Authorization Control Profile (ACP)

Bluetooth® **Implementation Conformance Statement (ICS) Proforma**

- **Revision:** ACP.ICS.p0
- **Revision Date:** 2022-09-20
- **Prepared By:** Medical Devices Working Group
- **Published during TCRL:** 2022-1-addition

Contents

1 Identification of the implementation

1.1 Implementation Under Test (IUT) identification

Identification of the Implementation Under Test (IUT) is to be filled in to provide as much detail as possible regarding version numbers and configuration options.

An ICS contact person to respond to queries regarding information supplied in this ICS proforma is named in the Declaration of Compliance: Summary of Selected Specifications in Implementation.

1.2   Roles

Table 1: Role Requirements

Item	Role	Reference	Status
1	AC Server	[1] 2.1	C.1
2	AC Client	[1] 2.1	C.1

C.1:   Mandatory to support at least one of ACP 1/1 "AC Server" OR ACP 1/2 "AC Client".

1.3   Transports

Table 2: Transport Requirements

Item	Transport	Reference	Status
1	Profile supported over BR/EDR	[1] 2.5	C.1
2	Profile supported over LE	[1] 2.5	C.1

C.1:   Mandatory to support at least one of ACP 2/1 "Profile supported over BR/EDR" OR ACP 2/2 "Profile supported over LE".

1.4   Authorization Control Server role

1.4.1   Versions

Table 3: X.Y Versions

Prerequisite: ACP 1/1 "AC Server"

Item	Version	Reference	Status
1	ACP v1.0	[1]	M

Table 4: X.Y.Z Versions

Table number reserved but not yet in use.

1.4.2   Service and Features Requirements

Table 5: Service and Features Requirement

Prerequisite: ACP 1/1 "AC Server"

Item	Capability	Reference	Status	Inter-Layer Dependency
1	Authorization Control Service	[1] 4	M	[4] ACS
2	Elliptic Curve Diffie Hellman (ECDH) key agreement scheme with Curve P-256 and key derivation function HKDF SHA-256 128-bit	[1] 4.1.1.1	C.1	N/A
3	Authentication encryption using Galois/Counter Mode (GCM)	[1] 4.1.1.2	C.2	N/A

Item	Capability	Reference	Status	Inter-Layer Dependency
4	Authentication messaging using Galois/Counter Mode Message Authentication Code (GMAC)	[1] 4.1.1.2	C.3	N/A

C.1: Mandatory IF ACS 3/7 "ECDH Key Exchange", otherwise Optional.

C.2: Mandatory IF ACS 4/1 "Confidentiality" AND ACS 4/2 "Integrity" AND ACS 4/3 "Authentication", otherwise Optional.

C.3: Mandatory IF ACS 4/2 "Integrity" AND ACS 4/3 "Authentication" AND NOT ACS 4/1 "Confidentiality", otherwise Optional.

1.4.3   GATT Requirements

Table 6: GATT Requirements

Prerequisite: ACP 1/1 "AC Server"

Item	Capability	Reference	Status	Inter-Layer Dependency
1	Generic Attribute Profile (GATT) Server	[1] 2.1	M	[2] GATT 1/2

1.5   Authorization Control Client role

1.5.1   Versions

Table 7: X.Y Versions

Prerequisite: ACP 1/2 "AC Client"

Item	Version	Reference	Status
1	ACP v1.0	[1]	M

Table 8: X.Y.Z Versions

Table number reserved but not yet in use.

1.5.2   Services and Characteristics

Table 9: Discovery of Services and Characteristics Requirements

Prerequisite: ACP 1/2 "AC Client"

Item	Capability	Reference	Status
1	Authorization Control Service	[1] 5	M
2	Discover Authorization Control Service	[1] 5.2	M
3	Discover ACS Status characteristic and Client Characteristic Configuration Descriptor	[1] 5.3, 5.3.1	M
4	Discover ACS Data In characteristic	[1] 5.3, 5.3.2	M
5	Discover ACS Data Out Notify characteristic and Client Characteristic Configuration Descriptor	[1] 5.3, 5.3.3	M

Item	Capability	Reference	Status
6	Discover ACS Data Out Indicate characteristic and Client Characteristic Configuration Descriptor	[1] 5.3, 5.3.4	M
7	Discover ACS Control Point characteristic and Client Characteristic Configuration Descriptor	[1] 5.3, 5.3.5	M

Table 10: Features

Prerequisite: ACP 1/2 "AC Client"

Item	Capability	Reference	Status
1	ECDH key agreement scheme	[1] 5.4.1	M
2	ECDH key agreement scheme with Curve P-256 and key derivation function HKDF SHA-256 128-bit	[1] 5.4.1.1	M
3	Galois/Counter Mode (GCM)	[1] 5.4.2	M
4	Galois/Counter Mode Message Authentication Code (GMAC)	[1] 5.4.2	M
5	Read ACS Status	[1] 5.5.2	O
6	Configure ACS Status characteristic for indication	[1] 5.5.2	O
7	Write to ACS Data In characteristic	[1] 5.5.3	M
8	Read ACS Data In characteristic	[1] 5.5.3	M
9	Configure ACS Data Out Notify characteristic for notifications	[1] 5.5.3	M
10	Configure ACS Data Out Indicate characteristic for indications	[1] 5.5.3	M
11	Configure ACS Control Point characteristic for indications	[1] 5.5.4	M
12	Write to ACS Control Point characteristic	[1] 5.5.4	O
13	Multiple Restriction Maps	[1] 5.5.4.1.7	O
14	Key Exchange	[1] 5.5.4.1.7	O
15	Set Security Controls Switch	[1] 5.5.4.1.7	O
16	OOB Key Exchange	[1] 5.5.4.1.7	O
17	Key URI	[1] 5.5.4.1.7	O

