIG has established the following conventions for use of the terms *“shall”*, *“mandatory”*, *“shall not”*, *“should”*, *“should not”*, *“may”*, *“optional”*, *“must”*, and *“can”*. In this Bluetooth specification, the terms in Table 1.1 have the specific meanings given in that table, irrespective of other meanings that exist.

Term	Definition
shall *or* mandatory	—used to express what is required by the specification and is to be implemented exactly as written without deviation
shall not	—used to express what is forbidden by the specification
should *or* may *or* optional	—not mandatory. Used to express either: 1. what is recommended by the specification without forbidding anything (“should”) 2. what is permissible within the limits of the specification (“may” or “optional”)
should not	—used to indicate that something is discouraged but not forbidden by the specification
may	—used to indicate something that is permissible within the limits of the specification
must	—used to indicate either: 1. an indisputable statement of fact that is always true regardless of the circumstances 2. an implication or natural consequence if a separately-stated requirement is followed
can	—used to express a statement of possibility or capability

Table 1.1: Language conventions terms and definitions

Where more than one item is permitted but not required, the choices to include or support those items are independent from one another unless the specification explicitly states otherwise. Each item that is implemented shall be implemented exactly as written without deviation.

1.1.1.1 Implementation alternatives

When specification content indicates that there are multiple alternatives to satisfy specification requirements, if one alternative is explained or illustrated in an example it is not intended to limit other alternatives that the specification requirements permit.

1.1.1.2 Discrepancies

It is the goal of Bluetooth SIG that specifications are clear, unambiguous, and do not contain discrepancies. However, members can report any perceived discrepancy by filing an erratum and can request a test case waiver as appropriate.

1.1.2 Reserved for Future Use

Where a field in a packet, Protocol Data Unit (PDU), or other data structure is described as "Reserved for Future Use" (irrespective of whether in uppercase or lowercase), the device creating the structure shall set its value to zero unless otherwise specified. Any device receiving or interpreting the structure shall ignore that field; in particular, it shall not reject the structure because of the value of the field.

Where a field, parameter, or other variable object can take a range of values, and some values are described as "Reserved for Future Use," a device sending the object shall not set the object to those values. A device receiving an object with such a value should reject it, and any data structure containing it, as being erroneous; however, this does not apply in a context where the object is described as being ignored or it is specified to ignore unrecognized values.

When a field value is a bit field, unassigned bits can be marked as Reserved for Future Use and shall be set to 0. Implementations that receive a message that contains a Reserved for Future Use bit that is set to 1 shall process the message as if that bit was set to 0, except where specified otherwise.

The acronym RFU is equivalent to Reserved for Future Use.

1.1.3 Prohibited

When a field value is an enumeration, unassigned values can be marked as “Prohibited.” These values shall never be used by an implementation, and any message received that includes a Prohibited value shall be ignored and shall not be processed and shall not be responded to.

Where a field, parameter, or other variable object can take a range of values, and some values are described as “Prohibited,” devices shall not set the object to any of those Prohibited values. A device receiving an object with such a value should reject it, and any data structure containing it, as being erroneous.

“Prohibited” is never abbreviated.

1.2 Requirements in tables

Requirements in this specification are defined as "Mandatory" (M), "Optional" (O), "Excluded" (E), “Not Applicable” (N/A), or "Conditional" (C.n). Conditional statements (C.n) are listed directly after the table in which they appear.

- "M” for mandatory. See Table 1.1 Language conventions terms and definitions.
- "O” for optional. See Table 1.1 Language conventions terms and definitions.
- “E” for excluded. “Excluded” means not permitted in this context; cannot be supported or included for this purpose. The item can still be supported or included if allowed for some other purpose (e.g., a feature can be mandatory for one role and excluded for another; a device that supports both roles must support this feature).
- “C.#” for conditional. “Conditional” means that an item is required, optional, or prohibited based on whether one or more other items are supported or included (# represents any number). Within the definition of the condition, if those other items mean that “not permitted” applies, it has the same meaning as “E”.

1.2.1 Table requirements for unused cells

An unused cell is a table cell without a value or content, which is indicated with either the word “none” (without quotation marks) or a hyphen (i.e., a “minus” sign).

1.3 Conformance

Each capability of this specification shall be supported in the specified manner. This specification may provide options for design flexibility, because, for example, some products do not implement every portion of the specification. For each implementation option that is supported, it shall be supported as specified.

1.4 Terminology

Table 1.2 lists terms that are used in CWP.

Term	Definition
Associated Cooking Zone	A Cooking Zone is considered Associated with a Cookware Device (CWD) when the Cooking Zone can deliver power to the CWD. For example, when a pot is placed on an induction cooktop or in an oven.
Associated Cookware Device	A CWD is considered Associated with a Cooking Zone when the CWD is placed such that the Cooking Zone can deliver power to the CWD.
Control Loop	A procedure that calculates the necessary cooking conditions, such as power level, based on the target cooking conditions (e.g., the desired temperature) and the measured cooking conditions. The Control Loop can be executed on a Cooking Controller, a Cooking Appliance, or a CWD.
Cooking Appliance	A device that can emit power to change the cooking conditions for the CWD. In this specification, the term Cooking Appliance mostly applies to traditional or induction cooktops, but it may also be used with gas cooktops, ovens, grills, refrigerators, or other heating or cooling appliances.
Cooking Controller	A device such as a smartphone, a tablet, a wearable device, or a dedicated control panel that can observe and/or modify the Cooking Appliance behavior.
Cooking Zone	A zone of the Cooking Appliance that provides heat or cold to a CWD. This can be, for example, a burner of the cooktop or a chamber of the oven.
Cookware Device (CWD)	A device such as a pot or pan, a temperature probe, or another external sensor that may be used to assist a cooking process that uses an oven, cooktop, or other food preparation device.
Recipe Parameters	In the context of the Sensor-Assisted Cooking System, the Recipe Parameters is a set of cooking parameters, including target temperature, pressure, and humidity (i.e., the amount of steam) that should be maintained in a CWD for the duration of the cooking step.

