

User Data Service

Bluetooth® Service Specification



- Date **2014-May-14**
- Revision **V1.0**
- Group Prepared By **SF WG**
- Feedback Email **sf-main@bluetooth.org**

Abstract:

This service exposes user-related data in the sports and fitness environment. This allows remote access and update of user data by a Client as well as the synchronization of user data between a Server and a Client.

Revision History

Revision Number	Date	Comments
V1.0	2014-06-10	Adopted by the Bluetooth SIG Board of Directors.

Contributors

Name	Company
Robert D. Hughes	Intel Corporation
Niclas Granqvist	Polar
Guillaume Schatz	Polar
Srikkanth Madhurbootheswaran	Mindtree
Anand Noubade	Mindtree

V1.0

DISCLAIMER AND COPYRIGHT NOTICE

This disclaimer applies to all draft specifications and final specifications adopted by the Bluetooth SIG Board of Directors (both of which are hereinafter referred to herein as a Bluetooth "Specification"). Your use of this Specification in any way is subject to your compliance with all conditions of such use, and your acceptance of all disclaimers and limitations as to such use, contained in this Specification. Any user of this Specification is advised to seek appropriate legal, engineering or other professional advice regarding the use, interpretation or effect of this Specification on any matters discussed in this Specification.

Use of Bluetooth Specifications and any related intellectual property is governed by the Promoters Membership Agreement among the Promoter Members and Bluetooth SIG (the "Promoters Agreement"), certain membership agreements between Bluetooth SIG and its Adopter and Associate Members, including, but not limited to, the Membership Application, the Bluetooth Patent/Copyright License Agreement and the Bluetooth Trademark License Agreement (collectively, the "Membership Agreements") and the Bluetooth Specification Early Adopters Agreements (1.2 Early Adopters Agreements) among Early Adopter members of the unincorporated Bluetooth SIG and the Promoter Members (the "Early Adopters Agreement"). Certain rights and obligations of the Promoter Members under the Early Adopters Agreements have been assigned to Bluetooth SIG by the Promoter Members.

Use of the Specification by anyone who is not a member of Bluetooth SIG or a party to an Early Adopters Agreement (each such person or party, a "Member") is prohibited. The use of any portion of a Bluetooth Specification may involve the use of intellectual property rights ("IPR"), including pending or issued patents, or copyrights or other rights. Bluetooth SIG has made no search or investigation for such rights and disclaims any undertaking or duty to do so. The legal rights and obligations of each Member are governed by the applicable Membership Agreements, Early Adopters Agreement or Promoters Agreement. No license, express or implied, by estoppel or otherwise, to any intellectual property rights are granted herein.

Any use of the Specification not in compliance with the terms of the applicable Membership Agreements, Early Adopters Agreement or Promoters Agreement is prohibited and any such prohibited use may result in (i) termination of the applicable Membership Agreements or Early Adopters Agreement and (ii) liability claims by Bluetooth SIG or any of its Members for patent, copyright and/or trademark infringement claims permitted by the applicable agreement or by applicable law.

THE SPECIFICATION IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, SATISFACTORY QUALITY, OR REASONABLE SKILL OR CARE, OR ANY WARRANTY ARISING OUT OF ANY COURSE OF DEALING, USAGE, TRADE PRACTICE, PROPOSAL, SPECIFICATION OR SAMPLE.

Each Member hereby acknowledges that products equipped with the Bluetooth wireless technology ("Bluetooth Products") may be subject to various regulatory controls under the laws and regulations applicable to products using wireless non licensed spectrum of various governments worldwide. Such laws and regulatory controls may govern, among other things, the combination, operation, use, implementation and distribution of Bluetooth Products. Examples of such laws and regulatory controls include, but are not limited to, airline regulatory controls, telecommunications regulations, technology transfer controls and health and safety regulations. Each Member is solely responsible for the compliance by their Bluetooth Products with any such laws and regulations and for obtaining any and all required authorizations, permits, or licenses for their Bluetooth Products related to such regulations within the applicable jurisdictions. Each Member acknowledges that nothing in the Specification provides any information or assistance in connection with securing such compliance, authorizations or licenses. NOTHING IN THE SPECIFICATION CREATES ANY WARRANTIES, EITHER EXPRESS OR IMPLIED, REGARDING SUCH LAWS OR REGULATIONS.

