Authorization Control Profile (ACP)

***Bluetooth*® Test Suite**

- **Revision:** ACP.TS.p1
- **Revision Date:** 2023-06-29
- **Prepared By:** Medical Devices Working Group
- **Published during TCRL:** TCRL.2023-1

Contents

1 Scope

This Bluetooth document contains the Test Suite Structure (TSS) and test cases to test the implementation of the Bluetooth Authorization Control Profile (ACP) Specification with the objective to provide a high probability of air interface interoperability between the tested implementation and other manufacturers' Bluetooth devices.

2 References, definitions, and abbreviations

2.1 References

This document incorporates provisions from other publications by dated or undated reference. These references are cited at the appropriate places in the text, and the publications are listed hereinafter. Additional definitions and abbreviations can be found in [1], [2], and [3].

[1] Bluetooth Core Specification, Version 4.2 or later

[2] Test Strategy and Terminology Overview

[3] Authorization Control Profile (ACP) Specification, Version 1.0

[4] Authorization Control Service (ACS) Specification, Version 1.0

[5] ICS Proforma for Authorization Control Profile (ACP)

[6] GATT Test Suite, GATT.TS

[7] Characteristic and Descriptor descriptions are accessible via the Bluetooth SIG Assigned Numbers

[8] ICS Proforma for Authorization Control Service (ACS)

[9] IXIT Proforma for Authorization Control Profile and Authorization Control Service

2.2 Definitions

In this Bluetooth document, the definitions from [1], [2], and [3] apply.

2.3 Acronyms and abbreviations

In this Bluetooth document, the definitions, acronyms, and abbreviations from [1], [2], and [3] apply.

3 Test Suite Structure (TSS)

3.1 Overview

The Authorization Control Profile requires the presence of GAP, SM (for LE), SDP (for BR/EDR), and GATT. This is illustrated in Figure 3.1.

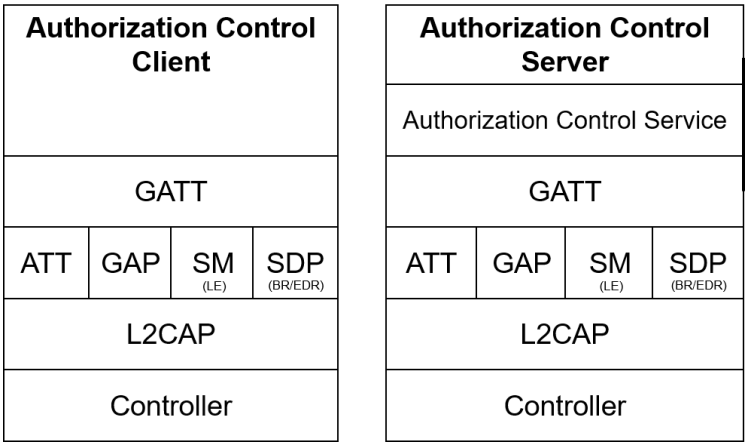

Figure 3.1: Authorization Control test models

3.2 Test Strategy

The test objectives are to verify the functionality of the Authorization Control Profile within a Bluetooth Host and enable interoperability between Bluetooth Hosts on different devices. The testing approach covers mandatory and optional requirements in the specification and matches these to the support of the IUT as described in the ICS. Any defined test herein is applicable to the IUT if the ICS logical expression defined in the Test Case Mapping Table (TCMT) evaluates to true.

The test equipment provides an implementation of the Radio Controller and the parts of the Host needed to perform the test cases defined in this Test Suite. A Lower Tester acts as the IUT's peer device and interacts with the IUT over-the-air interface. The configuration, including the IUT, needs to implement similar capabilities to communicate with the test equipment. For some test cases, it is necessary to stimulate the IUT from an Upper Tester. In practice, this could be implemented as a special test interface, a Man Machine Interface (MMI), or another interface supported by the IUT.

This Test Suite contains Valid Behavior (BV) tests complemented with Invalid Behavior (BI) tests where required. The test coverage mirrored in the Test Suite Structure is the result of a process that started with catalogued specification requirements that were logically grouped and assessed for testability enabling coverage in defined test purposes.

3.3 Test groups

The following test groups have been defined:

- Generic GATT Integrated Tests
- Access Protected Resource
- ACS Control Point Procedures
- General Error Handling

4 Test cases (TC)

4.1 Introduction

4.1.1 Test case identification conventions

Test cases are assigned unique identifiers per the conventions in [2]. The convention used here is:
<spec abbreviation>/<IUT role>/<class>/**<feat>**/<func>/<subfunc>/<cap>/**<xx>-<nn>-<y>**.

Additionally, testing of this specification includes tests from the GATT Test Suite [6] referred to as Generic GATT Integrated Tests (GGIT); when used, the GGIT tests are referred to through a TCID string using the following convention:
<spec abbreviation>/<IUT role>/<GGIT test group>/<GGIT class>/<xx>-<nn>-<y>.

Identifier Abbreviation	**Spec Identifier <spec abbreviation>**
ACP	Authorization Control Profile
Identifier Abbreviation	**Role Identifier <IUT role>**
CL	Client Role
SR	Server Role
Identifier Abbreviation	**Reference Identifier <GGIT test group>**
CGGIT	Client Generic GATT Integrated Tests
SGGIT	Server Generic GATT Integrated Tests
Identifier Abbreviation	**Reference Identifier <GGIT class>**
CHA	Characteristic
SDPNF	SDP Record Not Found
SER	Service
Identifier Abbreviation	**Features and Behaviors Identifier <feat>**
ACSCP	ACS Control Point Procedures
ACSD	ACS Data
GEH	General Error Handling

Table 4.1: ACP TC feature naming conventions

4.1.2 Conformance

When conformance is claimed for a particular specification, all capabilities are to be supported in the specified manner. The mandated tests from this Test Suite depend on the capabilities to which conformance is claimed.

The Bluetooth Qualification Program may employ tests to verify implementation robustness. The level of implementation robustness that is verified varies from one specification to another and may be revised for cause based on interoperability issues found in the market.

Such tests may verify:

- That claimed capabilities may be used in any order and any number of repetitions not excluded by the specification
- That capabilities enabled by the implementations are sustained over durations expected by the use case
- That the implementation gracefully handles any quantity of data expected by the use case

- That in cases where more than one valid interpretation of the specification exists, the implementation complies with at least one interpretation and gracefully handles other interpretations
- That the implementation is immune to attempted security exploits

A single execution of each of the required tests is required to constitute a Pass verdict. However, it is noted that to provide a foundation for interoperability, it is necessary that a qualified implementation consistently and repeatedly pass any of the applicable tests.

In any case, where a member finds an issue with the test plan generated by Launch Studio, with the test case as described in the Test Suite, or with the test system utilized, the member is required to notify the responsible party via an erratum request such that the issue may be addressed.

4.1.3 Pass/Fail verdict conventions

Each test case has an Expected Outcome section. The IUT is granted the Pass verdict when all the detailed pass criteria conditions within the Expected Outcome section are met.

The convention in this Test Suite is that, unless there is a specific set of fail conditions outlined in the test case, the IUT fails the test case as soon as one of the pass criteria conditions cannot be met. If this occurs, the outcome of the test is a Fail verdict.

4.2 Setup preambles

The procedures defined in this section are used to achieve specific conditions on the IUT and the test equipment within the tests defined in this document. The preambles here are commonly used to establish initial conditions.

4.2.1 ATT Bearer on LE transport

- Preamble Procedure

  1. Establish an LE transport connection between the IUT and the Lower Tester.
  2. Establish an L2CAP channel 0x0004 between the IUT and the Lower Tester over that LE transport.

4.2.2 ATT Bearer on BR/EDR transport

- Preamble Procedure

  1. Establish a BR/EDR transport connection between the IUT and the Lower Tester.
  2. Establish an L2CAP channel (PSM 0x001F) between the IUT and the Lower Tester over that BR/EDR transport.

4.2.3 ACS Characteristics and Control Point Configuration

- Preamble Purpose

  This preamble procedure enables the Lower Tester for use with the ACS characteristics and Control Point.

- Preamble Procedure

  1. If a connection exists, it is disconnected.
  2. Establish an ATT Bearer connection between the Lower Tester and the IUT as described in Section 4.2.1, if using an LE transport, or Section 4.2.2 if using a BR/EDR transport.
  3. The handles of the ACS Status, ACS Data In, ACS Data Out Notify, ACS Data Out Indicate, and ACS Control Point, if supported, have been previously discovered by the Upper Tester during the test procedures in Section 4.3 or are known to the Upper Tester by other means.

4. The handles of the Client Characteristic Configuration descriptor of the ACS Status, ACS Data Out Notify, ACS Data Out Indicate, and ACS Control Point have been previously discovered by the Upper Tester during the test procedure in Section 4.3 or are known to the Upper Tester by other means.
5. The ACS Status, ACS Data Out Notify, ACS Data Out Indicate, and ACS Control Point are configured for indications or notifications as described in Table 4.2.

Characteristic	Characteristic is configured for
ACS Status	Indication
ACS Data Out Notify	Notification
ACS Data Out Indicate	Indication
ACS Control Point	Indication

Table 4.2: Configuration preamble for ACS characteristics and Control Point

4.3 Generic GATT Integrated Tests

Execute the Generic GATT Integrated Tests defined in Section 6.3, Server test procedures (SGGIT), and Section 6.4, Client test procedures (CGGIT), in [6] using Table 4.3 below as input:

TCID	Service / Characteristic	Reference	Properties	Value Length (Octets)	Type
ACP/CL/CGGIT/SER/BV-01-C [Service GGIT – Authorization Control]	Authorization Control Service	[3] 5.2	-	-	Primary Service
ACP/CL/CGGIT/CHA/BV-02-C [Characteristic GGIT – ACS Status]	ACS Status Characteristic	[3] 5.3, 5.5.2	0x22 (Read, Indicate)	3	-
ACP/CL/CGGIT/CHA/BV-03-C [Characteristic GGIT – ACS Data In]	ACS Data In Characteristic	[3] 5.3, 5.5.3	0x08 (Write)	Skip	-
ACP/CL/CGGIT/CHA/BV-04-C [Characteristic GGIT – ACS Data Out Notify]	ACS Data Out Notify Characteristic	[3] 5.3, 5.5.3	0x10 (Notify)	Skip	-
ACP/CL/CGGIT/CHA/BV-05-C [Characteristic GGIT – ACS Data Out Indicate]	ACS Data Out Indicate Characteristic	[3] 5.3, 5.5.3	0x20 (Indicate)	Skip	-
ACP/CL/CGGIT/CHA/BV-06-C [Characteristic GGIT – ACS Control Point]	ACS Control Point Characteristic	[3] 5.3, 5.5.4	0x28 (Write, Indicate)	Skip	-
ACP/SR/SGGIT/SDPNF/BV-01-C [Not discoverable over BR/EDR – Authorization Control]	Authorization Control Service	[3] 5.2	-	-	-

Table 4.3: Input for the GGIT Client and Server test procedures

4.4 Access Protected Resource

Verify the IUT's ability to request, respond to, and interpret values when accessing a protected resource.

4.4.1 Authenticated Encryption or Messaging by Server

- Test Purpose

  Verify that the IUT can perform the authenticated encryption or authenticated messaging, described in Table 4.4, using the ACS Data characteristics.

- Reference

  [3] 4.1.1.2

  [4] 4.3.1

- Initial Condition

  - Perform the preamble described in Section 4.2.3 to configure the ACS Control Point, ACS Data Out Notify, and/or ACS Data Out Indicate characteristics.
  - The Lower Tester requests the Get Restriction Map Descriptor procedure using the ACS Control Point characteristic to acquire the protected resources.
  - The Lower Tester requests the Get Information Security Configuration Descriptor procedure using the ACS Control Point characteristic to acquire the information security configurations.
  - The IUT and the Lower Tester have established the necessary security by performing a key exchange.

- Test Case Configuration

Test Case	Protected resource uses
ACP/SR/ACSD/BV-01-C [Authenticated Encryption using GCM by Server]	GCM authenticated encryption
ACP/SR/ACSD/BV-02-C [Authenticated Messaging using GMAC by Server]	GMAC authenticated messaging

Table 4.4: Authenticated Encryption or Messaging by Server test cases

- Test Procedure

  1. The Lower Tester sends an ATT_Write_Request to the ACS Data In characteristic with a Segmentation_Header field and Payload field consisting of information security controls applied to access a protected resource using the security control described in Table 4.4.
  2. The IUT responds with the appropriate ACS Data Out characteristic in either ATT_Handle_Value_Indication(s) or ATT_Handle_Value_Notification(s). The response has the security configuration controls applied and has the necessary ACS Data Out characteristic header fields.
  3. For each indication, the IUT receives an ATT_Handle_Value_Confirmation from the Lower Tester.
  4. Verify that the characteristic value meets the requirements of the service.

- Expected Outcome

  Pass verdict

  The IUT allows access to the protected resource, to the Lower Tester, using the security control described in Table 4.4.

  The Segmentation_Header field in all requests and responses includes the First Segment bit, Last Segment bit, and Rolling Segment Counter bits with appropriate values.

4.4.2 Authenticated Encryption or Messaging by Client

- Test Purpose

  Verify that the IUT can perform authenticated encryption or authenticated messaging, as described in Table 4.5, on the ACS Data characteristics.

- Reference

  [3] 5.4.2, 5.5.3

- Initial Condition

  - Perform the preamble described in Section 4.2.3 to configure ACS Control Point, ACS Data Out Notify, and/or ACS Data Out Indicate characteristics.
  - The Upper Tester sends a command to the IUT to request the Get Restriction Map Descriptor procedure using the ACS Control Point characteristic to acquire the protected resources of the Lower Tester.
  - The Upper Tester sends a command to the IUT to request the Get Information Security Configuration Descriptor procedure using the ACS Control Point characteristic to acquire the information security configurations of the Lower Tester.
  - The IUT and Lower Tester have established the necessary security by performing a key exchange.