Table 1.2: Terminology

2 Configuration

2.1 Roles

CWP defines two roles: the Cookware Device (CWD) and the Cookware Client (CWC). A device such as a smart pot or a temperature probe can serve as a CWD. A Cooking Controller like a smartphone, or a kitchen appliance like an oven or a cooktop can serve as a CWC.

- CWD shall be a GATT Server.
- CWC shall be a GATT Client.

There are two major scenarios supported by CWP. In the first scenario, the CWC executes the Control Loop. In that scenario, the CWC collects sensor data (e.g., temperature measurements) from the CWD and adjusts cooking conditions (e.g., power level) of the Cooking Zone to satisfy the Recipe Parameters (see Section 4.4.1).

In the second scenario, the CWD knows the Recipe Parameters. The CWD executes the Control Loop by telling the CWC how to change the cooking conditions based on the internal sensor measurements (see Section 4.4.2).

2.1.1 Profile role support requirements

Devices that implement this Profile shall implement at least one profile role as specified in Table 2.1.

Profile role	Requirement	Description (optional)
CWD	C.1	A cookware device, such as a pot or a temperature probe
CWC	C.1	A device, such as a smartphone or a cooking appliance, that can communicate with a cookware device to support food preparation

*Table 2.1: Role **requirements** for devices implementing CWP*

C.1: Mandatory to support at least one role

2.2 Role and service relationships

A device acting as a CWC discovers and uses services from a CWD as shown in Figure 2.1.

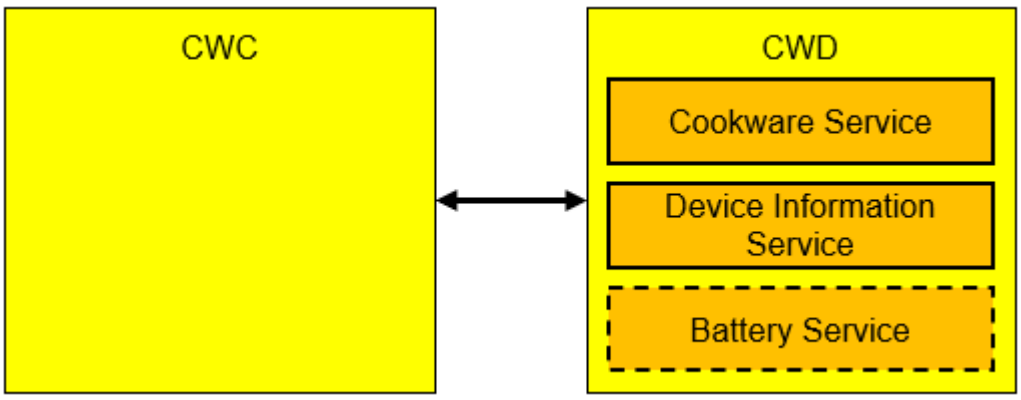

Figure 2.1: Overview of roles and services

2.3 Concurrency limitations and restrictions

There are no concurrency limitations or restrictions imposed by CWP.

2.4 GAP: Topology limitations and/or restrictions defined by GAP

As defined in Table 2.2, the CWD shall implement the Generic Access Profile (GAP) Peripheral role; the CWC shall implement the GAP Central role.

GAP role dependency	Support in CWD	Support in CWC
GAP Peripheral role	M	O
GAP Central role	O	M

Table 2.2: GAP role dependencies

2.5 Core Configuration dependencies

Enabling Bluetooth® wireless technology end-to-end in an implementation of CWP requires implementing a Core Configuration that supports either the LE or the BR/EDR transport, or both.

2.5.1 Core feature inter-layer dependencies

Devices that implement this profile over LE transport shall support the Link Layer (LL) features specified in Table 2.3.

LL	CWP Role	
	CWD	CWC
LE Encryption (see Volume 6, Part B, Section 4.6.1 in the Bluetooth Core Specification [1])	M	M
LL Privacy (see Volume 6, Part B, Section 4.6.7 in [1])	M	M
LE Encrypted Advertising Data (see Volume 3, Part C, Section 10.10 in [1])	M	M

Table 2.3: Core feature inter-layer dependencies

2.6 Dependencies on other specifications external to the Core

There are no dependencies on other specifications external to the Bluetooth Core Specification [1].

3 Cookware Device role requirements

A CWD shall instantiate one and only one instance of the Cookware Service (CWS) [2]. CWS shall be instantiated as a «Primary Service».

A CWD shall instantiate a single instance of the Device Information Service (DIS) [3].

A battery-operated CWD should instantiate the Battery Service (BAS) [4].

Service/role	Support in CWD	Section for additional requirements
Cookware Service	M	Section 3.1
Device Information Service	M	Section 3.2
Battery Service	O	Section 3.3

Table 3.1: Requirements for CWD role

3.1 Incremental Cookware Service requirements

3.1.1 Additional requirements for Low Energy transport

This section describes additional CWD requirements beyond those defined in CWS [2].

The CWD shall not enter GAP Discoverable, GAP Non-Connectable, or GAP Connectable mode (i.e., shall not advertise) while not in use.