ALL LIABILITY, INCLUDING LIABILITY FOR INFRINGEMENT OF ANY INTELLECTUAL PROPERTY RIGHTS OR FOR NONCOMPLIANCE WITH LAWS, RELATING TO USE OF THE SPECIFICATION IS EXPRESSLY DISCLAIMED. To the extent not prohibited by law, in no event will Bluetooth SIG or its Members or their affiliates be liable for any damages, including without limitation, lost revenue, profits, data or programs, or business interruption, or for special, indirect, consequential, incidental or punitive damages, however caused and regardless of the theory of liability, arising out of or related to any furnishing, practicing, modifying, use or the performance or implementation of the contents of this Specification, even if Bluetooth SIG or its Members or their affiliates have been advised of the possibility of such damages. BY USE OF THE SPECIFICATION, EACH MEMBER EXPRESSLY WAIVES ANY CLAIM AGAINST BLUETOOTH SIG AND ITS MEMBERS OR THEIR AFFILIATES RELATED TO USE OF THE SPECIFICATION.

If this Specification is an intermediate draft, it is for comment only. No products should be designed based on it except solely to verify the prototyping specification at SIG sponsored IOP events and it does not represent any commitment to release or implement any portion of the intermediate draft, which may be withdrawn, modified, or replaced at any time in the adopted Specification.

Bluetooth SIG reserves the right to adopt any changes or alterations to the Specification it deems necessary or appropriate.

Copyright © 2013 - 2014. The Bluetooth word mark and logos are owned by Bluetooth SIG, Inc. All copyrights in the Bluetooth Specifications themselves are owned by Ericsson AB, Lenovo (Singapore) Pte. Ltd., Intel Corporation, Microsoft Corporation, Motorola Mobility, LLC, Nokia Corporation and Toshiba Corporation. Other third-party brands and names are the property of their respective owners.

Document Terminology

The Bluetooth SIG has adopted Section 13.1 of the IEEE Standards Style Manual, which dictates use of the words “shall”, “should”, “may”, and “can” in the development of documentation, as follows:

The word *shall* is used to indicate mandatory requirements strictly to be followed in order to conform to the standard and from which no deviation is permitted (*shall* equals *is required to*).

The use of the word *must* is deprecated and shall not be used when stating mandatory requirements; *must* is used only to describe unavoidable situations.

The use of the word *will* is deprecated and shall not be used when stating mandatory requirements; *will* is only used in statements of fact.

The word *should* is used to indicate that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required; or that (in the negative form) a certain course of action is deprecated but not prohibited (*should* equals *is recommended that*).

The word *may* is used to indicate a course of action permissible within the limits of the standard (*may* equals *is permitted*).

The word *can* is used for statements of possibility and capability, whether material, physical, or causal (*can* equals *is able to*).

The term *Reserved for Future Use (RFU)* is used to indicate Bluetooth SIG assigned values that are reserved by the Bluetooth SIG and are not otherwise available for use by implementations.

Contents

1	Introduction	6
1.1	Conformance	6
1.2	Service Dependencies.....	6
1.3	Bluetooth Core Specification Release Compatibility	6
1.4	GATT Sub-Procedure Requirements	7
1.5	Transport Dependencies	7
1.5.1	Support for Multiple Clients	7
1.6	Application Error Codes.....	7
1.7	Byte Transmission Order.....	8
2	Service Declaration.....	9
3	Service Characteristics	10
3.1	UDS Characteristics	10
3.1.1	Characteristic Behavior	11
3.2	Database Change Increment Characteristic	11
3.2.1	Database Change Increment Characteristic Behavior	11
3.3	User Index Characteristic	12
3.3.1	User Index Characteristic Behavior	12
3.4	User Control Point	13
3.4.1	User Control Point Procedure Requirements	13
3.4.2	User Control Point Behavioral Description	14
3.4.2.1	Register New User Procedure	15
3.4.2.2	Consent Procedure	15
3.4.2.3	Delete User Data Procedure	15
3.4.2.4	Procedure Complete	16
3.4.3	General Error Handling procedures	18
3.4.4	Procedure Timeout	18
4	SDP Interoperability.....	19
5	Acronyms and Abbreviations.....	20
6	References.....	21
7	Appendix A - Recommended Client Behavior (INFORMATIVE).....	22
7.1	General Considerations	22
7.2	Considerations for Personal Clients	23
7.3	Considerations for Public Clients.....	24
8	Appendix B – User Control Point Message Sequence Charts (INFORMATIVE).....	24
8.1	Register New User Procedure	24
8.2	Consent Procedure.....	25
8.3	Delete User Data Procedure	25

1 Introduction

The User Data Service (UDS) exposes user-related data in the sports and fitness environment. This allows remote access and update of user data by a Client as well as the synchronization of user data between a Server and a Client.