- Test Case Configuration

Test Case	Protected resource uses
ACP/CL/ACSD/BV-03-C [Authenticated Encryption using GCM by Client]	GCM authenticated encryption
ACP/CL/ACSD/BV-04-C [Authenticated Messaging using GMAC by Client]	GMAC authenticated messaging

Table 4.5: Authenticated Encryption or Messaging by Client test cases

- Test Procedure

  1. The Upper Tester sends a command to the IUT to write a Segmentation_Header field and Payload field containing a request to the ACS Data In characteristic with information security controls applied to access a protected resource using the security control described in Table 4.5.
  2. The IUT sends an ATT_Write_Request to the ACS Data In characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 1.
  3. The Lower Tester responds with the appropriate ACS Data Out characteristic in either ATT_Handle_Value_Indication(s) or ATT_Handle_Value_Notification(s).
  4. The IUT receives the ATT_Handle_Value_Indication(s) or ATT_Handle_Value_Notification(s) from the Lower Tester and reports them to the Upper Tester.

5. For each indication, the IUT sends an ATT_Handle_Value_Confirmation to the ACS Data In characteristic of the Lower Tester.
6. Verify that the characteristic value meets the requirements of the service.

- Expected Outcome

  Pass verdict

  The IUT accesses the protected resource of the Lower Tester using the security control described in Table 4.5 and reports the value to the Upper Tester.

  The Segmentation_Header field in all requests and responses includes the First Segment bit, Last Segment bit, and Rolling Segment Counter bits with appropriate values.

ACP/CL/ACSD/BV-05-C [Write long characteristic value to ACS Data In]

- Test Purpose

  Verify that the IUT can write to the ACS Data In characteristic using the Write Long Characteristic Values sub-procedure.

- Reference

  [3] 5.5.3

- Initial Condition

  - Perform the preamble described in Section 4.2.3 to configure the ACS Control Point, ACS Data Out Notify, and/or ACS Data Out Indicate characteristics.
  - The Upper Tester sends a command to the IUT to request the Get All Active Descriptors procedure using the ACS Control Point characteristic to acquire the current restriction map descriptor, information security controls descriptor, and key descriptor of the Lower Tester.
  - The IUT and the Lower Tester have established the necessary security by performing a key exchange.

- Test Procedure

  1. The Upper Tester sends a command to the IUT to write, by executing the GATT Write Long Characteristic Values sub-procedure, Segmentation_Header and Payload fields containing a request to the ACS Data In characteristic of the value for a protected resource.
  2. The IUT sends ATT_Prepare_Write_Requests to the ACS Data In characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 1.
  3. For each received ATT_Prepare_Write_Request, the Lower Tester sends an ATT_Prepare_Write_Response.
  4. After receiving the ATT_Execute_Write_Request, the Lower Tester sends an ATT_Execute_Write_Response.
  5. Verify that the characteristic value meets the requirements of the service.

- Expected Outcome

  Pass verdict

  The IUT sends correctly formatted ATT_Prepare_Write_Requests to the Lower Tester.

  The IUT sends an ATT_Execute_Write_Request to the Lower Tester.

  The Segmentation_Header field in all requests and responses includes the First Segment bit, Last Segment bit, and Rolling Segment Counter bits with appropriate values.

4.5 ACS Control Point procedures

Verify the IUT's ability to configure, conduct compliant operations, and interpret values of the ACS Control Point characteristic.

Table 4.13 in [4] defines the opcodes and operands used in the ACS Control Point procedure test cases in this section.

ACP/CL/ACSCP/BV-01-C [Get All Active Descriptors]

- Test Purpose

  Verify that the IUT can perform the Get All Active Descriptors procedure when the restriction map is unprotected and can receive all the ACS descriptors.

- Reference

  [3] 5.5.4.2

- Initial Condition

  - Perform the preamble described in Section 4.2.3 to configure the ACS Control Point characteristic.
  - The restriction map descriptor of the Lower Tester is unprotected.

- Test Procedure

  1. The Upper Tester sends a command to the IUT to write a Segmentation_Header field and Payload field containing the Get All Active Descriptors opcode (0x01) to the ACS Control Point with no operand.
  2. The IUT sends an ATT_Write_Request to the ACS Control Point characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 1.
  3. The Lower Tester sends ATT_Handle_Value_Indication(s) on the ACS Control Point characteristic with the Segmentation_Header field and Payload field containing the Restriction Map Descriptor Response opcode (0x03) and an operand with one or more Restriction Map records.
  4. The IUT receives the ATT_Handle_Value_Indication(s) from the Lower Tester and reports them to the Upper Tester.
  5. For each indication, the IUT sends an ATT_Handle_Value_Confirmation on the ACS Control Point characteristic.
  6. After all confirmations have been received, the Lower Tester sends ATT_Handle_Value_Indication(s) on the ACS Control Point characteristic with the Segmentation_Header field and Payload field containing the Information Security Configuration Descriptor Response opcode (0x0C) and an operand with one or more Information Security Configuration records.
  7. The IUT receives the ATT_Handle_Value_Indication(s) from the Lower Tester and reports them to the Upper Tester.
  8. For each indication, the IUT sends an ATT_Handle_Value_Confirmation on the ACS Control Point characteristic.
  9. After all confirmations have been received, the Lower Tester sends ATT_Handle_Value_Indication(s) on the ACS Control Point characteristic with the Segmentation_Header field and Payload field containing the Key Descriptor Response opcode (0x0E) and an operand with one or more Key records.
  10. The IUT receives the ATT_Handle_Value_Indication(s) from the Lower Tester and reports them to the Upper Tester.

11. For each indication, the IUT responds with an ATT_Handle_Value_Confirmation on the ACS Control Point characteristic.
12. The Lower Tester sends ATT_Handle_Value_Indication(s) on the ACS Control Point characteristic with the Segmentation_Header field and Payload field containing the Response Code opcode (0x00) and an operand with the Request_Opcode field set to Get All Active Descriptors (0x01) and the Response_Code_Value field set to Success (0x01).
13. The IUT receives the ATT_Handle_Value_Indication(s) from the Lower Tester and reports them to the Upper Tester.
14. The IUT sends an ATT_Handle_Value_Confirmation on the ACS Control Point characteristic.
15. Verify that the characteristic value meets the requirements of the service.

- Expected Outcome

  Pass verdict

  The IUT receives one or more Restriction Map records from the Lower Tester and reports it to the Upper Tester.

  The IUT receives one or more Information Security Configuration records from the Lower Tester and reports it to the Upper Tester.

  The IUT receives one or more Key records from the Lower Tester and reports it to the Upper Tester.

  The IUT receives confirmation of the Get All Active Descriptors procedure requested from the Lower Tester and reports it to the Upper Tester.

  The Segmentation_Header field in all requests and responses includes the First Segment bit, Last Segment bit, and Rolling Segment Counter bits with appropriate values.

ACP/CL/ACSCP/BV-02-C [Get All Active Descriptors procedure with a restriction map that is protected]

- Test Purpose

  Verify that the IUT can perform the Get All Active Descriptors procedure when the restriction map is protected and can receive all the protected ACS descriptors.

- Reference

  [3] 5.5.4.2

- Initial Condition

  - Perform the preamble described in Section 4.2.3 to configure the ACS Control Point and ACS Data Out Indicate characteristics.
  - The Upper Tester sends a command to the IUT to request the Get Information Security Configuration Descriptor procedure using the ACS Control Point characteristic to acquire the information security configuration controls that are mapped to the restriction map IDs to be requested.
  - The restriction map descriptor of the Lower Tester is protected.
  - The IUT and the Lower Tester have established the necessary security by performing a key exchange.

- Test Procedure

  1. The Upper Tester sends a command to the IUT to write a Segmentation_Header field and Payload field containing the Get All Active Descriptors opcode (0x01) to the ACS Data In characteristic, with no operand, with information security controls applied.
  2. The IUT sends an ATT_Write_Request to the ACS Data In characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 1.
  3. The Lower Tester sends ATT_Handle_Value_Indication(s) on the ACS Data Out Indicate characteristic with the Segmentation_Header field and Payload field containing the Restriction Map Descriptor Response opcode (0x03) and an operand with one or more Restriction Map records with information security controls applied.
  4. The IUT receives the ATT_Handle_Value_Indication(s) from the Lower Tester and reports them to the Upper Tester.
  5. For each indication, the IUT sends an ATT_Handle_Value_Confirmation on the ACS Data Out Indicate characteristic.
  6. After all confirmations have been received, the Lower Tester sends ATT_Handle_Value_Indication(s) on the ACS Data Out Indicate characteristic with the Segmentation_Header field and Payload field containing the Information Security Configuration Descriptor Response opcode (0x0C) and an operand with one or more Information Security Configuration records with information security controls applied.
  7. The IUT receives the ATT_Handle_Value_Indication(s) from the Lower Tester and reports them to the Upper Tester.
  8. For each indication, the IUT sends an ATT_Handle_Value_Confirmation on the ACS Data Out Indicate characteristic.
  9. After all confirmations have been received, the Lower Tester sends ATT_Handle_Value_Indication(s) on the ACS Data Out Indicate characteristic with the Segmentation_Header field and Payload field containing the Key Descriptor Response opcode (0x0E) and an operand with one or more Key records with information security controls applied.
  10. The IUT receives the ATT_Handle_Value_Indication(s) from the Lower Tester and reports them to the Upper Tester.
  11. For each indication, the IUT sends an ATT_Handle_Value_Confirmation on the ACS Data Out Indicate characteristic.
  12. The Lower Tester sends ATT_Handle_Value_Indication(s) of the ACS Data Out Indicate characteristic with the Segmentation_Header field and Payload field containing the Response Code opcode (0x00) and an operand with the Request_Opcode field set to Get All Active Descriptors (0x01) and the Response_Code_Value field set to Success (0x01) with information security controls applied.
  13. The IUT receives the ATT_Handle_Value_Indication(s) from the Lower Tester and reports them to the Upper Tester.
  14. The IUT sends an ATT_Handle_Value_Confirmation on the ACS Data Out Indicate characteristic.
  15. Verify that the characteristic value meets the requirements of the service.

- Expected Outcome

  Pass verdict

  The IUT receives one or more Restriction Map records from the Lower Tester and reports it to the Upper Tester.

  The IUT receives one or more Information Security Configuration records from the Lower Tester and reports it to the Upper Tester.

  The IUT receives one or more Key records from the Lower Tester and reports it to the Upper Tester.

The IUT receives confirmation from the Lower Tester of the Get All Active Descriptors procedure requested and reports it to the Upper Tester.

The Segmentation_Header field in all requests and responses includes the First Segment bit, Last Segment bit, and Rolling Segment Counter bits with appropriate values.

4.5.1 Get Restriction Map Descriptor

- Test Purpose

  Verify that, for each selected test case in Table 4.6, the IUT can perform the Get Restriction Map Descriptor procedure when the restriction map is unprotected.

- Reference

  [3] 5.5.4.3

- Initial Condition

  - Perform the preamble described in Section 4.2.3 to configure the ACS Control Point characteristic.
  - The Upper Tester sends a command to the IUT to request the Get Restriction Map ID List procedure using the ACS Control Point characteristic to acquire the available restriction map IDs and requests an unprotected restriction map.
  - As provided by the Lower Tester, the Upper Tester knows the Resource Handle Filter value to be used by the IUT.

- Test Case Configuration

Test Case	Resource Handle Filter value	Response Operand
ACP/CL/ACSCP/BV-03-C [Get Restriction Map Descriptor]	The Resource_Handle_Filter field is set to no filtering (0xFFFF).	An operand containing one or more Restriction Map records.
ACP/CL/ACSCP/BV-04-C [Get Restriction Map Descriptor based on Resource Handle Filter]	The Resource_Handle_Filter field is set to the resource handle value provided by the Lower Tester.	An operand containing the Restriction Map record for the resource handle identified in the request.

Table 4.6: Get Restriction Map Descriptor test cases

- Test Procedure

  1. The Upper Tester sends a command to the IUT to write a Segmentation_Header field and Payload field containing the Get Restriction Map Descriptor opcode (0x02) to the ACS Control Point with an operand with the Restriction_Map_ID field set to an available unprotected restriction map ID and the Resource_Handle_Filter field set to <Resource Handle Filter value> as described in Table 4.6.
  2. The IUT sends an ATT_Write_Request to the ACS Control Point characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 1.
  3. The Lower Tester sends ATT_Handle_Value_Indication(s) of the ACS Control Point characteristic with the Segmentation_Header field and Payload field containing the Restriction Map Descriptor Response opcode (0x03) and an operand with the <Response Operand> as described in Table 4.6.
  4. The IUT receives ATT_Handle_Value_Indication(s) from the Lower Tester and reports it to the Upper Tester.

5. For each indication, the IUT sends an ATT_Handle_Value_Confirmation on the ACS Control Point characteristic.
6. Verify that the characteristic values meet the requirements of the service.

- Expected Outcome

  Pass verdict

  For each selected test case in Table 4.6, the IUT receives indication(s) from the Lower Tester of the ACS Control Point characteristic until all records of the Restriction Map, identified by the Resource Handle Filter included in the request, have been sent and reports it to the Upper Tester.

  The Segmentation_Header field in all requests and responses includes the First Segment bit, Last Segment bit, and Rolling Segment Counter bits with appropriate values.

ACP/CL/ACSCP/BV-05-C [Get Restriction Map Descriptor procedure with a restriction map that is protected]

- Test Purpose

  Verify that the IUT can perform the Get Restriction Map Descriptor procedure when the restriction map is protected.

- Reference

  [3] 5.5.4.3

- Initial Condition

  - Perform the preamble described in Section 4.2.3 to configure the ACS Control Point and ACS Data Out Indicate characteristics.
  - The Upper Tester sends a command to the IUT to request the Get Restriction Map ID List procedure using the ACS Control Point characteristic to acquire the available restriction map IDs and their mapping to a security configuration ID.
  - The Upper Tester sends a command to the IUT to request the Get Information Security Configuration Descriptor procedure using the ACS Control Point characteristic to acquire the information security configuration controls that are mapped to the restriction map IDs to be requested.
  - The restriction map ID to be requested is protected.
  - The IUT and the Lower Tester have established the necessary security by performing a key exchange.

- Test Procedure

  1. The Upper Tester sends a command to the IUT to write a Segmentation_Header field and Payload field containing the Get Restriction Map Descriptor opcode (0x02) to the ACS Data In characteristic with an operand with the Restriction_Map_ID field set to an available protected restriction map ID and no filtering by protected resource (0xFFFF) with information security controls applied.
  2. The IUT sends an ATT_Write_Request to the ACS Data In characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 1.
  3. The Lower Tester responds with ATT_Handle_Value_Indication(s) on the ACS Data Out Indicate characteristic with the Segmentation_Header field and Payload field containing the Restriction Map Descriptor Response opcode (0x03) and an operand with one or more Restriction Map records with information security controls applied.