The “in use” condition for a CWD means that either of two things have occurred:

- The CWD has detected heat.
- The CWD has received a signal from an embedded accelerometer that the CWD is being moved.

The CWD shall enter GAP Limited Discoverable mode when instructed by a user for initial connection with a CWC (e.g., when a user pushes a “Connect” button to perform pairing).

While in GAP Limited Discoverable mode, the CWD should include the following AD types in the advertisement packets:

- Service UUID AD type (see Section 3.1.1.1)
- Local Name AD type (see Section 3.1.1.2)
- Appearance AD type (see Section 3.1.1.3)

The CWD shall enter GAP Connectable mode if all three of the following conditions are met:

- The CWD has bonded clients.
- The CWD does not have connections established.
- The CWD detects an “in use” condition (e.g., when the CWD detects heat or when the CWD receives a signal from an embedded accelerometer that the CWD is being moved).

The CWD shall stay in GAP Connectable mode while the “in use” condition persists.

Even if the CWD has connection(s) established, it should continue advertising in GAP Connectable mode or in GAP Non-Connectable mode. Continuing to advertise in GAP Connectable mode allows other clients to monitor the cooking process or to establish connection with the CWD (see Section 5). Continuing to advertise in GAP Non-Connectable mode allows clients to monitor the cooking process without establishing a connection with the CWD.

While in either GAP Connectable mode or in GAP Non-Connectable mode, the CWD should include the following AD type in the advertisement packets:

- Service Data AD type (see Section 3.1.1.4)

3.1.1.1 Service UUID AD type

The Service UUID AD type field of the Advertising Data (AD) should include the CWS UUID defined in [5]. Including the CWS UUID enhances the user experience because the advertiser can be identified as a CWD before initiating a connection.

3.1.1.2 Local Name AD type

For an enhanced user experience, a CWD should include the Local Name AD type in its Advertising Data or Scan Response Data. The Local Name shall contain either the complete or shortened value of the Device Name characteristic (as defined in Volume 3, Part C, Section 12.1 of the Bluetooth Core Specification [1]). For privacy reasons, a CWD with the Privacy feature enabled should not include the Local Name AD Type in the advertisements when the CWD is not in GAP Discoverable mode.

3.1.1.3 Appearance AD type

For an enhanced user experience, a CWD should include the value of the Appearance characteristic defined in Volume 3, Part C, Section 12.2 [1]) in its Advertising Data or Scan Response Data.

3.1.1.4 Service Data AD type

The Service Data AD type is encrypted and is included in the advertising packets as Encrypted Data AD type. The advertisement PDU contains the Service Data AD type. Table 3.2 shows the advertisement PDU format containing the Service Data AD type.

Field	Data Type	Size (in Octets)	Description
Length	uint8	1	Length of the Encrypted Data field
Encrypted Data AD type (see Section 1.23 of CSS [6])	uint8	1	AD type: «Encrypted Data»
Randomizer	uint40	5	Randomizer

Field		Data Type	Size (in Octets)	Description
Payload	Length	uint8	1	Length of the Service Data field
	Service Data AD type (see Section 1.11 of CSS [6])	uint8	1	AD type: «Service Data»
	Service Data UUID	uint16	2	«CWS UUID»
	Cooking Step Status	struct	4	Current value of Cooking Step Status characteristic as defined in CWS [2]
	Cookware Sensor Data	variable	variable	Data from the cookware sensor(s)
MIC		uint32	4	Message Authentication Code (a.k.a., Message Integrity Check)

Table 3.2: Advertising packet format

The Randomizer, encrypted Payload, and the MIC fields are parts of the Encrypted Data as defined in Section 1.23 of the Supplement to the Bluetooth Core Specification [6].

To support encryption, the CWD shall include the Encrypted Data Key Material characteristic as defined in Volume 3, Part C, Section 12.6 [1]. The Cooking Step Status field allows CWC(s) to monitor the status of the cooking step being performed without the CWC(s) needing to establish a connection. The Cooking Step Status field contains the amount of time remaining until the completion of the current cooking step as well as information if this is the last step in the recipe and if the user action after the completion of the cooking step is required. The value of the field shall match the value of the CWS Cooking Step Status characteristic.

The Cookware Sensor Data field allows the CWC to monitor the state of the CWD sensors. If the Cookware Sensor Aggregate characteristic is not present in the CWS (i.e., if the CWD has a single Cookware Sensor Data characteristic), the format and the value of the Cookware Sensor Data field shall match the format and the value of the CWS Cookware Sensor Data characteristic.

If Cookware Sensor Aggregate characteristic is present, the format and the value of the field shall match the value of the CWS Cookware Sensor Aggregate characteristic. If the Cookware Sensor Aggregate characteristic does not fit in the advertising data, the CWD shall truncate the value so that the full advertising data does not exceed 31 octets.

3.1.2 Encrypted Data Key Material characteristic

If CWD supports sending Connectable or Non-Connectable advertising packets with the Encrypted Data AD type (which includes Service Data AD type), the GAP service of the CWD shall include the Encrypted Data Key Material characteristic as defined in Volume 3, Part C, Section 12.6 of the Bluetooth Core Specification [1].

3.1.3 Writable GAP Device Name characteristic

The CWD should support the Write property for the Device Name characteristic to allow a user to update a CWD device name.

3.2 Incremental Device Information Service requirements

Table 3.3 states the requirements for the instance of the DIS on a CWD in addition to the requirements specified in DIS [3].