The UDS uses a family of characteristics; one characteristic for each type of user data. The UUID of the characteristic identifies the user data that is being stored by the Server, as described in Section 3.1. The service exposes one or more such User Data Service characteristics, referred to generically from now on as “UDS Characteristics”.

The service also exposes the Database Change Increment characteristic (See Section 3.2) in order to provide a synchronization mechanism between devices as defined in Section 7.

The service also exposes the User Index characteristic (e.g. to differentiate between users of a multi-user device, as defined in Section 3.3) and the User Control Point characteristic (i.e. to register a new user, to allow the user to provide consent to share data and to delete the user data).

The term “consent” used in this document refers to a mechanism provided by this service to request an action from the user to give consent in order to access his user data and to restrict access to these data to other users. The consent mechanism described in this document is not intended as a security mechanism and is only used to ensure the user consents to share his or her data with a Client.

The full set of UDS Characteristics are listed online in the UDS Characteristics table for this specification [2]. The list may be updated whenever support for additional user data is required. To request UDS Characteristics to be added to this table to support new or future UDS applications, please contact the Sports and Fitness WG (sf-main@bluetooth.org). Since all UDS Characteristics are required to have identical behavioral options, extending the types of user data in this way does not require any change to be made to this service specification.

1.1 Conformance

If a device claims conformance to this service, all capabilities indicated as mandatory for this service shall be supported in the specified manner (process-mandatory). This also applies for all optional and conditional capabilities for which support is indicated. All mandatory capabilities, and optional and conditional capabilities for which support is indicated, are subject to verification as part of the Bluetooth qualification program.

1.2 Service Dependencies

This service is not dependent upon any other services.

1.3 Bluetooth Core Specification Release Compatibility

This specification is compatible with any of the following:

- Bluetooth Core Specification 4.0 [1].
- A Bluetooth Core Specification later than 4.0.

1.4 GATT Sub-Procedure Requirements

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

Table 1.1 summarizes *additional* GATT sub-procedure requirements beyond those required by all GATT Servers.

GATT Sub-Procedure	Requirements
Write Characteristic Value	M
Read Long Characteristic Value	C.1
Write Long Characteristic Value	C.1
Notification	C.2
Indication	M

Table 1.1: GATT Sub-procedure Requirements

C.1: Mandatory if the Server exposes at least one characteristic with a size that may exceed the available space needed for the GATT operations of the minimum default ATT_MTU, otherwise optional (e.g. utf8-based characteristics).

C.2: Mandatory if the Server supports the update of one or more UDS Characteristic values (e.g. through its User Interface or any other out-of-band mechanism), otherwise, excluded from this version of the service.

1.5 Transport Dependencies

There are no transport restrictions imposed by this service specification.

Where the term BR/EDR is used throughout this document, this also includes the optional use of AMP.

1.5.1 Support for Multiple Clients

If a Server supports the connection to two or more Clients simultaneously, the Server shall allow each Client to behave as if a single Client was connected. See Section 3.2 for handling the situation where one of the connected Clients updates the user data.

1.6 Application Error Codes

This service defines the following Attribute Protocol Application Error code:

Name	Error Code	Description
User Data Access Not Permitted	0x80	The user data access is not permitted (i.e. the user has not given consent in order to access these data).

Table 1.2: Attribute Protocol Application Error codes defined by this service

1.7 Byte Transmission Order

All characteristics used with this service shall be transmitted with the least significant octet first (i.e., little endian). The least significant octet is identified in the characteristic definitions in [\[2\]](#).

2 Service Declaration

The User Data Service is recommended to be instantiated as a «Primary Service».

The service UUID shall be set to «User Data Service» as defined in [\[2\]](#).

3 Service Characteristics

Each type of user data supported has a UDS Characteristic assigned to it. The service shall expose at least one UDS Characteristic and shall not expose more than one instance of the same UDS Characteristic.

The User Data Service shall expose the Database Change Increment characteristic in order to allow different devices to maintain data consistency between connections (i.e. synchronization) and at least one UDS Characteristic. The Server shall also expose the User Index characteristic as well as the User Control Point characteristic.

Where a characteristic can be notified or indicated, a Client Characteristic Configuration descriptor shall be included in that characteristic as required by the Core Specification [1].

Refer also to Section 7 for guidance on how this service is used by a Client.

Characteristic Name	Requirement	Mandatory Properties	Optional Properties	Security Permissions
UDS Characteristic	C.1	Read, Write	N/A	C.3
Database Change Increment	M	Read, Write	Notify (See C.2)	Read: Not specified Write: C.3
User Index	M	Read	N/A	C.3
User Control Point	M	Write, Indicate	N/A	C.3

Table 3.1: Requirements for each UDS Characteristic

C.1: At least one UDS Characteristic shall be exposed.