4. The IUT receives ATT_Handle_Value_Indication(s) from the Lower Tester and reports it to the Upper Tester.
5. For each indication, the IUT sends an ATT_Handle_Value_Confirmation on the ACS Data Out Indicate characteristic.
6. Verify that the characteristic values meet the requirements of the service.

- Expected Outcome

  Pass verdict

  The IUT receives one or more protected Restriction Map records from the Lower Tester, confirming the Get Restriction Map Descriptor procedure requested, and reports it to the Upper Tester.

  The Segmentation_Header field in all requests and responses includes the First Segment bit, Last Segment bit, and Rolling Segment Counter bits with appropriate values.

ACP/CL/ACSCP/BV-06-C [Get Restriction Map ID List]

- Test Purpose

  Verify that the IUT can perform the Get Restriction Map ID List procedure.

- Reference

  [3] 5.5.4.4

- Initial Condition

  - Perform the preamble described in Section 4.2.3 to configure the ACS Control Point characteristic.

- Test Procedure

1. The Upper Tester sends a command to the IUT to write a Segmentation_Header field and Payload field containing the Get Restriction Map ID List opcode (0x04) to the ACS Control Point with no operand.
2. The IUT sends an ATT_Write_Request to the ACS Control Point characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 1.
3. The Lower Tester sends ATT_Handle_Value_Indication(s) of the ACS Control Point characteristic with the Segmentation_Header field and Payload field containing the Restriction Map ID List Response opcode (0x05) and an operand with the available Restriction Map IDs each mapped to an Information Security Configuration ID.
4. The IUT receives ATT_Handle_Value_Indication(s) from the Lower Tester and reports it to the Upper Tester.
5. For each indication, the IUT sends an ATT_Handle_Value_Confirmation on the ACS Control Point characteristic.
6. Verify that the characteristic values meet the requirements of the service.

- Expected Outcome

  Pass verdict

  The IUT receives the list of Restriction Map IDs, each mapped to an Information Security Configuration ID from the Lower Tester, and reports it to the Upper Tester.

  The Segmentation_Header field in all requests and responses includes the First Segment bit, Last Segment bit, and Rolling Segment Counter bits with appropriate values.

ACP/CL/ACSCP/BV-07-C [Activate Restriction Map]

- Test Purpose

  Verify that the IUT can perform the Activate Restriction Map procedure when the restriction map is unprotected.

- Reference

  [3] 5.5.4.5

- Initial Condition

  - Perform the preamble described in Section 4.2.3 to configure the ACS Control Point characteristic.
  - The Upper Tester sends a command to the IUT to request the Get Restriction Map ID List procedure using the ACS Control Point characteristic to acquire the available unprotected restriction map IDs.

- Test Procedure

  1. The Upper Tester sends a command to the IUT to write a Segmentation_Header field and Payload field containing the Activate Restriction Map opcode (0x06) to the ACS Control Point with an operand with the Restriction_Map_ID field with the ID of the unprotected restriction map to be activated.
  2. The IUT sends an ATT_Write_Request to the ACS Control Point characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 1.
  3. The Lower Tester sends an ATT_Handle_Value_Indication of the ACS Control Point characteristic with the Segmentation_Header field and Payload field containing the Response Code opcode (0x00) and an operand representing the Request_Opcode field (0x06) followed by the Response_Code_Value field set to Success (0x01).
  4. The IUT receives an ATT_Handle_Value_Indication from the Lower Tester and reports it to the Upper Tester.
  5. The IUT sends an ATT_Handle_Value_Confirmation on the ACS Control Point characteristic.
  6. The Upper Tester sends a command to the IUT to read the ACS Status characteristic.
  7. The IUT sends an ATT_Read_Request to the ACS Status characteristic of the Lower Tester.
  8. The Lower Tester sends an ATT_Read_Response to the IUT.
  9. The IUT receives the ATT_Read_Response and reports the values to the Upper Tester.
  10. Verify that the characteristic values meet the requirements of the service.

- Expected Outcome

  Pass verdict

  The IUT receives confirmation from the Lower Tester of the Activate Restriction Map procedure requested and reports it to the Upper Tester.

  The IUT receives an ATT_Read_Response from the Lower Tester with the Current_Restriction_Map_ID field matching the ID sent in step 1 and reports it to the Upper Tester.

  The Segmentation_Header field in all requests and responses includes the First Segment bit, Last Segment bit, and Rolling Segment Counter bits with appropriate values.

ACP/CL/ACSCP/BV-08-C [Activate Restriction Map procedure with a restriction map that is protected]

- Test Purpose

  Verify that the IUT can perform the Activate Restriction Map procedure when the restriction map is protected.

- Reference

  [3] 5.5.4.5

- Initial Condition

  - Perform the preamble described in Section 4.2.3 to configure the ACS Control Point and ACS Data Out Indicate characteristics.
  - The Upper Tester sends a command to the IUT to request the Get Restriction Map ID List procedure using the ACS Control Point characteristic to acquire the restriction map to be activated.
  - The Upper Tester sends a command to the IUT to request the Get Information Security Configuration Descriptor procedure using the ACS Control Point characteristic to acquire the information security configuration controls that are mapped to the restriction map to be activated.
  - The restriction map ID to be activated is protected.
  - The IUT and the Lower Tester have established the necessary security by performing a key exchange.

- Test Procedure

  1. The Upper Tester sends a command to the IUT to write a Segmentation_Header field and Payload field containing the Activate Restriction Map opcode (0x06) to the ACS Data In characteristic with an operand with the Restriction_Map_ID field with the ID of the protected restriction map to be activated with information security controls applied.
  2. The IUT sends an ATT_Write_Request to the ACS Data In characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 1.
  3. The Lower Tester sends an ATT_Handle_Value_Indication on the ACS Data Out Indicate characteristic with the Segmentation_Header field and Payload field containing the Response Code opcode (0x00) and an operand representing the Request_Opcode field (0x06) followed by the Response_Code_Value field set to Success (0x01) with information security controls applied.
  4. The IUT receives an ATT_Handle_Value_Indication from the Lower Tester and reports it to the Upper Tester.
  5. The IUT sends an ATT_Handle_Value_Confirmation on the ACS Data Out Indicate characteristic.
  6. Verify that the characteristic values meet the requirements of the service.

- Expected Outcome

  Pass verdict

  The IUT receives confirmation from the Lower Tester of the Activate Restriction Map procedure requested and reports it to the Upper Tester.

  The Segmentation_Header field in all requests and responses includes the First Segment bit, Last Segment bit, and Rolling Segment Counter bits with appropriate values.

ACP/CL/ACSCP/BV-09-C [Get Resource Handle To UUID Map]

- Test Purpose

  Verify that the IUT can perform the Get Resource Handle to UUID Map procedure.

- Reference

  [3] 5.5.4.6

- Initial Condition

  - Perform the preamble described in Section 4.2.3 to configure the ACS Control Point characteristic.

- Test Procedure

  1. The Upper Tester sends a command to the IUT to write a Segmentation_Header field and Payload field containing the Get Resource Handle to UUID Map opcode (0x07) to the ACS Control Point with no operand.
  2. The IUT sends an ATT_Write_Request to the ACS Control Point characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 1.
  3. The Lower Tester sends ATT_Handle_Value_Indication(s) of the ACS Control Point characteristic with the Segmentation_Header field and Payload field containing the Resource Handle To UUID Map Response opcode (0x08) and an operand with the Resource Handle to UUID Map records.
  4. The IUT receives ATT_Handle_Value_Indication(s) from the Lower Tester and reports it to the Upper Tester.
  5. For each indication, the IUT sends an ATT_Handle_Value_Confirmation on the ACS Control Point characteristic.
  6. Verify that the characteristic values meet the requirements of the service.

- Expected Outcome

  Pass verdict

  The IUT receives the complete Resource Handle to UUID Map records from the Lower Tester confirming the Get Resource Handle To UUID Map procedure requested and reports it to the Upper Tester.

  The Segmentation_Header field in all requests and responses includes the First Segment bit, Last Segment bit, and Rolling Segment Counter bits with appropriate values.

ACP/CL/ACSCP/BV-10-C [Get Service And Characteristic UUIDs For Characteristic Resource Handle]

- Test Purpose

  Verify that the IUT can perform the Get Service And Characteristic UUIDs For Characteristic Resource Handle procedure.

- Reference

  [3] 5.5.4.7

- Initial Condition

  - Perform the preamble described in Section 4.2.3 to configure the ACS Control Point characteristic.

- Test Procedure

  1. The Upper Tester sends a command to the IUT to write a Segmentation_Header field and Payload field containing the Get Service And Characteristic UUIDs For Characteristic Resource Handle opcode (0x09) to the ACS Control Point with an operand with a Characteristic Resource Handle.
  2. The IUT sends an ATT_Write_Request to the ACS Control Point characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 1.
  3. The Lower Tester sends ATT_Handle_Value_Indication(s) of the ACS Control Point characteristic with the Segmentation_Header field and Payload field containing the Service And Characteristic UUIDs For Characteristic Resource Handle Response opcode (0x0A) and an operand with the service and characteristic UUIDs.
  4. The IUT receives ATT_Handle_Value_Indication(s) from the Lower Tester and reports it to the Upper Tester.
  5. For each indication, the IUT sends an ATT_Handle_Value_Confirmation on the ACS Control Point characteristic.
  6. Verify that the characteristic values meet the requirements of the service.

- Expected Outcome

  Pass verdict

  The IUT receives the service UUID and characteristic UUID size and values from the Lower Tester, confirming the Get Service And Characteristic UUIDs For Characteristic Resource Handle procedure requested, and reports them to the Upper Tester.

  The Segmentation_Header field in all requests and responses includes the First Segment bit, Last Segment bit, and Rolling Segment Counter bits with appropriate values.

4.5.2 Get Information Security Configuration Descriptor

- Test Purpose

  Verify that, for each selected test case in Table 4.7, the IUT can perform the Get Information Security Configuration Descriptor procedure.

- Reference

  [3] 5.5.4.8

- Initial Condition

  - Perform the preamble described in Section 4.2.3 to configure the ACS Control Point characteristic.
  - As provided by the Lower Tester, the Upper Tester knows the Information Security Configuration ID Filter value to be used by the IUT.

- Test Case Configuration

Test Case	Information Security Configuration ID Filter value	Response Operand
ACP/CL/ACSCP/BV-11-C [Get Information Security Configuration Descriptor]	The Information_Security_ Configuration_ID_Filter field is set to no filtering (0xFFFF).	An operand containing one or more Information Security Configuration records.

Test Case	Information Security Configuration ID Filter value	Response Operand
ACP/CL/ACSCP/BV-12-C [Get Information Security Configuration Descriptor based on filter value]	The Information_Security_ Configuration_ID_Filter field is set to the Information Security Configuration ID provided by the Lower Tester.	An operand containing the Information Security Configuration record for the Information Security Configuration ID identified in the request.

Table 4.7: Get Information Security Configuration Descriptor test cases

- Test Procedure

  1. The Upper Tester sends a command to the IUT to write a Segmentation_Header field and Payload field containing the Get Information Security Configuration Descriptor opcode (0x0B) to the ACS Control Point with an operand with the Information_Security_Configuration_ID_Filter field set to <Information Security Configuration ID Filter value> as described in Table 4.7.
  2. The IUT sends an ATT_Write_Request to the ACS Control Point characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 1.
  3. The Lower Tester sends ATT_Handle_Value_Indication(s) of the ACS Control Point characteristic with the Segmentation_Header field and Payload field containing the Information Security Configuration Descriptor Response opcode (0x0C) and an operand with the <Response Operand> as described in Table 4.7.
  4. The IUT receives an ATT_Handle_Value_Indication(s) from the Lower Tester and reports it to the Upper Tester.
  5. For each indication, the IUT sends an ATT_Handle_Value_Confirmation on the ACS Control Point characteristic.
  6. Verify that the characteristic values meet the requirements of the service.

- Expected Outcome

  Pass verdict

  For each selected test case in Table 4.7, the IUT receives indication(s) from the Lower Tester of the ACS Control Point characteristic until all records of the Information Security Configuration record, identified by the Information Security Configuration ID Filter included in the request, have been sent and reports it to the Upper Tester.

  The Segmentation_Header field in all requests and responses includes the First Segment bit, Last Segment bit, and Rolling Segment Counter bits with appropriate values.

4.5.3 Get Key Descriptor

- Test Purpose

  Verify that, for each selected test case in Table 4.8, the IUT can perform the Get Key Descriptor procedure.

- Reference

  [3] 5.5.4.9

- Initial Condition

  - Perform the preamble described in Section 4.2.3 to configure the ACS Control Point characteristic.

- As provided by the Lower Tester, the Upper Tester knows the Key ID Filter value to be used by the IUT.

- Test Case Configuration

Test Case	Key ID Filter value	Response Operand
ACP/CL/ACSCP/BV-13-C [Get Key Descriptor]	The Key_ID_Filter field is set to no filtering (0xFFFF).	An operand containing one or more Key records.
ACP/CL/ACSCP/BV-14-C [Get Key Descriptor based on filter value]	The Key_ID_Filter field is set to the key ID provided by the Lower Tester.	An operand containing the Key record for the key ID identified in the request.

Table 4.8: Get Key Descriptor test cases

- Test Procedure

1. The Upper Tester sends a command to the IUT to write a Segmentation_Header field and Payload field containing the Get Key Descriptor opcode (0x0D) to the ACS Control Point with an operand with a key ID filter set to <Key ID Filter value> as described in Table 4.8.
2. The IUT sends an ATT_Write_Request to the ACS Control Point characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 1.
3. The Lower Tester sends ATT_Handle_Value_Indication(s) of the ACS Control Point characteristic with the Segmentation_Header field and Payload field containing the Key Descriptor Response opcode (0x0E) and an operand with the <Response Operand> as described in Table 4.8.
4. The IUT receives ATT_Handle_Value_Indication(s) from the Lower Tester and reports it to the Upper Tester.
5. For each indication, the IUT sends an ATT_Handle_Value_Confirmation on the ACS Control Point characteristic.
6. Verify that the characteristic values meet the requirements of the service.