Characteristic	Requirement	Mandatory Properties	Security Permission
Manufacturer Name String	M	Read	C.1
Model Number String	M	Read	C.1
Serial Number String	M	Read	C.1

Table 3.3: Additional requirements for DIS

C.1: Encryption is Mandatory if the Privacy feature is enabled; otherwise Optional.

3.3 Incremental Battery Service requirements

CWP sets no additional requirements for the BAS instance [4].

4 Cookware Client role requirements

A CWC is a device that establishes connection to a CWD and acts as a client for CWS [2]. A Cooking Appliance or a Cooking Controller are examples of CWCs.

This section describes the CWC requirements.

Table 4.1 lists the service requirements for a CWC. The services supported by the CWC shall be discovered by the CWC (see Section 4.2).

Service	Support in CWC	Section
GATT service discovery for Cookware Service	M	Section 4.4
GATT service discovery for Device Information Service	O	Section 4.5
GATT service discovery for Battery Service	O	Section 4.6
GATT service discovery for GAP	M	Section 4.7

Table 4.1: CWC role service support requirements

Table 4.2 lists characteristic and descriptor requirements for a CWC. The characteristics and descriptors supported by the CWC shall be discovered by the CWC (see Section 4.3). If a characteristic is discovered that can be notified or indicated, the CWC shall also discover the associated Client Characteristic Configuration descriptor.

Service	Characteristic / Descriptor Requirements	Support in CWC	Additional Requirements
CWS	Cookware Description characteristic	M	Section 4.4.1.1
	Recipe Parameters characteristic	C.1	Section 4.4.2.1
	Recipe Control characteristic	C.1	Section 4.4.2.2
	Cooking Step Status characteristic	C.1	Section 4.4.2.3
	Cooking Zone Capabilities characteristic	C.1	Section 4.4.2.4
	Cooking Zone Desired Cooking Conditions characteristic	C.1	Section 4.4.2.5
	Cooking Zone Actual Cooking Conditions characteristic	C.1	Section 4.4.2.6
	Cookware Sensor Data characteristic	M	Section 4.4.1.2
	Cooking Sensor Info descriptor	M	Section 4.4.1.2.1
	Cooking Trigger Settings descriptor	O	Section 4.4.1.2.2
	Valid Range descriptor	O	Section 4.4.1.2.3
	Cookware Sensor Aggregate characteristic	O	Section 4.4.1.3

Service	Characteristic / Descriptor Requirements	Support in CWC	Additional Requirements
DIS	Manufacturer Name String characteristic	M	Section 4.5
	Model Number String characteristic	M	Section 4.5
	Serial Number String characteristic	M	Section 4.5
BAS	Battery Level characteristic	O	Section 4.6
GAP	Encrypted Data Key Material characteristic	C.2	Section 4.7

Table 4.2: CWC role characteristic and descriptor requirements

C.1: Mandatory if CWC supports execution of the Control Loop by the CWD; otherwise Optional.

C.2: Mandatory if CWC supports monitoring of the cooking step execution by listening to the CWD advertisements; otherwise Optional.

4.1 Summary of GATT sub-procedures for a Cookware Client

Requirements in this section represent a minimum set of requirements for a CWC. Other GATT sub-procedures may be used if supported by both a CWC and a CWD.

Table 4.3 summarizes the GATT sub-procedure requirements beyond those required by all GATT Clients defined in Table 4.1 in Volume 3, Part G of the Bluetooth Core Specification [1].

GATT Sub-Procedure	Requirements
Discover All Primary Services	C.1
Discover Primary Service by Service UUID	C.1
Discover All Characteristics of a Service	C.2
Discover Characteristics by UUID	C.2
Discover All Characteristic Descriptors	M
Read Characteristic Descriptor	M
Write Characteristic Descriptor	M
Read Characteristic Value	M
Write Characteristic Value	M
Single Notification	M
Indication	M

Table 4.3: GATT sub-procedure requirements

C.1: Mandatory to support at least one of these Service Discovery sub-procedures when using LE transport
C.2: Mandatory to support at least one of these Characteristic Discovery sub-procedures

4.2 Service discovery

For the CWC to discover services supported by the CWD, the CWC shall use either the GATT Discover All Primary Services sub-procedure or the GATT Discover Primary Service by Service UUID sub-procedure.

The CWC shall discover CWS.

The CWC may discover DIS.

If BAS is exposed by the CWD, the CWC may discover BAS.

The CWC may discover any other primary services and any included services.

4.3 Characteristic and descriptor discovery

The CWC shall use either the GATT Discover All Characteristics of a Service sub-procedure or the GATT Discover Characteristics by UUID sub-procedure to discover the characteristics listed in Table 4.2.

The number of Cookware Sensor Data characteristics discovered by the CWC shall match the number of Cookware Sensor Data characteristics present in CWS.

For each Cookware Sensor Data characteristic discovered, the CWC shall use the GATT Discover All Characteristic Descriptors sub-procedure to discover characteristic descriptors listed in Table 4.2.

The CWC shall discover the Client Characteristic Configuration descriptor of the discovered characteristics that support indications or notifications.

As required by GATT in Volume 3, Part G, Section 3.3.1.3 in [1], a CWC shall ignore any characteristic definition with an unknown Characteristic UUID.

4.4 Cookware Service Client role requirements

CWP supports two cooking procedures depending on which device is selected to execute the Control Loop:

- Cookware Client executes Control Loop (see Section 4.4.1)
- Cookware Device executes Control Loop (see Section 4.4.2)

The CWC may support both procedures. If the CWD does not support execution of the Control Loop, the CWC-executed procedure is used. Otherwise, the CWC decides which procedure is used.