C.2: The Notify property is Mandatory if the Server supports the update of one or more UDS Characteristic values (e.g. through its User Interface or any other out-of-band mechanism), otherwise, excluded from this version of the service.

C.3: Encryption is mandatory. If the IO capabilities of the device permit GAP Authentication and GAP Authorization, it is recommended to use these GAP procedures.

Notes:

Properties not listed as Mandatory or Optional are excluded for this version of the service.

3.1 UDS Characteristics

The Server shall expose at least one UDS Characteristic.

Each UDS Characteristic is defined in the User Data Service Characteristics table in [2].

The Server shall not expose multiple instances of the same UDS Characteristic in an instance of this service.

3.1.1 Characteristic Behavior

All UDS Characteristics have identical behavioral options as described in this sub-section.

The Server shall allow the Client to access the UDS Characteristics of a user only after that user has provided consent. The consent mechanism provided by this service is described in Section 3.4. The consent shall end when the connection is terminated.

If a Client attempts to access the UDS Characteristics of a user for which the user has not given consent, the Server shall respond with an ATT Error Response and an Application Error Code set to *User Data Access Not Permitted* as defined in Section 1.6. If the security requirements (e.g. encryption) do not meet the requirements of the Server, the Server shall respond with the appropriate error (e.g. *Insufficient Encryption*, *Insufficient Authentication* or *Insufficient Authorization*, as defined in [1]).

A UDS Characteristic returns its associated characteristic value when read.

The Server should store the UDS Characteristic value locally when written by the Client.

A Server shall populate the values of the UDS Characteristics with the local values for the current user (i.e. the user that has given consent) in order to process the requests from a Client. In other words, the UDS Characteristic values are stored on the Server on a per user basis.

For LE, if the Server exposes utf8-based characteristics, it should support longer values than the default ATT_MTU-3 in order to provide a better user experience (e.g. the Email Address characteristic value will most likely be longer than 20 bytes).

For LE, if the UDS Characteristic value exceeds the size that can be written using a GATT Write Request or read using a GATT Read Request (e.g. for long utf8s-based characteristics), the GATT Write Long Characteristic Value and GATT Read Long Characteristic Value sub-procedures shall be used, respectively.

If the UDS Characteristic value is updated through the User Interface (UI) of the Server or other out-of-band mechanism, it shall increment the value of the Database Change Increment characteristic defined in Section 3.2.

3.2 Database Change Increment Characteristic

The Server shall expose the Database Change Increment characteristic.

3.2.1 Database Change Increment Characteristic Behavior

When read or notified, the Database Change Increment characteristic returns a value that is used by a Client to determine whether or not the UDS Characteristics need to be synchronized between the Server and the Client.

The default value of the Database Change Increment characteristic value shall be 0 (i.e. for a new device or when the device is reset). This value shall also be set to 0 when the user has not given consent.

When the user has given consent, the Server shall populate the Database Change Increment value with the local Database Change Increment value for the current user.

When the UDS Characteristic value is updated through the User Interface (UI) of the Server or any other out-of-band mechanism, the Server shall increment the value of the Database Change Increment characteristic. The Server shall increment the Database Change Increment characteristic value only once, at the end of the update procedure, even if more than one UDS Characteristic value has been updated (e.g. when a user selects the 'save' button).

When the Server updates the value of the Database Change Increment while connected to a Client that has received consent from the user, the Server shall notify the Database Change Increment characteristic in order to inform the Client that one or more of the UDS Characteristic values has been updated at the Server. In this case, the Client should refresh its local values by reading the supported UDS Characteristics. The Server should notify the Database Change Increment only once, at the end of the update procedure, even if more than one UDS Characteristic value has been updated (e.g. when a user selects the 'save' button).

When the UDS Characteristic value is updated by the Client (i.e. using GATT Write Characteristic Value or GATT Write Long Characteristic Value sub-procedures), the Server shall not increment the Database Change Increment characteristic value. The value of the Database Change Increment characteristic is required to be updated by the Client once the update procedure has been completed by the Client (e.g. when a user selects the 'save' button).

When the Server is connected to two or more Clients associated with the same user (i.e. the same user has given consent to share data with two or more Clients), and if one of the Clients attempts to update the value of the Database Change Increment, the Server shall notify the Database Change Increment characteristic to the other connected Client(s) associated with the same user in order to inform them that one or more of the UDS Characteristic values has been updated. In this case, the Client(s) that have received the notification should refresh their local values by reading the supported UDS Characteristics.