- Expected Outcome

  Pass verdict

  For each selected test case in Table 4.8, the IUT receives indication(s) from the Lower Tester of the ACS Control Point characteristic until all records of the Key record, identified by the key ID filter included in the request, have been sent and reports it to the Upper Tester.

  The Segmentation_Header field in all requests and responses includes the First Segment bit, Last Segment bit, and Rolling Segment Counter bits with appropriate values.

ACP/CL/ACSCP/BV-15-C [Get Current Key List]

- Test Purpose

  Verify that the IUT can perform the Get Current Key List procedure.

- Reference

  [3] 5.5.4.10

- Initial Condition

  - Perform the preamble described in Section 4.2.3 to configure the ACS Control Point characteristic.

- Test Procedure

  1. The Upper Tester sends a command to the IUT to write a Segmentation_Header field and Payload field containing the Get Current Key List opcode (0x0F) to the ACS Control Point with no operand.
  2. The IUT sends an ATT_Write_Request to the ACS Control Point characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 1.
  3. The Lower Tester sends ATT_Handle_Value_Indication(s) of the ACS Control Point characteristic with the Segmentation_Header field and Payload field containing the Current Key List Response opcode (0x10) and an operand with the Number Of Key IDs and list of Key IDs for valid keys.
  4. The IUT receives ATT_Handle_Value_Indication(s) from the Lower Tester and reports it to the Upper Tester.
  5. For each indication, the IUT sends an ATT_Handle_Value_Confirmation on the ACS Control Point characteristic.
  6. Verify that the characteristic values meet the requirements of the service.

- Expected Outcome

  Pass verdict

  The IUT receives the Number Of Key IDs and list of Key IDs from the Lower Tester for valid keys confirming the Get Current Key List procedure requested and reports it to the Upper Tester.

  The Segmentation_Header field in all requests and responses includes the First Segment bit, Last Segment bit, and Rolling Segment Counter bits with appropriate values.

ACP/CL/ACSCP/BV-16-C [Invalidate All Established Security]

- Test Purpose

  Verify that the IUT can perform the Invalidate All Established Security procedure.

- Reference

  [3] 5.5.4.12

- Initial Condition

  - Perform the preamble described in Section 4.2.3 to configure the ACS Control Point characteristic.

- Test Procedure

  1. The Upper Tester sends a command to the IUT to write a Segmentation_Header field and Payload field containing the Invalidate All Established Security opcode (0x13) to the ACS Control Point with no operand.
  2. The IUT sends an ATT_Write_Request to the ACS Control Point characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 1.
  3. The Lower Tester sends an ATT_Handle_Value_Indication of the ACS Control Point characteristic with the Segmentation_Header field and Payload field containing the Response Code opcode (0x00) and an operand representing the Request_Opcode field (0x13) followed by the Response_Code_Value field set to Success (0x01).
  4. The IUT receives an ATT_Handle_Value_Indication from the Lower Tester and reports it to the Upper Tester.
  5. The IUT sends an ATT_Handle_Value_Confirmation on the ACS Control Point characteristic.
  6. Verify that the characteristic values meet the requirements of the service.

- Expected Outcome

  Pass verdict

  The IUT receives confirmation from the Lower Tester of the Invalidate All Established Security procedure requested and reports it to the Upper Tester.

  The Segmentation_Header field in all requests and responses includes the First Segment bit, Last Segment bit, and Rolling Segment Counter bits with appropriate values.

4.5.4 Invalidate Key

- Test Purpose

  Verify that, for each selected test case in Table 4.9, the IUT can perform the Invalidate Key procedure.

- Reference

  [3] 5.5.4.13

- Initial Condition

  - Perform the preamble described in Section 4.2.3 to configure the ACS Control Point characteristic.
  - As provided by the Lower Tester, the Upper Tester knows the Key ID value to be used by the IUT.

- Test Case Configuration

Test Case	Key ID value
ACP/CL/ACSCP/BV-17-C [Invalidate All Keys]	The Key_ID field is set to no filtering (0xFFFF).
ACP/CL/ACSCP/BV-18-C [Invalidate Key]	The Key_ID field is set to the Key ID provided by the Lower Tester.

Table 4.9: Invalidate Key test cases

- Test Procedure

  1. The Upper Tester sends a command to the IUT to write a Segmentation_Header field and Payload field containing the Invalidate Key opcode (0x14) to the ACS Control Point with an operand with a Key ID set to the <Key ID value> as described in Table 4.9.
  2. The IUT sends an ATT_Write_Request to the ACS Control Point characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 1.
  3. The Lower Tester sends an ATT_Handle_Value_Indication of the ACS Control Point characteristic with the Segmentation_Header field and Payload field containing the Response Code opcode (0x00) and an operand representing the Request_Opcode field (0x14) followed by the Response_Code_Value field set to Success (0x01).
  4. The IUT receives an ATT_Handle_Value_Indication from the Lower Tester and reports it to the Upper Tester.
  5. The IUT sends an ATT_Handle_Value_Confirmation on the ACS Control Point characteristic.
  6. Verify that the characteristic values meet the requirements of the service.

- Expected Outcome

  Pass verdict

  For each selected test case in Table 4.9, the IUT receives confirmation from the Lower Tester of the Invalidate Key procedure requested and reports it to the Upper Tester.

  The Segmentation_Header field in all requests and responses includes the First Segment bit, Last Segment bit, and Rolling Segment Counter bits with appropriate values.

ACP/CL/ACSCP/BV-19-C [Abort]

- Test Purpose

  Verify that the IUT can perform the Abort procedure.

- Reference

  [3] 5.5.4.14

- Initial Condition

  - Perform the preamble described in Section 4.2.3 to configure the ACS Control Point characteristic.
  - The Lower Tester has large descriptors that will take a few seconds to transmit.

- Test Procedure

  1. The Upper Tester sends a command to the IUT to write a Segmentation_Header field and Payload field containing the Get All Active Descriptors opcode (0x01) to the ACS Control Point with no operand.
  2. The IUT sends an ATT_Write_Request to the ACS Control Point characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 1.
  3. The Lower Tester starts to send indications of the ACS Control Point characteristic.
  4. The IUT receives one or more ATT_Handle_Value_Indication(s) from the Lower Tester and reports it to the Upper Tester.
  5. The Upper Tester sends a command to the IUT to write a Segmentation_Header field and Payload field containing the Abort opcode (0x15) to the ACS Control Point with no operand.
  6. The IUT sends an ATT_Write_Request to the ACS Control Point characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 5.
  7. The Lower Tester sends an ATT_Handle_Value_Indication of the ACS Control Point characteristic with the Segmentation_Header field and Payload field containing the Response Code opcode (0x00) and an operand representing the Request_Opcode field (0x15) followed by the Response_Code_Value field set to Success (0x01).
  8. The IUT receives an ATT_Handle_Value_Indication from the Lower Tester and reports it to the Upper Tester.
  9. The IUT sends an ATT_Handle_Value_Confirmation on the ACS Control Point characteristic.
  10. Verify that the characteristic values meet the requirements of the service.

- Expected Outcome

  Pass verdict

  The IUT receives some, but not all, of the active descriptors indications from the Lower Tester of the ACS Control Point characteristic.

The IUT receives an indication from the Lower Tester of the ACS Control Point characteristic, with the Response_Code_Value field set to Success (0x01), and reports it to the Upper Tester.

The Segmentation_Header field in all requests and responses includes the First Segment bit, Last Segment bit, and Rolling Segment Counter bits with appropriate values.

ACP/CL/ACSCP/BV-20-C [Set Security Controls Switch]

- Test Purpose

  Verify that the IUT can perform the Set Security Controls Switch procedure.

- Reference

  [3] 5.5.4.15

- Initial Condition

  - Perform the preamble described in Section 4.2.3 to configure the ACS Status and ACS Control Point characteristics.
  - The Lower Tester's Security Controls Switch bit, in the Status_Flags field of the ACS Status characteristic, is set to 1.

- Test Procedure

  1. The Upper Tester sends a command to the IUT to write a Segmentation_Header field and Payload field containing the Set Security Controls Switch opcode (0x16) to the ACS Control Point with an operand containing a Switch_State field set to 0.
  2. The IUT sends an ATT_Write_Request to the ACS Control Point characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 1.
  3. The Lower Tester sends an ATT_Handle_Value_Indication of the ACS Control Point characteristic with the Segmentation_Header field and Payload field containing the Response Code opcode (0x00) and an operand representing the Request_Opcode field (0x16) followed by the Response_Code_Value field set to Success (0x01).
  4. The IUT receives an ATT_Handle_Value_Indication from the Lower Tester and reports it to the Upper Tester.
  5. The IUT sends an ATT_Handle_Value_Confirmation on the ACS Control Point characteristic.
  6. The Lower Tester sends an ATT_Handle_Value_Indication of the ACS Status characteristic.
  7. The IUT receives an ATT_Handle_Value_Indication from the Lower Tester and reports it to the Upper Tester.
  8. The IUT sends an ATT_Handle_Value_Confirmation on the ACS Status characteristic.
  9. Verify that the characteristic values meet the requirements of the service.

- Expected Outcome

  Pass verdict

  The IUT receives indication from the Lower Tester of the ACS Status characteristic with the Status_Flags field Security Controls Switch bit set to 0 and reports it to the Upper Tester.

  The IUT receives confirmation from the Lower Tester of the Set Security Controls Switch procedure requested and reports it to the Upper Tester.

  The Segmentation_Header field in all requests and responses includes the First Segment bit, Last Segment bit, and Rolling Segment Counter bits with appropriate values.

ACP/CL/ACSCP/BV-21-C [Get Key URI]

- Test Purpose

  Verify that the IUT can perform the Get Key URI procedure.

- Reference

  [3] 5.5.4.16

- Initial Condition

  - Perform the preamble described in Section 4.2.3 to configure the ACS Control Point characteristic.
  - The Upper Tester sends a command to the IUT to request the Get Key Descriptor procedure using the ACS Control Point characteristic to acquire the key ID of the key with URI.

- Test Procedure

  1. The Upper Tester sends a command to the IUT to write a Segmentation_Header field and Payload field containing the Get Key URI opcode (0x17) to the ACS Control Point with an operand with the Key ID.
  2. The IUT sends an ATT_Write_Request to the ACS Control Point characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 1.
  3. The Lower Tester sends ATT_Handle_Value_Indication(s) of the ACS Control Point characteristic with the Segmentation_Header field and Payload field containing the Key URI Response opcode (0x18) and an operand with the Key ID and Key URI.
  4. The IUT receives ATT_Handle_Value_Indication(s) from the Lower Tester and reports it to the Upper Tester.
  5. For each indication, the IUT sends an ATT_Handle_Value_Confirmation on the ACS Control Point characteristic.
  6. Verify that the characteristic values meet the requirements of the service.

- Expected Outcome

  Pass verdict

  The IUT receives the Key ID and Key URI from the Lower Tester of the Get Key URI procedure requested and reports it to the Upper Tester.

  The Segmentation_Header field in all requests and responses includes the First Segment bit, Last Segment bit, and Rolling Segment Counter bits with appropriate values.

ACP/CL/ACSCP/BV-22-C [Get ACS Feature]

- Test Purpose

  Verify that the IUT can perform the Get ACS Feature procedure.

- Reference

  [3] 5.5.4.17

- Initial Condition

  - Perform the preamble described in Section 4.2.3 to configure the ACS Control Point characteristic.

- Test Procedure

  1. The Upper Tester sends a command to the IUT to write a Segmentation_Header field and Payload field containing the Get ACS Feature opcode (0x19) to the ACS Control Point with no operand.
  2. The IUT sends an ATT_Write_Request to the ACS Control Point characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 1.
  3. The Lower Tester sends ATT_Handle_Value_Indication(s) of the ACS Control Point characteristic with the Segmentation_Header field and Payload field containing the ACS Feature Response opcode (0x1A) and an operand comprising all the mandatory fields.
  4. The IUT receives ATT_Handle_Value_Indication(s) from the Lower Tester and reports it to the Upper Tester.
  5. For each indication, the IUT sends an ATT_Handle_Value_Confirmation on the ACS Control Point characteristic.
  6. Verify that the characteristic values meet the requirements of the service.

- Expected Outcome

  Pass verdict

  The IUT receives confirmation from the Lower Tester of the Get ACS Feature procedure requested and reports it to the Upper Tester.

  The Segmentation_Header field in all requests and responses includes the First Segment bit, Last Segment bit, and Rolling Segment Counter bits with appropriate values.

ACP/CL/ACSCP/BV-23-C [OOB key exchange]

- Test Purpose

  Verify that the IUT can perform the Key Exchange ECDH procedures with a key ID that references an OOB key.

- Reference

  [3] 5.5.4.18.1

- Initial Condition

  - Perform the preamble described in Section 4.2.3 to configure the ACS Control Point characteristic.
  - The Upper Tester sends a command to the IUT to request the Get ACS Feature procedure using the ACS Control Point characteristic to acquire the Lower Tester's OOB key exchange capabilities, confirmation Static OOB number capabilities, confirmation input and output OOB number maximum value, and confirmation input and output OOB number capabilities.
  - The OOB key is defined by TSPX_key_oob_value in [9], or the Upper Tester sends a command to the IUT to request the Get Key URI procedure, using the ACS Control Point characteristic, to acquire the key URI for the requested key ID.
  - The Upper Tester sends a command to the IUT to request the Get Key Descriptor procedure using the ACS Control Point characteristic to acquire the key records (e.g., OOB Key Exchange record, the Nonce_Type field value). If the Nonce_Type field value, for the selected key ID in the security algorithm additional parameters, is Sequence Number Different Fixed Parts, then the Upper Tester sends a command to the IUT to request the Set AC Client Nonce Fixed procedure using the ACS Control Point characteristic to have a nonce set.