4.4.1 Cookware Client executes Control Loop

When the Cooking Appliance is the CWC that executes the Control Loop, the CWC reads or receives notifications that contain measurements from sensors located in the CWD and adjusts the cooking conditions (such as the power emitted by the Associated Cooking Zone) to achieve cooking conditions specified in the Recipe Parameters.

When a Cooking Controller, such as a smartphone, is the CWC that executes the Control Loop, the Cooking Controller may display sensor data to the user, and the user may adjust the cooking conditions. The Cooking Controller may also be able to adjust the cooking conditions by communicating with the CA, as shown in Figure 1.1.

Figure 4.1 shows an example of a message sequence chart (MSC) for a CWC executing the Control Loop.

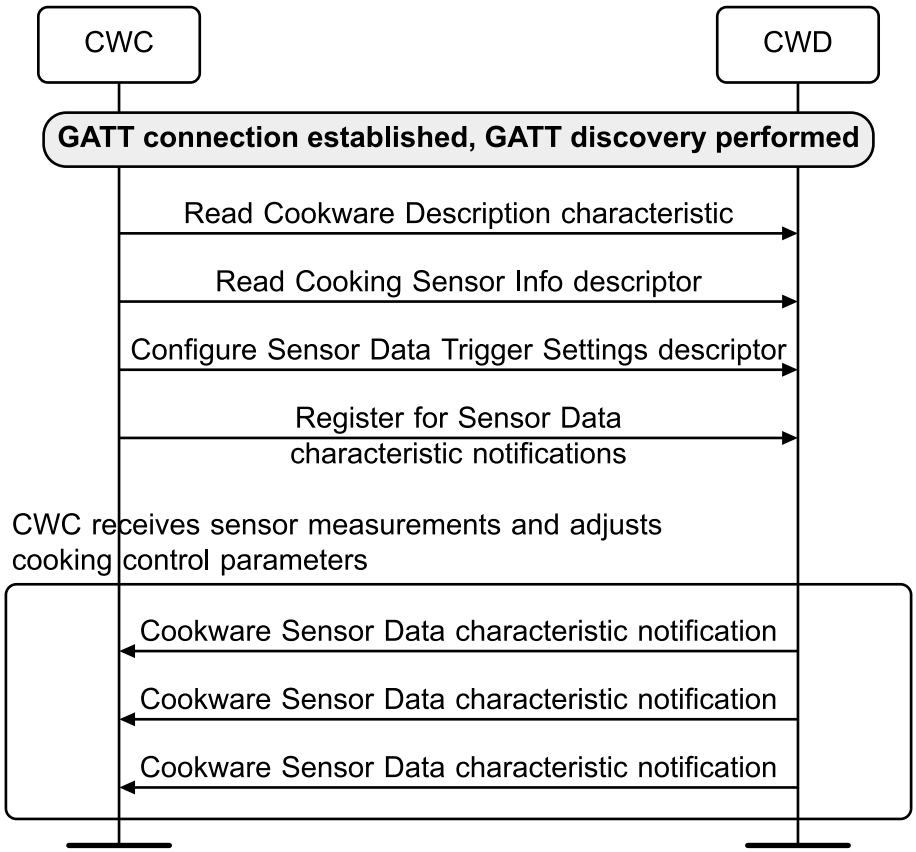

Figure 4.1: CWC executes the Control Loop

4.4.1.1 Cookware Description characteristic

To obtain information about the CWD, the CWC shall read the value of the Cookware Description characteristic. The value obtained by the CWC may be used to execute the Control Loop.

4.4.1.2 Cookware Sensor Data characteristic

The CWC may read the Cookware Sensor Data characteristic to find out the status and values measured by the CWD sensor(s).

The CWC uses Cookware Sensor Data characteristic descriptors (see Sections 4.4.1.2.1, 4.4.1.2.2, and 4.4.1.2.3) to find out additional information about the sensor or to configure sensor behavior.

To receive notifications of the changes to the Cookware Sensor Data characteristic from a CWS that supports these notifications, the CWC shall register for notifications via the Client Characteristic Configuration descriptor. If there is a writable Cooking Trigger Settings descriptor associated with the Cookware Sensor Data characteristic, the CWC may also control the conditions under which the notifications occur by writing to the Cooking Trigger Settings descriptor (see Section 4.4.1.2.2).

The CWC shall be tolerant of CWS exposing Cookware Sensor Data characteristics with UUIDs not recognized by the CWC.

The CWC shall support the CWS exposing multiple Cookware Sensor Data characteristics.

4.4.1.2.1 Cooking Sensor Info descriptor

The CWC shall read the Sensor Info descriptor to find out the type of the sensor, the location, the measurement uncertainty of the sensor, and if present, the offset of the sensor data in the Cookware Sensor Aggregate characteristic.

If the CWD exposes multiple Cookware Sensor Data characteristics with the same UUID (e.g., if multiple Cooking Temperature characteristics are exposed to support a device that includes multiple temperature sensors), the CWC may use the Sensor Location field of the Cooking Sensor Info descriptor to differentiate between Sensor Data characteristics related to different sensors.

4.4.1.2.2 Cooking Trigger Settings descriptor

If the Cooking Trigger Settings descriptor is present, the CWC may read the value of the Cooking Trigger Settings descriptor to identify the condition(s) under which the associated Cookware Sensor Data characteristic value will be notified by the CWD.

If the Cooking Trigger Settings descriptor is writable, the CWC may write to the descriptor to specify the condition(s) under which the associated Cookware Sensor Data characteristic will be notified by the CWD. The CWC shall be tolerant of CWS rejecting the update of the Cooking Trigger Setting descriptor.