A race condition may occur (e.g. if UDS Characteristic values are updated simultaneously at the Server and the Client) even if very unlikely. If this occurs, it is left to the application to handle this situation (e.g. the Server should not accept the requests from the Client while the user data is being updated at the Server).

The Server has authority of data and can always reject updates for any reason (e.g. if the Client writes an unexpected value).

3.3 User Index Characteristic

The Server shall expose the User Index characteristic.

3.3.1 User Index Characteristic Behavior

When read, the User Index characteristic returns the index of the current user (i.e. the user that has given consent) to access the UDS Characteristics.

When no user is allowed to access the UDS Characteristics exposed by the Server or no user is currently selected, the special value 0xFF (Unknown User) shall be used.

The Server shall store the UDS Characteristics and the Database Change Increment characteristic values separately for each supported user.

By default, the value of this characteristic shall be set to Unknown User (0xFF) (e.g. when the Client initiates a connection and when no user is currently selected). When a user has given consent to access his data by using the Consent procedure defined in Section 3.4.2.2, the Server shall populate the User Index characteristic value with the value associated to that particular user. The User Index value is defined by the Server when the Register New User procedure is executed (See Section 3.4.2.1). This value is unique in the context of the Server and can be any value within the range of 0x00 to 0xFE and is not required to be assigned in a sequence starting at 1 for each supported user.

3.4 User Control Point

The Server shall expose the User Control Point.

The User Control Point characteristic is identified using the UUID «User Control Point», as defined in [2]. The User Control Point characteristic is used to request a specific function to be executed on the receiving device.

The format of the User Control Point characteristic is defined in Table 3.2.

	LSO	MSO
	Op Code (see Table 3.3)	Parameter (see Table 3.3)
Byte Order	N/A	LSO...MSO
Data type	UINT8	Variable
Size	1 octet	0 to 18 octets
Units	None	None

Table 3.2: User Control Point Characteristic Format

The Op Codes, the Parameters and the requirements for the User Control Point are defined in Section 3.4.1.

3.4.1 User Control Point Procedure Requirements

A Client shall use the *GATT Write Characteristic Value* sub-procedure to initiate a procedure defined in the Table 3.3.

The Op Codes, the Parameters and their requirements are defined in Table 3.3.

Op Code Value	Requirement	Definition	Parameter Value	Description
0x00	N/A	Reserved for future use	N/A	N/A
0x01	M	Register New User See Section 3.4.2.1	Consent Code See Section 3.4.2	Initiates the procedure to register a new user. The Consent Code for that user is sent as parameter to this op

Op Code Value	Requirement	Definition	Parameter Value	Description
				code. The response to this control point is Op Code 0x20 followed by the appropriate Response Value including the User Index.
0x02	M	Consent See Section 3.4.2.2	User Index, Consent Code See Section 3.4.2	Initiate the procedure to allow a Client to access the user data stored in the Server (i.e. the user gives consent). The User Index and the Consent Code are sent as parameters to this op code. The response to this control point is Op Code 0x20 followed by the appropriate Response Value.
0x03	M	Delete User Data See Section 3.4.2.3	None	Deletes the user data of the current user as well as its Consent Code. The response to this control point is Op Code 0x20 followed by the appropriate Response Value.
0x04-0x1F	N/A	Reserved for future use	N/A	N/A
0x20	M	Response Code See Section 3.4.2.4	See Section 3.4.2.4	Used to identify the response to this Control Point.
0x21-0xFF	N/A	Reserved for future use	N/A	N/A

Table 3.3: User Control Point Procedure Requirements

3.4.2 User Control Point Behavioral Description

The User Control Point is used by a Client to control certain behaviors of the Server. Procedures are triggered by a Write to this characteristic value that includes an Op Code specifying the operation (See [Table 3.3](#)) which may be followed by a Parameter that is valid within the context of that Op Code.

Where used, the format of the Consent Code is a UINT16 value in the range of 0x0000 to 0x270F (i.e. 0 to 9999). The values from 0x2710 to 0xFFFF are reserved for future use.

Where used, the format of the User Index value is the same as the format of the User Index characteristic defined in [2].

Refer also to Section 8 for informative message sequence charts for the User Control Point procedures.

3.4.2.1 Register New User Procedure

When the *Register New User* Op Code is written to the User Control Point (along with the Consent Code), the Server shall create new records for the new user with the supported UDS Characteristics initialized to default values. The Server shall also assign an available User Index value to the new user. Additionally, the Server shall store the Consent Code Parameter for future use (i.e. when the Client uses the Consent procedure defined in Section 3.4.2.2). The format of the Parameter Value of this Control Point is defined in Section 3.4.2.