- Test Procedure

1. The Upper Tester sends a command to the IUT to write a Segmentation_Header field and Payload field containing the Start Key Exchange opcode (0x11) to the ACS Control Point characteristic with an operand with the Key ID, for the OOB key to be exchanged, and how the exchanged key is to be confirmed.
2. The IUT sends an ATT_Write_Request to the ACS Control Point characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 1.
3. The Lower Tester sends an ATT_Handle_Value_Indication of the ACS Control Point characteristic with the Segmentation_Header field and Payload field containing the Response Code opcode (0x00) and an operand with the Request_Opcode field set to Start Key Exchange (0x11) and the Response_Code_Value field set to Success (0x01).
4. The IUT receives an ATT_Handle_Value_Indication from the Lower Tester and reports it to the Upper Tester.
5. The IUT sends an ATT_Handle_Value_Confirmation on the ACS Control Point characteristic.
6. The Upper Tester sends a command to the IUT to write Segmentation_Header and Payload fields to send the Key Exchange ECDH opcode (0x1B) to the ACS Control Point characteristic with an operand with the Key ID used in step 1, and the AC Client Public Key of the IUT.
7. The IUT sends ATT_Write_Requests to the ACS Control Point characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 6. The exact number of ATT_Write_Requests depends on the payload size.
8. The Lower Tester sends ATT_Handle_Value_Indication(s) of the ACS Control Point characteristic with the Segmentation_Header field and Payload field containing the Response Code opcode (0x00) and an operand with the Request_Opcode field set to Key Exchange ECDH (0x1B) and the Response_Code_Value field set to Success (0x01).
9. The IUT receives ATT_Handle_Value_Indication(s) from the Lower Tester and reports it to the Upper Tester.
10. For each indication, the IUT sends an ATT_Handle_Value_Confirmation on the ACS Control Point characteristic.
11. The Upper Tester sends a command to the IUT to write a Segmentation_Header field and Payload field containing the Key Exchange KDF opcode (0x21) and an operand containing the Key ID used in step 1.
12. The IUT sends an ATT_Write_Request to the ACS Control Point characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 11.
13. The Lower Tester sends ATT_Handle_Value_Indication(s) of the ACS Control Point characteristic with the Segmentation_Header field and Payload field containing the Key Exchange KDF Response opcode (0x22) and an operand containing the Key ID used in step 1, KDF Salt size and value, and KDF Info size and value.
14. The IUT receives ATT_Handle_Value_Indication(s) from the Lower Tester and reports it to the Upper Tester.
15. For each indication, the IUT sends an ATT_Handle_Value_Confirmation on the ACS Control Point characteristic.
16. The Lower Tester and the IUT exchange the OOB random number described in the start key exchange request, and the IUT reports the OOB random number to the Upper Tester.
17. The Upper Tester sends a command to the IUT to write Segmentation_Header and Payload fields to send the Key Exchange ECDH Confirmation Code opcode (0x1D) to the ACS Control Point characteristic with an operand with the Key ID used in step 1, and the AC Client Confirmation Code of the IUT.
18. The IUT sends two ATT_Write_Requests to the ACS Control Point characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 17.

19. The Lower Tester sends ATT_Handle_Value_Indication(s) of the ACS Control Point characteristic with the Segmentation_Header field and Payload field containing the Key Exchange ECDH Confirmation Code Response opcode (0x1E) and an operand with the Key ID used in step 1, and the AC Server Confirmation Code of the Lower Tester.
20. The IUT receives ATT_Handle_Value_Indication(s) from the Lower Tester and reports it to the Upper Tester.
21. For each indication, the IUT sends an ATT_Handle_Value_Confirmation on the ACS Control Point characteristic.
22. The Upper Tester sends a command to the IUT to write Segmentation_Header and Payload fields to send the Key Exchange ECDH Confirmation Random Number opcode (0x1F) to the ACS Control Point characteristic with an operand with the Key ID used in step 1, and the AC Client Confirmation Random Number of the IUT.
23. The IUT sends two ATT_Write_Requests to the ACS Control Point characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 22.
24. The Lower Tester sends ATT_Handle_Value_Indication(s) of the ACS Control Point characteristic with the Segmentation_Header field and Payload field containing the Key Exchange ECDH Confirmation Random Number Response opcode (0x20) and an operand with the Key ID used in step 1, and the AC Server Confirmation Random Number of the Lower Tester.
25. The IUT receives ATT_Handle_Value_Indication(s) from the Lower Tester and reports it to the Upper Tester.
26. For each indication, the IUT sends an ATT_Handle_Value_Confirmation on the ACS Control Point characteristic.
27. The Lower Tester sends an ATT_Handle_Value_Indication of the ACS Control Point characteristic with the Segmentation_Header field and Payload field containing the Key Exchange Response opcode (0x12) and an operand with the Key ID used in step 1, and the key exchange result.
28. The IUT receives an ATT_Handle_Value_Indication from the Lower Tester and reports it to the Upper Tester.
29. The IUT sends an ATT_Handle_Value_Confirmation on the ACS Control Point characteristic.
30. Verify that the characteristic value meets the requirements of the service.

- Expected Outcome

  Pass verdict

  The IUT sends a write request to the ACS Control Point characteristic with the Start Key Exchange opcode (0x11) and an operand comprising the Key ID, for the OOB key to be exchanged, and how the exchanged key is to be confirmed.

  The IUT receives indication(s) from the Lower Tester on the ACS Control Point characteristic with the Response_Code_Value field set to Success (0x01) and reports it to the Upper Tester.

  The IUT sends write requests to the ACS Control Point characteristic with the Key Exchange ECDH opcode (0x1B) and an operand comprising the Key ID used in step 1, and the AC Client Public Key of the IUT.

  The IUT receives indication(s) from the Lower Tester on the ACS Control Point characteristic with the Response_Code_Value field set to Success (0x01).

  The IUT sends a write request to the ACS Control Point characteristic with the Key Exchange KDF opcode (0x21) and an operand containing the Key ID used in step 1.

  The IUT receives indication(s) from the Lower Tester on the ACS Control Point characteristic with the Key Exchange KDF Response opcode (0x22) and an operand containing the Key ID used in step 1, and the expected values for the KDF Salt size and value, and KDF Info size and value.

The IUT sends write requests to the ACS Control Point characteristic with the Key Exchange ECDH Confirmation Code opcode (0x1D) and an operand comprising the Key ID used in step 1, and the AC Client Confirmation Code of the IUT.

The IUT receives indication(s) from the Lower Tester of the ACS Control Point characteristic with the Key Exchange ECDH Confirmation Code Response opcode (0x1E) and an operand comprising the Key ID used in step 1, and the AC Server Confirmation Code of the Lower Tester.

The IUT sends write requests to the ACS Control Point characteristic with the Key Exchange ECDH Confirmation Random Number opcode (0x1F) and an operand comprising the Key ID used in step 1, and the AC Client Confirmation Random Number of the IUT.

The IUT receives indication(s) from the Lower Tester of the ACS Control Point characteristic with the Key Exchange ECDH Confirmation Random Number Response opcode (0x20) and an operand comprising the Key ID used in step 1, and the AC Server Confirmation Random number of the Lower Tester.

The IUT receives indication(s) from the Lower Tester of the ACS Control Point characteristic with the Key Exchange Response opcode (0x12) and an operand comprising the key ID used in step 1, and the Response_Code field value of Key Exchange Successful (0x00) and reports it to the Upper Tester.

The Segmentation_Header field in all requests and responses includes the First Segment bit, Last Segment bit, and Rolling Segment Counter bits with appropriate values.

ACP/CL/ACSCP/BV-24-C [ECDH key exchange]

- Test Purpose

  Verify that the IUT can perform the Key Exchange ECDH procedures with a key ID that references an ECDH key.

- Reference

  [3] 5.5.4.18.1

- Initial Condition

  - Perform the preamble described in Section 4.2.3 to configure the ACS Control Point characteristic.
  - The Upper Tester sends a command to the IUT to request the Get ACS Feature procedure using the ACS Control Point characteristic to acquire the Lower Tester’s input and output capabilities.
  - The Upper Tester sends a command to the IUT to request the Get Key Descriptor procedure using the ACS Control Point characteristic to acquire the key records (e.g., the ECDH Key Exchange record, the Nonce_Type field value). If the Nonce_Type field value, for the selected key ID in the security algorithm’s additional parameters, is Sequence Number Different Fixed Parts, then the Upper Tester sends a command to the IUT to request that the Set AC Client Nonce Fixed procedure using the ACS Control Point characteristic have a nonce set.

- Test Procedure

  1. The Upper Tester sends a command to the IUT to write a Segmentation_Header field and Payload field containing the Start Key Exchange opcode (0x11) to the ACS Control Point characteristic with an operand with the Key ID, for the ECDH key to be exchanged, and how the exchanged key is to be confirmed.
  2. The IUT sends an ATT_Write_Request to the ACS Control Point characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 1.

3. The Lower Tester sends an ATT_Handle_Value_Indication of the ACS Control Point characteristic with the Segmentation_Header field and Payload field containing the Response Code opcode (0x00) and an operand with the Request_Opcode field set to Start Key Exchange (0x11) and the Response_Code_Value field set to Success (0x01).
4. The IUT receives an ATT_Handle_Value_Indication from the Lower Tester and reports it to the Upper Tester.
5. The IUT sends an ATT_Handle_Value_Confirmation on the ACS Control Point characteristic.
6. The Upper Tester sends a command to the IUT to write Segmentation_Header and Payload fields to send the Key Exchange ECDH opcode (0x1B) to the ACS Control Point characteristic with an operand with the Key ID used in step 1, and the AC Client Public Key of the IUT.
7. The IUT sends ATT_Write_Requests to the ACS Control Point characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 6. The exact number of ATT_Write_Requests depends on the payload size.
8. The Lower Tester sends ATT_Handle_Value_Indication(s) of the ACS Control Point characteristic with the Segmentation_Header field and Payload field containing the Key Exchange ECDH Response opcode (0x1C) and an operand with the Key ID used in step 1, and the AC Server Public Key of the Lower Tester.
9. The IUT receives ATT_Handle_Value_Indication(s) from the Lower Tester and reports it to the Upper Tester.
10. For each indication, the IUT sends an ATT_Handle_Value_Confirmation on the ACS Control Point characteristic.
11. The Upper Tester sends a command to the IUT to write a Segmentation_Header field and Payload field containing the Key Exchange KDF opcode (0x21) and an operand containing the Key ID used in step 1.
12. The IUT sends an ATT_Write_Request to the ACS Control Point characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 11.
13. The Lower Tester sends ATT_Handle_Value_Indication(s) of the ACS Control Point characteristic with the Segmentation_Header field and Payload field containing the Key Exchange KDF Response opcode (0x22) and an operand containing the Key ID used in step 1, KDF Salt size and value, and KDF Info size and value.
14. The IUT receives ATT_Handle_Value_Indication(s) from the Lower Tester and reports it to the Upper Tester.
15. For each indication, the IUT sends an ATT_Handle_Value_Confirmation on the ACS Control Point characteristic.
16. The Lower Tester and the IUT exchange the OOB random number as described in the start key exchange request, and the IUT reports the OOB random number to the Upper Tester.
17. The Upper Tester sends a command to the IUT to write Segmentation_Header and Payload fields to send the Key Exchange ECDH Confirmation Code opcode (0x1D) to the ACS Control Point characteristic with an operand with the Key ID used in step 1, and the AC Client Confirmation Code of the IUT.
18. The IUT sends two ATT_Write_Requests to the ACS Control Point characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 17.
19. The Lower Tester sends ATT_Handle_Value_Indication(s) of the ACS Control Point characteristic with the Segmentation_Header field and Payload field containing the Key Exchange ECDH Confirmation Code Response opcode (0x1E) and an operand with the Key ID used in step 1, and the AC Server Confirmation Code of the Lower Tester.
20. The IUT receives an ATT_Handle_Value_Indication from the Lower Tester and reports it to the Upper Tester.
21. For each indication, the IUT sends an ATT_Handle_Value_Confirmation on the ACS Control Point characteristic.

22. The Upper Tester sends a command to the IUT to write Segmentation_Header and Payload fields to send the Key Exchange ECDH Confirmation Random Number opcode (0x1F) to the ACS Control Point characteristic with an operand with the Key ID used in step 1, and the AC Client Confirmation Random Number of the IUT.
23. The IUT sends two ATT_Write_Requests to the ACS Control Point characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 22.
24. The Lower Tester sends ATT_Handle_Value_Indication(s) of the ACS Control Point characteristic with the Segmentation_Header field and Payload field containing the Key Exchange ECDH Confirmation Random Number Response opcode (0x20) and an operand with the Key ID used in step 1, and the AC Server Confirmation Random Number of the Lower Tester.
25. The IUT receives an ATT_Handle_Value_Indication from the Lower Tester and reports it to the Upper Tester.
26. For each indication, the IUT sends an ATT_Handle_Value_Confirmation on the ACS Control Point characteristic.
27. The Lower Tester sends an ATT_Handle_Value_Indication of the ACS Control Point characteristic with the Segmentation_Header field and Payload field containing the Key Exchange Response opcode (0x12) and an operand with the Key ID used in step 1, and the key exchange result.
28. The IUT receives an ATT_Handle_Value_Indication from the Lower Tester and reports it to the Upper Tester.
29. The IUT sends an ATT_Handle_Value_Confirmation on the ACS Control Point characteristic.
30. Verify that the characteristic value meets the requirements of the service.

- Expected Outcome

  Pass verdict

  The IUT sends write requests to the ACS Control Point characteristic with the Key Exchange ECDH opcode (0x1B) and an operand comprising the Key ID, for the ECDH key to be exchanged, and the AC Client Public Key of the IUT.

  The IUT receives indication(s) from the Lower Tester on the ACS Control Point characteristic with the Key Exchange ECDH Response opcode (0x1C) and an operand comprising the Key ID used in step 1, and the AC Server Public Key of the Lower Tester.

  The IUT sends a write request to the ACS Control Point characteristic with the Key Exchange KDF opcode (0x21) and an operand containing the Key ID used in step 1.

  The IUT receives indication(s) from the Lower Tester on the ACS Control Point characteristic with the Key Exchange KDF Response opcode (0x22) and an operand containing the Key ID used in step 1, and the expected values for the KDF Salt size and value, and KDF Info size and value.

  The IUT sends write requests to the ACS Control Point characteristic with the Key Exchange ECDH Confirmation Code opcode (0x1D) and an operand comprising the Key ID used in step 1, and the AC Client Confirmation Code of the IUT.

  The IUT receives indication(s) from the Lower Tester of the ACS Control Point characteristic with the Key Exchange ECDH Confirmation Code Response opcode (0x1E) and an operand comprising the Key ID used in step 1, and the AC Server Confirmation Code of the Lower Tester.