To receive periodic notification of the Cookware Sensor Data characteristic, the CWC shall write a non-zero value to the Interval field of the Cooking Trigger Settings descriptor. To disable periodic notifications, the CWC shall write zero to the Interval field of the Cooking Trigger Settings descriptor.

To receive notification when the value of the Cookware Sensor Data characteristic changes by the specified delta value, the CWC shall write a non-zero value to the Delta field of the Cooking Trigger Settings descriptor. To disable notifications based on the changes of the measured value, the CWC shall write zero to the Delta field of the Cooking Trigger Settings descriptor.

4.4.1.2.3 Valid Range descriptor

If the Valid Range descriptor is present, the CWC may read the Valid Range descriptor of the Cookware Sensor Data characteristic to discover the operating range of the corresponding sensor.

4.4.1.3 Cookware Sensor Aggregate characteristic

If the Cookware Sensor Aggregate characteristic is present, the CWC may read the Cookware Sensor Aggregate characteristic to determine the latest measurements from all the CWD sensors at once.

To receive notifications of the Aggregate characteristic, the CWC shall register for notifications via the Client Characteristic Configuration descriptor of the Cookware Sensor Aggregate characteristic.

To control the conditions under which the Cookware Sensor Aggregate characteristic is notified, the CWC shall write to the Cooking Trigger Settings descriptors associated with the individual Cookware Sensor Data characteristics (see Section 4.4.1.2.2). Whenever a condition for at least one of the Cookware Sensor Data characteristic's Cooking Trigger Settings descriptors is satisfied, the Cookware Sensor Aggregate characteristic is notified.

4.4.2 Cookware Device executes Control Loop

As defined in CWS [2], the following characteristics are only present in CWS if the CWD supports execution of the Control Loop:

- Recipe Parameters characteristic
- Recipe Control characteristic
- Cooking Step Status characteristic
- Cooking Zone Capabilities characteristic
- Cooking Zone Desired Cooking Conditions characteristic
- Cooking Zone Actual Cooking Conditions characteristic

While performing service characteristics discovery (see Section 4.3), the CWC confirms if the CWD supports the execution of the Control Loop.

Figure 4.2 shows an example of an MSC for a CWC (such as a Cooking Appliance or a Cooking Controller) delegating the execution of the Control Loop to the CWD.