The response shall be indicated when the Register New User Procedure is completed using the *Response Code* Op Code, the *Request Op Code* along with the appropriate *Response Value* as defined in Section 3.4.2.4.

If the Server supports only one user and if a user has already been registered, the Server should delete the existing record of UDS Characteristic values and create a new record for the new user. This is to ensure that devices without a User Interface can be reconfigured.

If the operation results in an error condition where the User Control Point cannot be indicated (i.e. the Client Characteristic Configuration descriptor is not configured for indication or if a procedure is already in progress), see Section 3.4.3 for details on handling this condition.

3.4.2.2 Consent Procedure

When the *Consent* Op Code is written to the User Control Point (along with the User Index followed by the Consent Code sent as parameters to this Op Code), the Server shall compare the Consent Code associated to the User Index with its internal Consent Code for the user. The Consent Code and the User Index are used by the Server to grant access to the UDS Characteristics exposed by the Server. The format of the User Index and the Consent Code Parameter are defined in Section 3.4.2. The response shall be indicated when the Consent procedure has completed using the *Response Code* Op Code, the *Request Op Code* along with the appropriate *Response Value* as defined in Section 3.4.2.4.

When this procedure succeeds, the Server shall populate the value of the User Index characteristic with the value of the User Index Parameter. The Server shall also populate the values of the UDS Characteristics with the values belonging to the user that has given consent.

If the operation results in an error condition where the User Control Point cannot be indicated (i.e. the Client Characteristic Configuration descriptor is not configured for indication or if a procedure is already in progress or if the number of attempts reaches the maximum number allowed by the Server), see Section 3.4.3 for details on handling this condition.

3.4.2.3 Delete User Data Procedure

When the *Delete User Data* Op Code is written to the User Control Point, the Server shall delete the user data of the current user as well as its Consent Code (i.e. the user data is no longer accessible). The User

Index characteristic value shall be set to 0xFF (Unknown User). The response shall be indicated using the *Response Code Op Code*, the *Request Op Code*, along with the appropriate *Response Value* as defined in Section 3.4.2.4.

If the operation results in an error condition where the User Control Point cannot be indicated (i.e. the Client Characteristic Configuration descriptor is not configured for indication or if a procedure is already in progress), see Section 3.4.3 for details on handling this condition.

3.4.2.4 Procedure Complete

When the procedures described in Sections 3.4.2.1, 3.4.2.2 and 3.4.2.3 have been executed by the Server or if the procedure generated an error as defined below in this section, the Server shall indicate the User Control Point to the Client. The format of the indication is defined in Table 3.4.

	LSO			MSO
	Response Code Op Code	Request Op Code	Response Value	Response Parameter (if present)
Byte Order	N/A	N/A	N/A	LSO...MSO
Data type	UINT8	UINT8	UINT8	See Table 3.5
Size	1 octet	1 octet	1 octet	0 to 17 octets

Table 3.4: User Control Point characteristic – Parameter Value Format of the Response Indication

The Op Code field shall be set to 0x20.

The Request Op Code field shall be set to the value of the Op Code representing the requested procedure.

Table 3.5 defines the Response Values for the User Control Point.

Response Value	Definition	Request Op Code	Response Parameter
0x00	Reserved For Future Use	N/A	N/A
0x01	Success	Register New User	User Index (UINT8)
		Consent, Delete User Data	None
0x02	Op Code not supported	Unassigned Op Code (RFU)	None
0x03	Invalid Parameter	Register New User, Consent	None

0x04	Operation Failed	Register New User, Consent	None
0x05	User Not Authorized	Delete User Data, Consent	None
0x05-0xFF	Reserved For Future Use	N/A	N/A

Table 3.5: User Control Point characteristic – Response Values

If an Op Code is written to the User Control Point that results in a success operation, the Server, after sending a Write Response, shall indicate the User Control Point with the Response Code Op Code, the Request Op Code and the Response Value set to “Success”.

If an Op Code is written to the User Control Point characteristic that is unsupported by the Server (e.g. an Op Code that is Reserved for Future Use), the Server, after sending a Write Response, shall indicate the User Control Point with a *Response Code Op Code*, the *Request Op Code* and *Response Value* set to *Op Code Not Supported*.