  The IUT sends write requests to the ACS Control Point characteristic with the Key Exchange ECDH Confirmation Random Number opcode (0x1F) and an operand comprising the Key ID used in step 1, and the AC Client Confirmation Random Number of the IUT.

  The IUT receives indication(s) from the Lower Tester of the ACS Control Point characteristic with the Key Exchange ECDH Confirmation Random Number Response opcode (0x20) and an operand

comprising the Key ID used in step 1, and the AC Server Confirmation Random Number of the Lower Tester.

The IUT receives indication(s) from the Lower Tester of the ACS Control Point characteristic with the Key Exchange Response opcode (0x12) and an operand comprising the key ID used in step 1, and the Response_Code field value of Key Exchange Successful (0x00) and reports it to the Upper Tester.

The Segmentation_Header field in all requests and responses includes the First Segment bit, Last Segment bit, and Rolling Segment Counter bits with appropriate values.

ACP/CL/ACSCP/BV-25-C [KDF key exchange]

- Test Purpose

  Verify that the IUT can perform a KDF key exchange.

- Reference

  [3] 5.5.4.18.2

- Initial Condition

  - Perform the preamble described in Section 4.2.3 to configure the ACS Control Point characteristic.
  - The Upper Tester and the IUT have exchanged the higher-level parent key (e.g., OOB key, ECDH key, KDF key, or manufacturer-specific type) so that the lower-level child key can be derived.
  - The Upper Tester sends a command to the IUT to request the Get Key Descriptor procedure using the ACS Control Point characteristic to acquire the key records (e.g., the KDF Key Exchange record, the Nonce_Type field value). If the Nonce_Type field value, for the selected key ID in the security algorithm's additional parameters, is Sequence Number Different Fixed Parts, then the Upper Tester sends a command to the IUT to request that the Set AC Client Nonce Fixed procedure using the ACS Control Point characteristic have a nonce set.

- Test Procedure

  1. The Upper Tester sends a command to the IUT to write a Segmentation_Header field and Payload field containing the Start Key Exchange opcode (0x11) to the ACS Control Point characteristic with an operand with the Key ID, for the KDF key to be exchanged, the Selected_Confirmation_Method field set to No Confirmation OOB Method Used, and the Selected_Confirmation_Action field set to 0xFF (i.e., no user action nor static confirmation).
  2. The IUT sends an ATT_Write_Request to the ACS Control Point characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 1.
  3. The Lower Tester sends an ATT_Handle_Value_Indication of the ACS Control Point characteristic with the Segmentation_Header field and Payload field containing the Response Code opcode (0x00) and an operand with the Request_Opcode field set to Start Key Exchange (0x11) and the Response_Code_Value field set to Success (0x01).
  4. The IUT receives an ATT_Handle_Value_Indication from the Lower Tester and reports it to the Upper Tester.
  5. The IUT sends an ATT_Handle_Value_Confirmation on the ACS Control Point characteristic.
  6. The Upper Tester sends a command to the IUT to write a Segmentation_Header field and Payload field containing the Key Exchange KDF opcode (0x21) and an operand containing the key ID used in step 1.

7. The IUT sends an ATT_Write_Request to the ACS Control Point characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 6.
8. The Lower Tester sends ATT_Handle_Value_Indication(s) of the ACS Control Point characteristic with the Segmentation_Header field and Payload field containing the Key Exchange KDF Response opcode (0x22) and an operand containing the key ID used in step 1, KDF Salt size and value, and KDF Info size and value.
9. The IUT receives ATT_Handle_Value_Indication(s) from the Lower Tester and reports it to the Upper Tester.
10. For each indication, the IUT sends an ATT_Handle_Value_Confirmation on the ACS Control Point characteristic.
11. The Lower Tester sends an ATT_Handle_Value_Indication of the ACS Control Point characteristic with the Segmentation_Header field and Payload field containing the Key Exchange Response opcode (0x12) and an operand with the Key ID used in step 1, and the key exchange result.
12. The IUT receives an ATT_Handle_Value_Indication from the Lower Tester and reports it to the Upper Tester.
13. The IUT sends an ATT_Handle_Value_Confirmation on the ACS Control Point characteristic.
14. Verify that the characteristic value meets the requirements of the service.

- Expected Outcome

  Pass verdict

  The IUT sends a write request to the ACS Control Point characteristic with the Key Exchange KDF opcode (0x21) and an operand containing the Key ID for the KDF key to be exchanged.

  The IUT receives indication(s) from the Lower Tester on the ACS Control Point characteristic with the Key Exchange KDF Response opcode (0x22) and an operand containing the Key ID used in step 1, KDF Salt size and value, and KDF Info size and value.

  The IUT receives indication(s) from the Lower Tester of the ACS Control Point characteristic with the Key Exchange Response opcode (0x12) and an operand comprising the Key ID used in step 1, and the Response_Code field value of Key Exchange Successful (0x00) and reports it to the Upper Tester.

  The Segmentation_Header field in all requests and responses includes the First Segment bit, Last Segment bit, and Rolling Segment Counter bits with appropriate values.

ACP/CL/ACSCP/BV-26-C [Set AC Client Nonce Fixed]

- Test Purpose

  Verify that the IUT can perform the Set AC Client Nonce Fixed procedure.

- Reference

  [3] 5.5.4.19

- Initial Condition

  - Perform the preamble described in Section 4.2.3 to configure the ACS Control Point characteristic.
  - The Upper Tester sends a command to the IUT to request the Get Key Descriptor procedure using the ACS Control Point characteristic to acquire the key records (e.g., Key_ID and Nonce_Fixed_Size).

- Test Procedure

  1. The Upper Tester sends a command to the IUT to write a Segmentation_Header field and Payload field containing the Set AC Client Nonce Fixed opcode (0x23) to the ACS Control Point with an operand containing the Key ID and AC Client Nonce Fixed Value.
  2. The IUT sends an ATT_Write_Request to the ACS Control Point characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 1.
  3. The Lower Tester sends an ATT_Handle_Value_Indication of the ACS Control Point characteristic with the Segmentation_Header field and Payload field containing the Response Code opcode (0x00) and an operand representing the Request_Opcode field (0x23) followed by the Response_Code_Value field set to Success (0x01).
  4. The IUT receives an ATT_Handle_Value_Indication from the Lower Tester and reports it to the Upper Tester.
  5. The IUT sends an ATT_Handle_Value_Confirmation on the ACS Control Point characteristic.
  6. Verify that the characteristic values meet the requirements of the service.

- Expected Outcome

  Pass verdict

  The IUT receives an indication from the Lower Tester of the ACS Control Point characteristic, with the Response_Code_Value field set to Success (0x01), and reports it to the Upper Tester.

  The Segmentation_Header field in all requests and responses includes the First Segment bit, Last Segment bit, and Rolling Segment Counter bits with appropriate values.

ACP/CL/ACSCP/BV-27-C [Get ATT_MTU]

- Test Purpose

  Verify that the IUT can perform the Get ATT_MTU procedure.

- Reference

  [3] 5.5.4.20

- Initial Condition

  - Perform the preamble described in Section 4.2.3 to configure the ACS Control Point characteristic.

- Test Procedure

  1. The Upper Tester sends a command to the IUT to write a Segmentation_Header field and Payload field containing the Get ATT_MTU opcode (0xDD) to the ACS Control Point with no operand.
  2. The IUT sends an ATT_Write_Request to the ACS Control Point characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 1.
  3. The Lower Tester sends an ATT_Handle_Value_Indication of the ACS Control Point characteristic with the Segmentation_Header field and Payload field containing the ATT_MTU Response opcode (0xDE) and an operand with the ATT_MTU size value.
  4. The IUT receives an ATT_Handle_Value_Indication from the Lower Tester and reports it to the Upper Tester.
  5. The IUT sends an ATT_Handle_Value_Confirmation on the ACS Control Point characteristic.
  6. Verify that the characteristic values meet the requirements of the service.

- Expected Outcome

  Pass verdict

  The IUT receives confirmation from the Lower Tester of the Get ATT_MTU procedure requested and reports it to the Upper Tester.

  The Segmentation_Header field in all requests and responses includes the First Segment bit, Last Segment bit, and Rolling Segment Counter bits with appropriate values.

ACP/CL/ACSCP/BV-28-C [Initiate Pairing]

- Test Purpose

  Verify that the IUT can perform the Initiate Pairing procedure.

- Reference

  [3] 5.5.4.21

- Initial Condition

  - Perform the preamble described in Section 4.2.3 to configure the ACS Control Point characteristic.

- Test Procedure

  1. The Upper Tester sends a command to the IUT to write a Segmentation_Header field and Payload field containing the Initiate Pairing opcode (0xDF) to the ACS Control Point with no operand.
  2. The IUT sends an ATT_Write_Request to the ACS Control Point characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 1.
  3. The Lower Tester sends an ATT_Handle_Value_Indication of the ACS Control Point characteristic with the Segmentation_Header field and Payload field containing the Response Code opcode (0x00) and an operand representing the Request_Opcode field (0xDF) followed by the Response_Code_Value field set to Success (0x01).
  4. The IUT receives an ATT_Handle_Value_Indication from the Lower Tester and reports it to the Upper Tester.
  5. The IUT sends an ATT_Handle_Value_Confirmation on the ACS Control Point characteristic.
  6. Verify that the characteristic values meet the requirements of the service.

- Expected Outcome

  Pass verdict

  The IUT receives confirmation from the Lower Tester of the Initiate Pairing procedure requested and reports it to the Upper Tester.

  The Segmentation_Header field in all requests and responses includes the First Segment bit, Last Segment bit, and Rolling Segment Counter bits with appropriate values.

4.5.5 ACS Control Point: Error Handling

Verify the appropriate operation of the IUT when an ACS Control Point error is received from the AC Server (Lower Tester).

ACP/CL/ACSCP/BI-01-C [Opcode not supported]

- Test Purpose

  Verify that the IUT responds appropriately when it receives an Opcode Not Supported ACS Control Point Response Code Value.

- Reference

  [3] 5.5.4.23

- Initial Condition

  - Perform the preamble described in Section 4.2.3 to configure the ACS Control Point characteristic.
  - The Lower Tester does not support descriptors.

- Test Procedure

  1. The Upper Tester sends a command to the IUT to write a Segmentation_Header field and Payload field containing the Get All Active Descriptors opcode (0x01) to the ACS Control Point with no operand.
  2. The IUT sends an ATT_Write_Request to the ACS Control Point characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 1.
  3. The Lower Tester sends an ATT_Handle_Value_Indication of the ACS Control Point characteristic with the Segmentation_Header field and Payload field containing the Response Code opcode (0x00) and an operand representing the Request_Opcode field (0x01) followed by the Response_Code_Value field set to Opcode Not Supported (0x02).
  4. The IUT receives an ATT_Handle_Value_Indication from the Lower Tester and reports it to the Upper Tester.
  5. The IUT sends an ATT_Handle_Value_Confirmation on the ACS Control Point characteristic.
  6. Verify that the IUT returns to a stable state and can process commands normally.

- Expected Outcome

  Pass verdict

  The IUT receives the Response Code Value of Opcode Not Supported (0x02) from the Lower Tester and reports it to the Upper Tester.

  The Segmentation_Header field in all requests and responses includes the First Segment bit, Last Segment bit, and Rolling Segment Counter bits with appropriate values.

ACP/CL/ACSCP/BI-02-C [Procedure not completed]

- Test Purpose

  Verify that the IUT responds appropriately when it receives a Procedure Not Completed ACS Control Point Response Code Value.

- Reference

  [3] 5.5.4.2, 5.5.4.23

- Initial Condition
  - Perform the preamble described in Section 4.2.3 to configure the ACS Control Point characteristic.
- Test Procedure
  1. The Upper Tester sends a command to the IUT to write a Segmentation_Header field and Payload field containing the Get All Active Descriptors opcode (0x01) to the ACS Control Point with no operand.
  2. The IUT sends an ATT_Write_Request to the ACS Control Point characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 1.
  3. The Lower Tester sends an ATT_Handle_Value_Indication of the ACS Control Point characteristic with the Segmentation_Header field and Payload field containing the Response Code opcode (0x00) and an operand representing the Request_Opcode field (0x01) followed by the Response_Code_Value field set to Procedure Not Completed (0x04).
  4. The IUT receives an ATT_Handle_Value_Indication from the Lower Tester and reports it to the Upper Tester.
  5. The IUT sends an ATT_Handle_Value_Confirmation on the ACS Control Point characteristic.
  6. Verify that the IUT returns to a stable state and can process commands normally.
- Expected Outcome

  Pass verdict

  The IUT receives the Response Code Value of Procedure Not Completed (0x04) from the Lower Tester and reports it to the Upper Tester.

  The Segmentation_Header field in all requests and responses includes the First Segment bit, Last Segment bit, and Rolling Segment Counter bits with appropriate values.

ACP/CL/ACSCP/BI-03-C [Parameter out of range]

- Test Purpose

  Verify that the IUT responds appropriately when it receives a Parameter Out Of Range ACS Control Point Response Code Value.
- Reference

  [3] 5.5.4.3, 5.5.4.23
- Initial Condition
  - Perform the preamble described in Section 4.2.3 to configure the ACS Control Point characteristic.
  - The Upper Tester sends a command to the IUT to request the Get Restriction Map ID List procedure using the ACS Control Point characteristic to acquire the available restriction map IDs.
- Test Procedure
  1. The Upper Tester sends a command to the IUT to write a Segmentation_Header field and Payload field containing the Get Restriction Map Descriptor opcode (0x02) to the ACS Control Point with an operand with the Restriction_Map_ID field set to a restriction map ID that is not available on the Lower Tester and no filter by resource handle (0xFFFF).
  2. The IUT sends an ATT_Write_Request to the ACS Control Point characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 1.

3. The Lower Tester sends an ATT_Handle_Value_Indication of the ACS Control Point characteristic with the Segmentation_Header field and Payload field containing the Response Code opcode (0x00) and an operand representing the Request_Opcode field (0x02) followed by the Response_Code_Value field set to Parameter Out Of Range (0x05).
4. The IUT receives an ATT_Handle_Value_Indication from the Lower Tester and reports it to the Upper Tester.
5. The IUT sends an ATT_Handle_Value_Confirmation on the ACS Control Point characteristic.
6. Verify that the IUT returns to a stable state and can process commands normally.