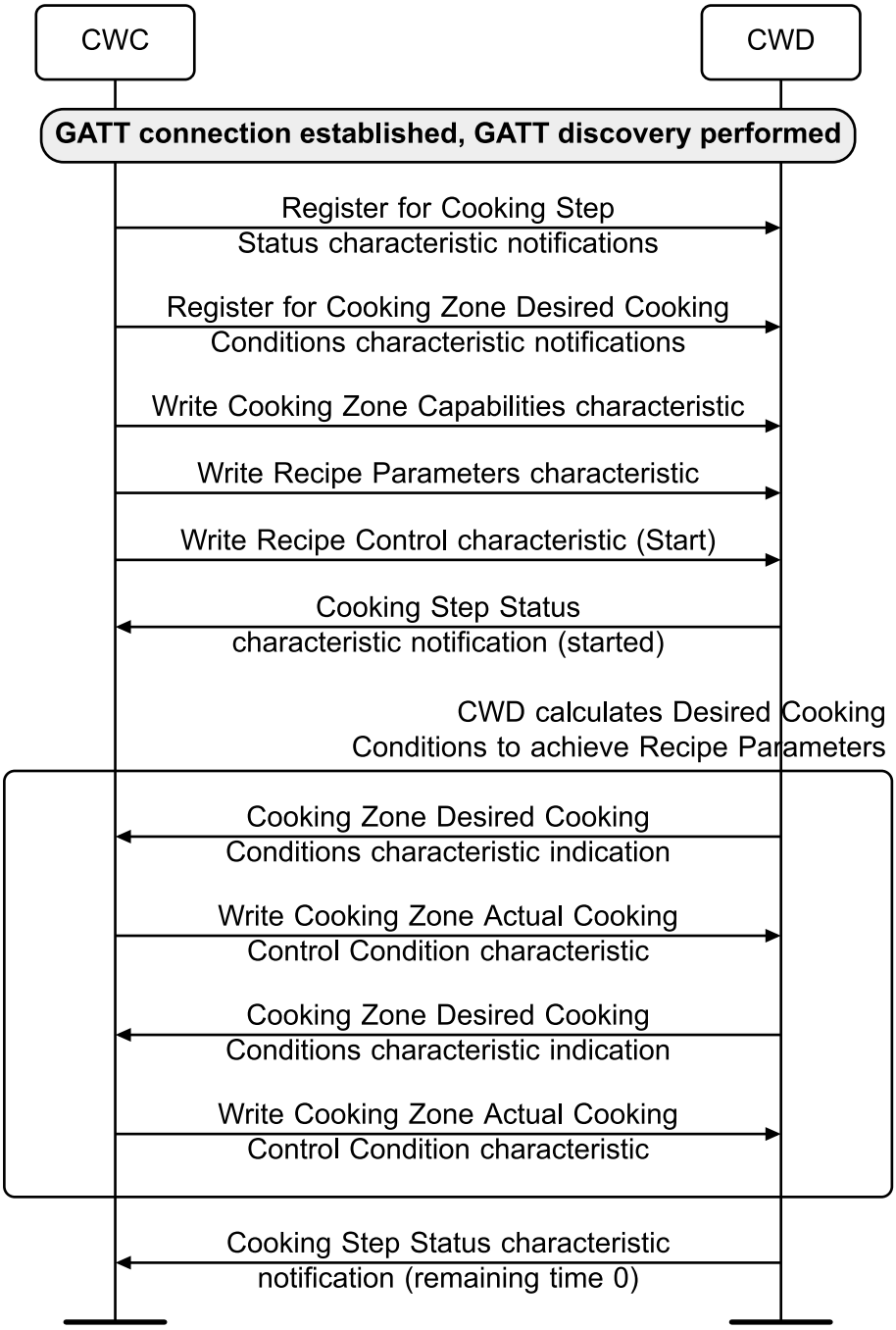

Figure 4.2:The CWC delegates execution of the Control Loop to the CWD

4.4.2.1 Recipe Parameters characteristic

To inform the CWD about the required cooking conditions (e.g., temperature or pressure), the CWC shall write to the Recipe Parameters characteristic.

To receive information about the cooking step stored in the CWD, the CWC shall read the value of the Recipe Parameters characteristic or write a command to the Recipe Control characteristic with the Op Code set to Read (see Section 4.4.2.2).

4.4.2.2 Recipe Control characteristic

To retrieve the value of the Recipe Parameters characteristic of the cooking step stored in the CWS, the CWC may write to the Recipe Control characteristic with the Op Code value set to 0 (Read).

To start execution of the cooking step by the CWD, the CWC shall write to the Recipe Control characteristic with the Op Code value set to 1 (Start).

To stop execution of the cooking step by the CWD, the CWC shall write to the Recipe Control characteristic with the Op Code value set to 2 (Stop). The value of the Recipe Parameters characteristic will be preserved by the CWS, and the CWC may restart the execution of the cooking step by issuing the Start command.

To abort execution of the cooking step and to delete recipe parameters for the cooking step being executed, the CWC shall write to the Recipe Control characteristic with the Op Code value set to 3 (Delete). After the delete, the CWS discards the previous value of the Recipe Parameters characteristic. To start execution of a new cooking step, the CWC must write to the Recipe Parameters characteristic and then to the Recipe Control characteristic indicating Op Code 1 (Start).

4.4.2.3 Cooking Step Status characteristic

To receive a notification when the CWD starts or completes the execution of the cooking step, the CWC shall register with CWS via the Client Characteristic Configuration descriptor of the Cooking Step Status characteristic.

A CWC may read the Cooking Step Status characteristic to find the estimated time until the cooking step that was started by the most recent write to the Recipe Parameters characteristic will be completed.

4.4.2.4 Cooking Zone Capabilities characteristic

When a CWD is Associated with a Cooking Zone (e.g., when a CWD is placed within a Cooking Appliance), the CWC shall write to the Cooking Zone Capabilities characteristic of CWS to make the CWD aware of the conditions (e.g., nominal power, humidity, etc.) that the Cooking Zone can deliver to the CWD.

If the CWC detects that the Cooking Zone capabilities have changed (e.g., when two Cooking Zones have been aggregated), the CWC shall write the new value to the Cooking Zone Capabilities characteristic.

4.4.2.5 Cooking Zone Desired Cooking Conditions characteristic

To receive indications of the Cooking Zone Desired Cooking Conditions characteristic, the CWC shall register for the indications by writing to the Client Characteristic Configuration descriptor of the Cooking Zone Desired Cooking Conditions characteristic.

When a CWD indicates the Cooking Zone Desired Cooking Conditions characteristic, the CWC should adjust the cooking conditions of the Cooking Zone associated with the CWD to the requested levels. For example, when a cooking pot (the CWD) indicates to the cooktop (the CWC) to set the Cooking Zone Desired Cooking Conditions characteristic to 50 percent power, the cooktop (CWC) should adjust the power to 50 percent on the related Cooking Zone (the burner, in this case, where the cooking pot/CWD is located).

4.4.2.6 Cooking Zone Actual Cooking Conditions characteristic

The CWC shall write to the Cooking Zone Actual Cooking Conditions characteristic to notify the CWD about current cooking conditions applied by the CWC in the Cooking Zone where the CWD is placed.

While the CWD is executing the Control Loop, the CWC shall write to the Cooking Zone Actual Cooking Conditions characteristic in response to one of the following cases:

- When the CWD indicates the Cooking Zone Desired Cooking Conditions characteristic
- When the user adjusts conditions manually (e.g., when the user turns off the power applied to the Cooking Zone)

4.5 Device Information Service Client role requirements

The CWC may read the values of the DIS characteristics to identify the CWD manufacturer, model number, serial number, and other properties supported by the CWD.

4.6 Battery Service Client role requirements

The CWC may read the value of the Battery Level characteristic. If the CWD supports the notification of the Battery Level characteristic, the CWC may also configure this characteristic for notifications via the Client Characteristic Configuration descriptor of the Battery Level characteristic.

The CWC may read other BAS characteristics supported by the CWD. For example, this will allow the CWC to inform the user if the battery level is critically low (Battery Critical Status characteristic) or show the time remaining until the battery is fully discharged (Battery Time Status characteristic).

4.7 GAP Client role requirements

To be able to decode advertising data, the CWC shall read the value of the Encrypted Data Key Material characteristic.

4.8 Cooking step execution monitoring

Some CWDs include the cooking step execution status in the Service Data AD Type of the Connectable or Non-Connectable advertising packets. This allows CWCs to monitor execution of the current cooking step without establishing connection to the CWD. The data in the advertising packets is encrypted as described in Section 3.1.1.4.