If the Client attempts to use the Register New User procedure of the User Control Point defined in Section 3.4.2.1, and when there is no space available for a new user, the Server, after sending a Write Response, shall indicate the User Control Point with a *Response Code Op Code*, the *Request Op Code* and *Response Value* set to *Operation Failed*.

If a Parameter is written to the User Control Point characteristic that is invalid (e.g., the Client writes the *Create New User Op Code*, or the *Consent Op Code* with a Parameter that is improperly formatted or the User Index is set to 0xFF), the Server, after sending a Write Response, shall indicate the User Control Point with a *Response Code Op Code*, the *Request Op Code* and *Response Value* set to *Invalid Parameter*.

If the Client attempts to use the Consent procedure of the User Control Point defined in Section 3.4.2.2, with a User Index and a Consent Code that does not match the value in the Server, the Server, after sending a Write Response, shall indicate the User Control Point with a *Response Code Op Code*, the *Request Op Code* and *Response Value* set to *User Not Authorized*.

However, if the Client exceeds the maximum number of consent tries (i.e. Consent procedure defined in Section 3.4.2.2) defined by the Server without success (e.g. typically 3 or 4), the Server, after sending a Write Response, shall indicate the User Control Point with a *Response Code Op Code*, the *Request Op Code* and *Response Value* set to *Operation Failed*. In order to unlock the Server for that particular user, the user may perform an action on the Server, or any other mechanisms left to the implementation may be used.

If the Client attempts to use the Delete User Data procedure of the User Control Point defined in Section 3.4.2.3, and if no user has given consent, the Server, after sending a Write Response, shall indicate the User Control Point with a *Response Code Op Code*, the *Request Op Code* and *Response Value* set to *User Not Authorized*.

If the operation results in an error condition that cannot be reported to the Client using the User Control Point (e.g. the User Control Point cannot be indicated), see Section 3.4.3 for details on handling this condition.

3.4.3 General Error Handling procedures

Other than error handling procedures that are specific to certain Op Codes, the following apply:

If an Op Code is written to the User Control Point characteristic while the Server is performing a previously triggered User Control Point operation (i.e., resulting from invalid Client behavior), the Server shall return an error response with the Attribute Protocol error code set to *Procedure Already In Progress* as defined in CSS Part B, Section 1.2 [3].

If an Op Code is written to the User Control Point characteristic and the *Client Characteristic Configuration* descriptor of the User Control Point is not configured for indications, the Server shall return an error response with the Attribute Protocol error code set to *Client Characteristic Configuration Descriptor Improperly Configured* as defined in CSS Part B, Section 1.2 [3].

3.4.4 Procedure Timeout

In the context of the User Control Point characteristic, a procedure is started when a write to the User Control Point characteristic is successfully completed (i.e., the Server sends a Write Response). When a procedure is complete, the Server shall indicate the User Control Point with the Op Code set to *Response Code*.

In the context of the User Control Point characteristic, a procedure is not considered started and not queued in the Server when a write to the User Control Point results in an error response with the Attribute Protocol error code defined in CSS Part B, Section 1.2 [3].

4 SDP Interoperability

If this service is exposed over BR/EDR then it shall have the following SDP record.

Item	Definition	Type	Value	Status
Service Class ID List				M
Service Class #0		UUID	«User Data Service»	M
Protocol Descriptor List				M
Protocol #0		UUID	L2CAP	M
Parameter #0 for Protocol #0	PSM	Uint16	PSM = ATT	M
Protocol #1		UUID	ATT	M
Parameter #0 for Protocol #1	GATT Start Handle	Uint16	First handle of this service in the GATT database	M
Parameter #1 for Protocol #1	GATT End Handle	Uint16	Last handle of this service in the GATT database	M
BrowseGroupList			PublicBrowseRoot*	M

Table 4.1: SDP Record

* PublicBrowseRoot shall be present; however, other browse UUIDs may also be included in the list.

5 Acronyms and Abbreviations

Abbreviation or Acronym	Meaning
AMP	Alternate MAC PHY
ATT	Attribute Protocol
BR/EDR	Basic Rate / Enhanced Data Rate
GAP	Generic Access Profile
GATT	Generic Attribute Profile
LE	Low Energy
RFU	Reserved for Future Use
SDP	Service Discovery Protocol
UDS	User Data Service
UI	User Interface
UUID	Universally Unique Identifier

Table 5.1: *Abbreviations and Acronyms*

6 References

- [1] Bluetooth Core Specification v4.0 or later version of the Core Specification.
- [2] Characteristic and Descriptor descriptions are accessible via the [Bluetooth SIG Assigned Numbers](#).
- [3] Supplement to the Bluetooth Core Specification, Version 3 or later

7 Appendix A - Recommended Client Behavior (INFORMATIVE)

This Service is aimed to be used in several profiles and the Client behavior will be integrated within other Profiles (e.g. the Weight Scale Profile) to define Client behavior. This section provides recommendations for UDS integration into profiles and can be used as guidance for Profile developers.