- Expected Outcome

  Pass verdict

  The IUT receives the Response Code Value of Parameter Out Of Range (0x05) from the Lower Tester and reports it to the Upper Tester.

  The Segmentation_Header field in all requests and responses includes the First Segment bit, Last Segment bit, and Rolling Segment Counter bits with appropriate values.

ACP/CL/ACSCP/BI-04-C [Procedure not applicable]

- Test Purpose

  Verify that the IUT responds appropriately when it receives a Procedure Not Applicable ACS Control Point Response Code Value.

- Reference

  [3] 5.5.4.14, 5.5.4.23

- Initial Condition

  - Perform the preamble described in Section 4.2.3 to configure the ACS Control Point characteristic.

- Test Procedure

1. The Upper Tester sends a command to the IUT to write a Segmentation_Header field and Payload field containing the Abort opcode (0x15) to the ACS Control Point with no operand.
2. The IUT sends an ATT_Write_Request to the ACS Control Point characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 1.
3. The Lower Tester sends an ATT_Handle_Value_Indication of the ACS Control Point characteristic with the Segmentation_Header field and Payload field containing the Response Code opcode (0x00) and an operand representing the Request_Opcode field (0x15) followed by the Response_Code_Value field set to Procedure Not Applicable (0x06).
4. The IUT receives an ATT_Handle_Value_Indication from the Lower Tester and reports it to the Upper Tester.
5. The IUT sends an ATT_Handle_Value_Confirmation on the ACS Control Point characteristic.
6. Verify that the IUT returns to a stable state and can process commands normally.

- Expected Outcome

  Pass verdict

  The IUT receives the Response Code Value of Procedure Not Applicable (0x06) from the Lower Tester and reports it to the Upper Tester.

  The Segmentation_Header field in all requests and responses includes the First Segment bit, Last Segment bit, and Rolling Segment Counter bits with appropriate values.

ACP/CL/ACSCP/BI-05-C [No records found]

- Test Purpose

  Verify that the IUT responds appropriately when it receives a No Records Found ACS Control Point Response Code Value.

- Reference

  [3] 5.5.4.3, 5.5.4.23

- Initial Condition

  - Perform the preamble described in Section 4.2.3 to configure the ACS Control Point characteristic.
  - The Upper Tester sends a command to the IUT to request the Get Restriction Map ID List procedure using the ACS Control Point characteristic to acquire the available restriction map IDs.
  - The Upper Tester sends a command to the IUT to request the Get Restriction Map Descriptor procedure using the ACS Control Point characteristic to acquire the Resource Handles of resources that have a record in the restriction map.

- Test Procedure

  1. The Upper Tester sends a command to the IUT to write a Segmentation_Header field and Payload field containing the Get Restriction Map Descriptor opcode (0x02) to the ACS Control Point with an operand with the Restriction_Map_ID field set to a value of an available restriction map and the Resource_Handle_Filter field set to a Resource Handle value that does not have a record in the corresponding restriction map.
  2. The IUT sends an ATT_Write_Request to the ACS Control Point characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 1.
  3. The Lower Tester sends an ATT_Handle_Value_Indication of the ACS Control Point characteristic with the Segmentation_Header field and Payload field containing the Response Code opcode (0x00) and an operand representing the Request_Opcode field (0x02) followed by the Response_Code_Value field set to No Records Found (0x08).
  4. The IUT receives an ATT_Handle_Value_Indication from the Lower Tester and reports it to the Upper Tester.
  5. The IUT sends an ATT_Handle_Value_Confirmation on the ACS Control Point characteristic.
  6. Verify that the IUT returns to a stable state and can process commands normally.
  7. Verify that the characteristic values meet the requirements of the service.

- Expected Outcome

  Pass verdict

  The IUT receives the Response Code Value of No Records Found (0x08) from the Lower Tester and reports it to the Upper Tester.

  The Segmentation_Header field in all requests and responses includes the First Segment bit, Last Segment bit, and Rolling Segment Counter bits with appropriate values.

ACP/CL/ACSCP/BI-06-C [Abort Unsuccessful]

- Test Purpose

  Verify that the IUT responds appropriately when it receives an Abort Unsuccessful ACS Control Point Response Code Value.

- Reference

  [3] 5.5.4.14

- Initial Condition

  - Perform the preamble described in Section 4.2.3 to configure the ACS Control Point characteristic.
  - The Lower Tester has a large restriction map descriptor that will take a few seconds to transmit.

- Test Procedure

  1. The Upper Tester sends a command to the IUT to write a Segmentation_Header field and Payload field containing the Get Restriction Map Descriptors opcode (0x02) to the ACS Control Point with an operand with the Restriction_Map_ID field set to a restriction map ID and no filter by resource handle (0xFFFF).
  2. The IUT sends an ATT_Write_Request to the ACS Control Point characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 1.
  3. The Lower Tester starts to send indications of the ACS Control Point characteristic.
  4. The IUT receives one or more ATT_Handle_Value_Indication(s) from the Lower Tester and reports it to the Upper Tester.
  5. For each indication, the IUT sends an ATT_Handle_Value_Confirmation on the ACS Control Point characteristic.
  6. The Upper Tester sends a command to the IUT to write a Segmentation_Header field and Payload field containing the Abort opcode (0x15) to the ACS Control Point with no operand.
  7. The IUT sends an ATT_Write_Request to the ACS Control Point characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 6.
  8. The Lower Tester sends an ATT_Handle_Value_Indication of the ACS Control Point characteristic with the Segmentation_Header field and Payload field containing the Response Code opcode (0x00) and an operand representing the Request_Opcode field (0x15) followed by the Response_Code_Value field set to Abort Unsuccessful (0x07).
  9. The IUT receives an ATT_Handle_Value_Indication from the Lower Tester and reports it to the Upper Tester.
  10. The IUT sends an ATT_Handle_Value_Confirmation on the ACS Control Point characteristic.
  11. The Lower Tester sends the remaining indications until the complete restriction map descriptor has been sent.
  12. Verify that the IUT returns to a stable state and can process commands normally.
  13. Verify that the characteristic values meet the requirements of the service.

- Expected Outcome

  Pass verdict

  The IUT receives the Response Code Value of Abort Unsuccessful (0x07) from the Lower Tester and reports it to the Upper Tester.

  The Segmentation_Header field in all requests and responses includes the First Segment bit, Last Segment bit, and Rolling Segment Counter bits with appropriate values.

ACP/CL/ACSCP/BI-07-C [Procedure Already in Progress]

- Test Purpose

  Verify that the IUT responds appropriately when it receives an ATT Error Response with error code set to Procedure Already in Progress.

- Reference

  [3] 5.5.4.2, 5.5.4.23

- Initial Condition

  - Perform the preamble described in Section 4.2.3 to configure the ACS Control Point characteristic.

- Test Procedure

  1. The Upper Tester sends a command to the IUT to write a Segmentation_Header field and Payload field containing the Get All Active Descriptors opcode (0x01) to the ACS Control Point characteristic with no operand.
  2. The IUT sends an ATT_Write_Request to the ACS Control Point characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 1.
  3. Before the procedure is completed, the Upper Tester sends a command to the IUT to write a Segmentation_Header field and Payload field containing the Invalidate All Established Security opcode (0x13) to the ACS Control Point with no operand.
  4. The IUT sends an ATT_Write_Request to the ACS Control Point characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 3.
  5. The Lower Tester sends an ATT_Read_Response with error code Procedure Already in Progress (0xFE).
  6. The IUT receives an ATT_Read_Response from the Lower Tester and reports its error code to the Upper Tester.
  7. Verify that the IUT returns to a stable state and can process commands normally.

- Expected Outcome

  Pass verdict

  The IUT receives the Attribute Protocol Application error code set to Procedure Already in Progress (0xFE) from the Lower Tester and reports it to the Upper Tester.

  The Segmentation_Header field in all requests and responses includes the First Segment bit, Last Segment bit, and Rolling Segment Counter bits with appropriate values.

ACP/CL/ACSCP/BI-08-C [Reject Invalid Public Key]

- Test Purpose

  Verify that the IUT detects and rejects an invalid public key (e.g., the public key is not on the curve) during key exchange.

- Reference

  [3] 5.5.4.11, 5.5.4.18.1

  [4] 4.4.3.17.1.1

- Initial Condition
  - Perform the preamble described in Section 4.2.3 to configure the ACS Control Point characteristic.
  - The Upper Tester sends a command to the IUT to request the Get ACS Feature procedure using the ACS Control Point characteristic to acquire the Lower Tester's input and output capabilities.
  - The Upper Tester sends a command to the IUT to request the Get Key Descriptor procedure using the ACS Control Point characteristic to acquire the key records (e.g., the ECDH Key Exchange record, the Nonce_Type field value). If the Nonce_Type field value, for the selected key ID in the security algorithm's additional parameters, is Sequence Number Different Fixed Parts, then the Upper Tester sends a command to the IUT to request that the Set AC Client Nonce Fixed procedure using the ACS Control Point characteristic have a nonce set.
- Test Procedure
  1. The Upper Tester sends a command to the IUT to write a Segmentation_Header field and Payload field containing the Start Key Exchange opcode (0x11) to the ACS Control Point characteristic with an operand with the Key ID to be exchanged and how the exchanged key is to be confirmed.
  2. The IUT sends an ATT_Write_Request to the ACS Control Point characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 1.
  3. The Lower Tester sends an ATT_Handle_Value_Indication of the ACS Control Point characteristic with the Segmentation_Header field and Payload field containing the Response Code opcode (0x00) and an operand with the Request_Opcode field set to Start Key Exchange (0x11) and the Response_Code_Value field set to Success (0x01).
  4. The IUT receives an ATT_Handle_Value_Indication from the Lower Tester and reports it to the Upper Tester.
  5. The IUT sends an ATT_Handle_Value_Confirmation on the ACS Control Point characteristic.
  6. The Upper Tester sends a command to the IUT to write Segmentation_Header and Payload fields to send the Key Exchange ECDH opcode (0x1B) to the ACS Control Point characteristic with an operand with the Key ID used in step 1 and the AC Client Public Key of the IUT.
  7. The IUT sends ATT_Write_Requests to the ACS Control Point characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 6. The exact number of ATT_Write_Requests depends on the payload size.
  8. The Lower Tester sends ATT_Handle_Value_Indication(s) of the ACS Control Point characteristic with the Segmentation_Header field and Payload field containing the Key Exchange ECDH Response opcode (0x1C) and an operand with the Key ID used in step 1 and an invalid AC Server Public Key. The Lower Tester verifies that this public key is invalid (e.g., not on the curve) before sending it. If the new coordinates happen to be valid, then the generation procedure is repeated.
  9. The IUT receives an ATT_Handle_Value_Indication from the Lower Tester and reports it to the Upper Tester.
  10. For each indication, the IUT sends an ATT_Handle_Value_Confirmation on the ACS Control Point characteristic.
  11. The IUT detects the invalid key and does not continue the key exchange.
  12. Verify that the characteristic value meets the requirements of the service.
- Expected Outcome

  Pass verdict

  The IUT detects the invalid public key and does not continue the key exchange.

4.6 General Error Handling

Verify the IUT's error handling behavior for various scenarios.

ACP/CL/GEH/BI-01-C [Non-zero RFU bit values]

- Test Purpose

  Verify that the IUT responds appropriately when it receives a non-zero RFU bit value.

- Reference

  [3] 1.1.2, 5.5.2

- Initial Condition

  - A connection between the Lower Tester and the IUT has been established.

- Test Procedure

  1. The Upper Tester sends a command to the IUT to read the ACS Status characteristic.
  2. The IUT sends an ATT_Read_Request to the ACS Status characteristic of the Lower Tester.
  3. The Lower Tester sends an ATT_Read_Response to the IUT with at least one RFU bit of the Flags field set to 1.
  4. The IUT receives the ATT_Read_Response and reports the values to the Upper Tester.
  5. Verify that the IUT returns to a stable state and can process commands normally.

- Expected Outcome

  Pass verdict

  The IUT sends an ATT_Read_Request to read the ACS Status characteristic.

  The IUT receives the ATT_Read_Response from the Lower Tester with at least one RFU bit set to 1. The IUT processes the RFU bit(s) set to 1 as if they were set to 0. The IUT reports the values to the Upper Tester.

ACP/CL/GEH/BI-02-C [Client Characteristic Configuration Descriptor Improperly Configured]

- Test Purpose

  Verify that the IUT responds appropriately when it receives a Client Characteristic Configuration Descriptor Improperly Configured ATT error code.

- Reference

  [3] 5.5.4.12, 5.5.4.23

- Initial Condition

  - A connection between the Lower Tester and the IUT has been established.

- Test Procedure

  1. The Upper Tester sends a command to the IUT to write a Segmentation_Header field and Payload field containing the Invalidate All Established Security opcode (0x13) to the ACS Control Point with no operand.
  2. The IUT sends an ATT_Write_Request to the ACS Control Point characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 1.

3. The Lower Tester sends an ATT_Read_Response with error code Client Characteristic Configuration Descriptor Improperly Configured (0xFD).
4. The IUT receives an ATT_Read_Response from the Lower Tester and reports its error code to the Upper Tester.
5. Verify that the IUT returns to a stable state and can process commands normally.

- Expected Outcome

  Pass verdict

  The IUT receives the ATT error code of Client Characteristic Configuration Descriptor Improperly Configured (0xFD) from the Lower Tester and reports it to the Upper Tester.

ACP/CL/GEH/BI-03-C [Insufficient Authorization]

- Test Purpose

  Verify that the IUT responds appropriately when it receives an Insufficient Authorization ATT error code.

- Reference

  [3] 5.5.3, 5.5.4.23

- Initial Condition

  - Perform the preamble described in Section 4.2.3 to configure the ACS Control Point characteristic.
  - The Upper Tester sends a command to the IUT to request the Get Restriction Map ID List procedure using the ACS Control Point characteristic to acquire the available restriction map descriptors.