Table 11: ACS Control Point Procedures

Prerequisite: ACP 1/2 "AC Client"

Item	Capability	Reference	Status
1	Get All Active Descriptors	[1] 5.5.4.2	M
2	Get Restriction Map Descriptor	[1] 5.5.4.3	M
3	Get Restriction Map ID List	[1] 5.5.4.4	M
4	Activate Restriction Map	[1] 5.5.4.5	C.1
5	Get Resource Handle To UUID Map	[1] 5.5.4.6	M
6	Get Service And Characteristic UUIDs For Characteristic Resource Handle	[1] 5.5.4.7	M
7	Get Information Security Configuration Descriptor	[1] 5.5.4.8	M
8	Get Key Descriptor	[1] 5.5.4.9	M
9	Get Current Key List	[1] 5.5.4.10	C.2

Item	Capability	Reference	Status
10	Start Key Exchange	[1] 5.5.4.11	C.2
11	Invalidate All Established Security	[1] 5.5.4.12	O
12	Invalidate Key	[1] 5.5.4.13	C.2
13	Abort	[1] 5.5.4.14	M
14	Set Security Controls Switch	[1] 5.5.4.15	C.3
15	Get Key URI	[1] 5.5.4.16	C.4
16	Get ACS Feature	[1] 5.5.4.17	M
17	Key Exchange ECDH	[1] 5.5.4.18.1.1	C.2
18	Key Exchange ECDH Confirmation Code	[1] 5.5.4.18.1.2	C.2
19	Key Exchange ECDH Confirmation Random Number	[1] 5.5.4.18.1.3	C.2
20	Key Exchange KDF	[1] 5.5.4.18.2.1	C.2
21	Set AC Client Nonce Fixed	[1] 5.5.4.19	C.2
22	Get ATT_MTU	[1] 5.5.4.20	O
23	Initiate Pairing	[1] 5.5.4.21	O

C.1:   Mandatory IF ACP 10/13 "Multiple Restriction Maps", otherwise Excluded.

C.2:   Mandatory IF ACP 10/14 "Key Exchange", otherwise Excluded.

C.3:   Mandatory IF ACP 10/15 "Set Security Controls Switch", otherwise Excluded.

C.4:   Mandatory IF ACP 10/16 "OOB Key Exchange" AND ACP 10/17 "Key URI", otherwise Excluded.

1.5.3   GATT Requirements

Table 12: GATT Requirements

Prerequisite: ACP 1/2 "AC Client"

Item	Capability	Reference	Status	Inter-Layer Dependency
1	Generic Attribute Profile (GATT) Client	[1] 2.1	M	[2] GATT 1/1
2	Discover All Primary Services	[1] 5.1, 5.2	C.1	[2] GATT 3/2
3	Discover Primary Services by Service UUID	[1] 5.1, 5.2	C.1	[2] GATT 3/3
4	Discover All Characteristics of a Service	[1] 5.1, 5.3	C.2	[2] GATT 3/5
5	Discover Characteristics by UUID	[1] 5.1, 5.3	C.2	[2] GATT 3/6
6	Discover All Characteristic Descriptors	[1] 5.1, 5.3	M	[2] GATT 3/7
7	Notifications	[1] 5.1	M	[2] GATT 3/17
8	Indications	[1] 5.1	M	[2] GATT 3/18
9	Read Characteristic Value	[1] 5.1	M	[2] GATT 3/8
10	Write Characteristic Value	[1] 5.1	M	[2] GATT 3/14
11	Write Long Characteristic Values	[1] 5.1	O	[2] GATT 3/15
12	Read Characteristic Descriptors	[1] 5.1	M	[2] GATT 3/19

Item	Capability	Reference	Status	Inter-Layer Dependency
13	Write Characteristic Descriptors	[1] 5.1	M	[2] GATT 3/21

C.1: Mandatory to support at least one of ACP 12/2 "Discover All Primary Services" OR ACP 12/3 "Discover Primary Services by Service UUID".

C.2: Mandatory to support at least one of ACP 12/4 "Discover All Characteristics of a Service" OR ACP 12/5 "Discover Characteristics by UUID".

1.5.4 GAP Requirements

Table 13: GAP Requirements

Prerequisite: ACP 1/2 "AC Client"

Item	Capability	Reference	Status	Inter-Layer Dependency
1	Central	[1] 6	M	[3] GAP 5/4 or GAP 38/4
2	Bondable mode	[1] 7.2	C.1	[3] GAP 34/2
3	LE security mode 1	[1] 7.2	C.2	[3] GAP 35/1

C.1: Optional IF ACP 2/2 "Profile supported over LE", otherwise not defined.

C.2: Mandatory IF ACP 2/2 "Profile supported over LE", otherwise not defined.

2 References

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

[2] ICS Proforma for Generic Attribute Profile (GATT)

[3] ICS Proforma for Generic Access Profile (GAP)

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

3 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.

Acknowledgments

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