Before the CWC is able to monitor cooking step execution status, the CWC shall first establish authenticated and authorized connection with the CWD and read the value of the Encrypted Data Key Material characteristic as defined in the Volume 3, Part C, Section 12.6 of the Bluetooth Core Specification [1]. The CWC shall use Key Material value to decrypt and authenticate the Encrypted Data AD Type.

5 Connection establishment procedures

This section describes the connection establishment and connection termination procedures used by each role that go beyond GAP as described in Volume 3, Part C, Section 7 in the Bluetooth Core Specification [1] connection establishment procedures.

5.1 Connection establishment procedures for Low Energy

5.1.1 Peripheral connection establishment

As described in Section 3.1.1, the CWD advertises when instructed by a user or while an “in use” condition is detected. In the first case, the CWD is using connectable advertisements. In the second case, the CWD shall use connectable advertisement if it does not have active connections. The CWD should use connectable advertisements if multiple connections are supported.

5.1.2 Central connection establishment

The CWC should connect when it receives connectable advertisements from a bonded CWD.

5.2 Connection establishment procedures for BR/EDR

There are no GAP inter-layer dependencies for BR/EDR.

6 Security requirements

This section describes the security requirements for each role for the LE and BR/EDR transports.

6.1 CWD role security requirements for Low Energy

LE Security Mode 1 Level 2 or stronger, with LE Secure Connections pairing (Vol. 3, Part H, Section 2.3.5.6 [1]) and 128-bit or longer encryption keys (Vol. 3, Part H, Section 2.3.4 [1]), shall be required for access to all services used by this profile, except for service and characteristic discovery (as allowed by the Bluetooth Core Specification, see Vol. 3, Part G, Section 8.1 [1]).

Legacy pairing methods and key sizes less than 128 bits shall be rejected.

Full Man-in-the-Middle (MITM) protection would not be provided by LE Security Mode 1 Level 2 even with LE Secure Connections pairing, and therefore implementations will be vulnerable to active MITM attacks. To enable protection against active Man-in-the-Middle attacks, LE Security Mode 1 Level 4 or stronger shall be used.

The CWD shall support bonding with at least one CWC. The CWD should support bonding with multiple CWCs.

All characteristics exposed by DIS for use by CWP should be set to the same security mode and level as the characteristics in CWS.

All characteristics exposed by BAS for use by CWP should be set to the same security mode and level as the characteristics in CWS.

The Encrypted Data Key Material characteristic exposed by GAP shall be set to the same security mode and level as the characteristics in CWS.

6.2 Privacy

The Privacy feature (Vol. 3, Part C, Section 10.7 [1]) shall be supported and enabled. Resolvable Private Addresses shall be used, and the device shall exchange its Identity Resolving Key during the key distribution phase (Vol. 3, Part H, Section 3.6.1 [1]) of the pairing procedure.

When not in the GAP Discoverable Mode, advertising PDUs (including scan responses) should not contain the device name or any other static data.

If the CWD supports advertising of the cooking step status by sending the Connectable or Non-Connectable advertising packets, the CWD shall use the Encrypted Advertising Data feature as described in Section 3.1.1.4.

The CWD shall include a new Randomizer value in each advertising packet that the CWD transmits.

6.3 CWC role security requirements for Low Energy

This section describes the security requirements for the CWC role for the LE transport.

The CWC shall bond with a CWD before starting any other procedure.

The CWC shall accept any request by a CWD for LE Security Mode 1 and Security Level 2 or higher.

6.4 Security requirements for BR/EDR

This section describes the security requirements for the BR/EDR transport.

BR/EDR Security Mode 4 Level 2 or stronger, with BR/EDR Secure Connections and 128-bit or longer encryption keys, shall be required for access to all services used by this profile, except for service and characteristic discovery (as allowed by the Bluetooth Core Specification, see Vol. 3, Part B, Section 6 [1]).

Legacy pairing methods and key sizes less than 128 bits shall be rejected.

Full Man-in-the-Middle (MITM) protection would not be provided by BR/EDR Security Mode 4 Level 2 even with BR/EDR Secure Connections, and therefore implementations will be vulnerable to active MITM attacks. To enable protection against active Man-in-the-Middle attacks, BR/EDR Security Mode 4 Level 4 or stronger shall be required for access to all services used by this profile, except for service and characteristic discovery.

While operating in one of the LE roles, the device shall remain in non-discoverable mode in BR/EDR.

Bonding shall be supported by the CWD.

Bonding shall be supported by the CWC.

7 Additional requirements for BR/EDR

There are no additional requirements beyond those found in the Bluetooth Core Specification [1].

8 Acronyms and abbreviations

Acronym/Abbreviation	Meaning
AD	Advertising Data
BAS	Battery Service
BR/EDR	Basic Rate/Enhanced Data Rate
CA	Cooking Appliance
CWC	Cookware Client
CWD	Cookware Device
CWP	Cookware Profile
CWS	Cookware Service
DIS	Device Information Service
GAP	Generic Access Profile
GATT	Generic Attribute Profile
LE	Low Energy
MSC	Message sequence chart
PDU	Protocol Data Unit
RFU	Reserved for Future Use
UUID	Universally unique identifier

Table 8.1: Acronyms and abbreviations

9 References

[1] Bluetooth Core Specification, Version 6.1 or later

[2] Cookware Service, Version 1.0 or later

[3] Device Information Service, Version 1.2 or later

[4] Battery Service, Version 1.1 or later

[5] Bluetooth Assigned Numbers, https://www.bluetooth.com/specifications/assigned-numbers

[6] Supplement to the Bluetooth Core Specification, Version 13 or later