This section provides recommendation for two types of Clients.

- 1) A personal Client (e.g. a fitness watch or a mobile phone) should cache the UDS Characteristic values read from a Server as well as the Database Change Increment value. A personal Client may also implement the Server role to share UDS Characteristics with a public Client.
- 2) A public Client (e.g. gym equipment) should not cache the UDS Characteristic values read from a Server when the devices are disconnected. The Database Change Increment characteristic is not meaningful to a public Client.

7.1 General Considerations

When a connection is established, and if the Client needs to access the user data exposed by the Server, the Client is required to use the consent mechanism defined in Section 3.4.

Upon initial configuration, the Client should register a new user by using the procedure defined in Section 3.4.2.1. This procedure requires the user to enter a personal code (i.e. 4-digit code) that will be used as a Consent Code for future connections. When this procedure has completed, the Client will receive the User Index associated with the new user. The Client should cache both, the User Index received by the Server as well as the Consent Code entered by the user in order to facilitate the future connections.

Then, the Client may configure the UDS Characteristic values so the values will be stored in the Server for future use.

When the UDS Characteristic value is updated by the Client, the Client is required to increment the Database Change Increment characteristic value of the Server (i.e. using the GATT Write sub-procedure). The Client should increment the Database Change Increment characteristic value only once, at the end of the update procedure, even if more than one UDS Characteristic value has been updated (e.g. when a user selects the 'save' button).

If the Client is required to support either the Age characteristic or the Date of Birth characteristic, it should support both. When connected to a simple Server with no real time clock (RTC) that exposes only the Age characteristic, the Client should update this characteristic when appropriate.

Later, when the Client initiates a connection to the Server, it should first initiate the Consent procedure defined in Section 3.4.2.2.

When connected, and if a UDS Characteristic value has been updated at the Client (e.g. through its UI), the public Client should write this value to the Server.

The Client should also allow the user to delete his user data records from the Server (e.g. through the Client's UI). The procedure described in Section 3.4.2.3 is typically initiated when requested by the user (e.g. through the UI of the Client).

If the Server includes a Client Characteristic Configuration descriptor in the Database Change Increment, it should configure this descriptor for notification.

If the Client receives a notification of the Database Change Increment characteristic, it should read the UDS Characteristic values it supports in order to use the most recent values.

Clients that implement UDS are required to support the GATT Read Long and GATT Write Long sub-procedures in order to read and write long characteristics exposed by a UDS Server.

7.2 Considerations for Personal Clients

The personal Client, once connected and allowed to access the user data, should read the Database Change Increment characteristic in order to determine whether the local copy of the UDS Characteristic values is the most recent or needs to be refreshed in either the Client or the Server (e.g. the Server or the Client have been updated by another device or through the UI of the Server). The conditions described in [Table 7.1](#) should be considered when the Client compares the local copy of the Database Change Increment value with the one read from the Server.

Condition	Action
Database Change Increment values are equal in both, the Server and the personal Client	The databases are synchronized and do not require any action by the personal Client.
Database Change Increment value of the Server is greater than the value in the personal Client (i.e. the user data at the Server are more recent)	The personal Client should read and cache all the available User Data characteristics from the Server. The Client should also cache the Database Change Increment value for future use.
Database Change Increment value of the Server is less than the value in the personal Client (i.e. the user data at the personal Client are more recent)	The personal Client should write updated User Data characteristics to the Server. When the user data are updated, the personal Client should also write its local Database Change Increment value in order to complete the synchronization procedure.

Table 7.1: Recommended Personal Client Behavior for Database Synchronization

The personal Client may also provide a manual synchronization mechanism (e.g. through its UI) to allow the user to write its local UDS Characteristic values to the Server or to read all the values from the Server regardless of the value of the Database Change Increment characteristic value.

The personal Client should increment by one its local Database Change Increment value each time the UDS Characteristics are updated through its UI at the end of the updated procedure (e.g. when the user presses the 'save' button).

The public Client, once connected and allowed to access the user data, should read the UDS Characteristics it supports each time a connection is established with a Server.

8 Appendix B – User Control Point Message Sequence Charts (INFORMATIVE)

The following sections show message sequence charts for the User Control Point procedures defined in Section 3.4.2.

8.1 Register New User Procedure