- Test Procedure

1. The Upper Tester sends a command to the IUT to write a Segmentation_Header field and Payload field containing the Get Restriction Map Descriptor opcode (0x02) to the ACS Control Point characteristic with an operand with the Restriction_Map_ID field set to a value of an available restriction map ID and no filter by resource handle (0xFFFF).
2. The IUT sends an ATT_Write_Request to the ACS Control Point characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 1.
3. The Lower Tester sends an ATT_Read_Response with error code Insufficient Authorization (0x08).
4. The IUT receives an ATT_Read_Response from the Lower Tester and reports its error code to the Upper Tester.
5. Verify that the IUT returns to a stable state and can process commands normally.

- Expected Outcome

  Pass verdict

  The IUT receives the ATT error code of Insufficient Authorization (0x08) from the Lower Tester and reports it to the Upper Tester.

ACP/CL/GEH/BI-04-C [Resource not protected]

- Test Purpose

  Verify that the IUT responds appropriately when it receives a Resource Not Protected application error code on the ACS Data characteristic.

- Reference

  [3] 5.5.3

- Initial Condition

  - Perform the preamble described in Section 4.2.3 to configure the ACS Data Out Notify and ACS Data Out Indicate characteristics.
  - The IUT and the Lower Tester have established the necessary security by performing a key exchange.

- Test Procedure

  1. The Upper Tester sends a command to the IUT to write a Segmentation_Header field and Payload field as a request to a resource via the ACS Data In characteristic with information security controls applied.
  2. The IUT sends an ATT_Write_Request to the ACS Data In characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 1.
  3. The Lower Tester sends an ATT_Read_Response with error code Resource Not Protected (0x81).
  4. The IUT receives an ATT_Read_Response from the Lower Tester and reports its error code to the Upper Tester.
  5. Verify that the IUT returns to a stable state and can process commands normally.

- Expected Outcome

  Pass verdict

  The IUT receives the application error code of Resource Not Protected (0x81) from the Lower Tester and reports it to the Upper Tester.

ACP/CL/GEH/BI-05-C [Incorrect security configuration]

- Test Purpose

  Verify that the IUT responds appropriately when it receives an Incorrect Security Configuration application error code on the ACS Data characteristic.

- Reference

  [3] 5.5.3

- Initial Condition

  - Perform the preamble described in Section 4.2.3 to configure the ACS Data Out Notify and ACS Data Out Indicate characteristics.
  - The IUT and the Lower Tester have established the necessary security by performing a key exchange.

- Test Procedure

  1. The Upper Tester sends a command to the IUT to write a Segmentation_Header field and Payload field as a request to a protected resource via the ACS Data In characteristic with information security controls applied.
  2. The IUT sends an ATT_Write_Request to the ACS Data In characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 1.
  3. The Lower Tester sends an ATT_Read_Response with error code Incorrect Security Configuration (0x82).
  4. The IUT receives an ATT_Read_Response from the Lower Tester and reports its error code to the Upper Tester.
  5. Verify that the IUT returns to a stable state and can process commands normally.

- Expected Outcome

  Pass verdict

  The IUT receives the application error code of Incorrect Security Configuration (0x82) from the Lower Tester and reports it to the Upper Tester.

ACP/CL/GEH/BI-06-C [Invalid Key]

- Test Purpose

  Verify that the IUT responds appropriately when it receives an Invalid Key application error code on the ACS Data characteristic.

- Reference

  [3] 5.5.3, 5.5.4.23

- Initial Condition

  - Perform the preamble described in Section 4.2.3 to configure the ACS Data Out Notify and ACS Data Out Indicate characteristics.
  - The IUT and the Lower Tester have established the necessary security by performing a key exchange.

- Test Procedure

  1. The Upper Tester sends a command to the IUT to write a Segmentation_Header field and Payload field as a request to a protected resource via the ACS Data In characteristic with information security controls applied.
  2. The IUT sends an ATT_Write_Request to the ACS Data In characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 1.
  3. The Lower Tester sends an ATT_Read_Response with error code Invalid Key (0x80).
  4. The IUT receives an ATT_Read_Response from the Lower Tester and reports its error code to the Upper Tester.
  5. Verify that the IUT returns to a stable state and can process commands normally.

- Expected Outcome

  Pass verdict

  The IUT receives the application error code of Invalid Key (0x80) from the Lower Tester and reports it to the Upper Tester.

ACP/CL/GEH/BI-07-C [Invalid Rolling Segment Counter]

- Test Purpose

  Verify that the IUT responds appropriately when it receives an Invalid Rolling Segment Counter application error code.

- Reference

  [3] 5.5.1

- Initial Condition

  - Perform the preamble described in Section 4.2.3 to configure the ACS Data Out Notify and ACS Data Out Indicate characteristics.
  - The IUT and the Lower Tester have established the necessary security by performing a key exchange.

- Test Procedure

  1. The Upper Tester sends a command to the IUT to write a Segmentation_Header field and Payload field as a request to a protected resource via the ACS Data In characteristic with information security controls applied.
  2. The IUT sends an ATT_Write_Request to the ACS Data In characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 1.
  3. The Lower Tester sends an ATT_Read_Response with error code Invalid Rolling Segment Counter (0x83).
  4. The IUT receives an ATT_Read_Response from the Lower Tester and reports its error code to the Upper Tester.
  5. Verify that the IUT returns to a stable state and can process commands normally.

- Expected Outcome

  Pass verdict

  The IUT receives the application error code of Invalid Rolling Segment Counter (0x83) from the Lower Tester and reports it to the Upper Tester.

ACP/CL/GEH/BI-08-C [Procedure Timeout]

- Test Purpose

  Verify the IUT's behavior when it does not receive a response to a secure write to the ACS Data In characteristic within the Attribute Protocol transaction timeout period.

- Reference

  [3] 5.5.3.1

- Initial Condition

  - Perform the preamble described in Section 4.2.3 to configure the ACS Data Out Notify and ACS Data Out Indicate characteristics.
  - The Upper Tester sends a command to the IUT to request the Get Information Security Configuration Descriptor procedure using the ACS Control Point characteristic to acquire the information security configuration controls that are mapped to the restriction map IDs to be requested.

- The restriction map descriptor of the Lower Tester is protected.
- The IUT and the Lower Tester have established the necessary security by performing a key exchange.

- Test Procedure

  1. The Upper Tester sends a command to the IUT to write a Segmentation_Header field and Payload field containing the Get All Active Descriptors opcode (0x01) to the ACS Data In characteristic, with no operand, with information security controls applied.
  2. The IUT sends an ATT_Write_Request to the ACS Data In characteristic of the Lower Tester, using the parameters provided by the Upper Tester in step 1.
  3. The Lower Tester sends one ATT_Handle_Value_Indication on the ACS Data Out Indicate characteristic, with the Segmentation_Header field and Payload field, but it does not send one of the additional indication segments for a duration that is at least longer than the Attribute protocol transaction timeout period.
  4. After the ATT transaction timeout period, the IUT reports the Attribute Protocol transaction timeout to the Upper Tester.

- Expected Outcome

  Pass verdict

  The IUT reports the Attribute Protocol transaction timeout to the Upper Tester.

5 Test case mapping

The Test Case Mapping Table (TCMT) maps test cases to specific requirements in the ICS. The IUT is tested in all roles for which support is declared in the ICS document.

The columns for the TCMT are defined as follows:

Item: Contains a logical expression based on specific entries from the associated ICS document. Contains a logical expression (using the operators AND, OR, NOT as needed) based on specific entries from the applicable ICS document(s). The entries are in the form of y/x references, where y corresponds to the table number and x corresponds to the feature number as defined in the ICS document for Authorization Control Profile [5].

Feature: A brief, informal description of the feature being tested.

Test Case(s): The applicable test case identifiers are required for Bluetooth Qualification if the corresponding y/x references defined in the Item column are supported. Further details about the function of the TCMT are elaborated in [2].

For the purpose and structure of the ICS/IXIT, refer to [2].

Item	Feature	Test Case(s)
ACP 9/1 OR ACP 9/2	Service Discovery	ACP/CL/CGGIT/SER/BV-01-C
ACP 2/2 AND ACP 5/1 AND GATT 1a/4 AND GAP 0/3 AND (NOT ACP 2/1)	Authorization Control Service not discoverable over BR/EDR	ACP/SR/SGGIT/SDPNF/BV-01-C
ACP 9/3	ACS Status	ACP/CL/CGGIT/CHA/BV-02-C
ACP 9/4	ACS Data In	ACP/CL/CGGIT/CHA/BV-03-C
ACP 9/5	ACS Data Out Notify	ACP/CL/CGGIT/CHA/BV-04-C
ACP 9/6	ACS Data Out Indicate	ACP/CL/CGGIT/CHA/BV-05-C
ACP 9/7	ACS Control Point	ACP/CL/CGGIT/CHA/BV-06-C
ACP 10/5	Read ACS Status	ACP/CL/GEH/BI-01-C
ACP 5/3	Authenticated Encryption using GCM by Server	ACP/SR/ACSD/BV-01-C
ACP 5/4	Authenticated Messaging using GMAC by Server	ACP/SR/ACSD/BV-02-C
ACP 10/3	Authenticated Encryption using GCM by Client	ACP/CL/ACSD/BV-03-C
ACP 10/4	Authenticated Messaging using GMAC by Client	ACP/CL/ACSD/BV-04-C
ACP 12/11	Write long characteristic value to ACS Data In	ACP/CL/ACSD/BV-05-C
ACP 11/1	Get All Active Descriptors	ACP/CL/ACSCP/BV-01-C ACP/CL/ACSCP/BV-02-C ACP/CL/ACSCP/BI-01-C ACP/CL/ACSCP/BI-02-C ACP/CL/ACSCP/BI-07-C ACP/CL/GEH/BI-08-C

Item	Feature	Test Case(s)
ACP 11/2	Get Restriction Map Descriptor	ACP/CL/ACSCP/BV-03-C ACP/CL/ACSCP/BV-04-C ACP/CL/ACSCP/BV-05-C ACP/CL/ACSCP/BI-03-C ACP/CL/ACSCP/BI-05-C ACP/CL/GEH/BI-03-C
ACP 11/3	Get Restriction Map ID List	ACP/CL/ACSCP/BV-06-C
ACP 11/4	Activate Restriction Map	ACP/CL/ACSCP/BV-07-C ACP/CL/ACSCP/BV-08-C
ACP 11/5	Get Resource Handle to UUID Map	ACP/CL/ACSCP/BV-09-C
ACP 11/6	Get Service and Characteristic UUIDs for Characteristic Resource Handle	ACP/CL/ACSCP/BV-10-C
ACP 11/7	Get Information Security Configuration Descriptor	ACP/CL/ACSCP/BV-11-C ACP/CL/ACSCP/BV-12-C
ACP 11/8	Get Key Descriptor	ACP/CL/ACSCP/BV-13-C ACP/CL/ACSCP/BV-14-C
ACP 11/9	Get Current Key List	ACP/CL/ACSCP/BV-15-C
ACP 11/11	Invalidate All Established Security	ACP/CL/ACSCP/BV-16-C ACP/CL/GEH/BI-02-C
ACP 11/12	Invalidate Key	ACP/CL/ACSCP/BV-17-C ACP/CL/ACSCP/BV-18-C
ACP 11/13	Abort	ACP/CL/ACSCP/BV-19-C ACP/CL/ACSCP/BI-04-C ACP/CL/ACSCP/BI-06-C
ACP 11/14	Set Security Controls Switch	ACP/CL/ACSCP/BV-20-C
ACP 11/15	Get Key URI	ACP/CL/ACSCP/BV-21-C
ACP 11/16	Get ACS Features	ACP/CL/ACSCP/BV-22-C
ACP 10/14	Key exchange	ACP/CL/ACSCP/BV-23-C ACP/CL/ACSCP/BV-24-C ACP/CL/ACSCP/BV-25-C ACP/CL/ACSCP/BI-08-C
ACP 11/21	Set AC Client Nonce Fixed	ACP/CL/ACSCP/BV-26-C
ACP 11/22	Get ATT_MTU	ACP/CL/ACSCP/BV-27-C
ACP 11/23	Initiate Pairing	ACP/CL/ACSCP/BV-28-C
ACP 10/7	Resource not protected, Incorrect information security configuration and Invalid Key	ACP/CL/GEH/BI-04-C ACP/CL/GEH/BI-05-C ACP/CL/GEH/BI-06-C ACP/CL/GEH/BI-07-C

Table 5.1: Test case mapping

6 ACS Control Point Response Code Test Matrix

The following table summarizes the combination of some of the ACS Control Point opcodes and the Response Code Values that are tested and not tested. For the table, below, the following key applies:

YES = A test for this combination exists.

NO = A test for this combination does not exist.

N/A = Not a valid combination.

ACS Control Point Response Code	**ACS Control Point Opcode**			
	Get All Active Descriptor	Get Restriction Map Descriptor	Abort	Invalidate All Established Security
Success	YES	N/A	YES	YES
Opcode not supported	YES	NO	NO	N/A
Invalid Operand	NO	NO	N/A	N/A
Procedure not completed	YES	N/A	N/A	NO
Parameter out of range	NO	YES	N/A	N/A
Procedure not applicable	NO	NO	YES	N/A
Abort unsuccessful	N/A	N/A	YES	N/A
No records found	NO	YES	N/A	N/A
Procedure already in progress	NO	NO	NO	YES

Table 6.1: ACS Control Point Response Code test coverage

7 ACS Data Error Code Test Matrix

The following table summarizes the combination of some of the ACS Data error codes that are tested and not tested. For the tables, below, the following key applies:

YES = A test for this combination exists.

NO = A test for this combination does not exist.

N/A = Not a valid combination.

Error Codes	ACS Data characteristic
Invalid Key	YES
Resource not protected	YES
Incorrect security configuration	YES
Invalid Rolling Segment Counter	YES

Table 7.1: ACS Data error code test coverage

8 Revision history and acknowledgments

Revision History

Publication Number	Revision Number	Date	Comments
0	p0	2022-09-20	Approved by BTI on 2022-08-31. ACP v1.0 adopted by the BoD on 2022-09-13. Prepared for initial publication.
	p1r00	2023-04-04	TSE 22880 (rating 1): Globally changed all TCIDs ending with “-I” to “-C” tests.
1	p1	2023-06-29	Approved by BTI on 2023-05-28. Prepared for TCRL 2023-1 publication.

Acknowledgments

Name	Company
Ismail Mohamud	Bluetooth SIG, Inc.
Christoph Fischer	F. Hoffmann-La Roche AG
Nathaniel Hamming	HMT Consulting