ISO/IEC 14543-5-104

Edition 1.0 2024-01

INTERNATIONAL STANDARD

colour inside

Information technology – Home electronic system (HES) architecture – Part 5-104: Intelligent grouping and resource sharing for HES Class 2 and Class 3 – RA server-based smart lock application

IEC Secretariat
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee, …). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

IEC Products & Services Portal - products.iec.ch
Discover our powerful search engine and read freely all the publications previews. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 500 terminological entries in English and French, with equivalent terms in 25 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

ISO/IEC 14543-5-104

Edition 1.0 2024-01

INTERNATIONAL STANDARD

colour inside

Information technology – Home electronic system (HES) architecture – Part 5-104: Intelligent grouping and resource sharing for HES Class 2 and Class 3 – RA server-based smart lock application

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 35.240.67

ISBN 978-2-8322-8091-1

CONTENTS

INFORMATION TECHNOLOGY –
HOME ELECTRONIC SYSTEM (HES) ARCHITECTURE –

Part 5-104: Intelligent grouping and resource sharing for HES Class 2 and Class 3 – RA server-based smart lock application

FOREWORD

1) ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

2) The formal decisions or agreements of IEC and ISO on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC and ISO National bodies.

3) IEC and ISO documents have the form of recommendations for international use and are accepted by IEC and ISO National bodies in that sense. While all reasonable efforts are made to ensure that the technical content of IEC and ISO documents is accurate, IEC and ISO cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.

4) In order to promote international uniformity, IEC and ISO National bodies undertake to apply IEC and ISO documents transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC and ISO document and the corresponding national or regional publication shall be clearly indicated in the latter.

5) IEC and ISO do not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC and ISO marks of conformity. IEC and ISO are not responsible for any services carried out by independent certification bodies.

6) All users should ensure that they have the latest edition of this document.

7) No liability shall attach to IEC and ISO or their directors, employees, servants or agents including individual experts and members of its technical committees and IEC and ISO National bodies for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this ISO/IEC document or any other IEC and ISO documents.

8) Attention is drawn to the Normative references cited in this document. Use of the referenced publications is indispensable for the correct application of this document.

9) IEC and ISO draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). IEC and ISO take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, IEC and ISO had not received notice of (a) patent(s), which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at https://patents.iec.ch and www.iso.org/patents. IEC and ISO shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 14543-5-104 has been prepared by subcommittee 25: Interconnection of information technology equipment, of ISO/IEC joint technical committee 1: Information technology. It is an International Standard.

The text of this International Standard is based on the following documents:

Draft	Report on voting
JTC1-SC25/3122/CDV	JTC1-SC25/3171/RVC

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this International Standard is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1, available at www.iec.ch/members_experts/refdocs and www.iso.org/directives.

The list of all currently available parts of the ISO/IEC 14543 series, under the general title *Information technology – Home Electronic System (HES) architecture*, can be found on the IEC web site and ISO web site.

IMPORTANT – The "colour inside" logo on the cover page of this document indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

ISO/IEC 14543-5 (all parts) specifies the services and protocol of the application layer for Intelligent Grouping and Resource Sharing (IGRS) devices and services in the Home Electronic System (HES). Some parts reference Classes 1, 2 and 3, which are HES designations specified in the HES architecture standard, ISO/IEC 14543-2-1.

ISO/IEC 14543-5 includes the following parts:

– ISO/IEC 14543-5-1: Core protocol

- Specifies the TCP/IP protocol stack as the basis and the HTTP protocol as the message-exchange framework among devices.
- Specifies a series of device and service interaction/invocation standards, such as device and service discovery protocol, device and service description, service invocation and security mechanisms.
- Specifies core protocols for a type of home network that supports streaming media and other high-speed data transports within a home.

– ISO/IEC 14543-5-2#: Application profile

- Based on the IGRS core protocol.
- Specifies a device and service interaction mechanism, as well as application interfaces used in IGRS basic applications.
- Multiple application profiles are specified, including:

  a) ISO/IEC 14543-5-21: AV profile

  b) ISO/IEC 14543-5-22: File profile

– ISO/IEC 14543-5-3: Basic application

- Includes an IGRS basic application list.
- Specifies a basic application framework.
- Specifies operation details (device grouping, service description template, etc.), function definitions and service invocation interfaces.

– ISO/IEC 14543-5-4: Device validation

- Specifies a standard method to validate an IGRS-compliant device.

– ISO/IEC 14543-5-5: Device type

- Specifies IGRS device types used in IGRS applications.

– ISO/IEC 14543-5-6: Service type

- Specifies basic service types used in IGRS applications.

– ISO/IEC 14543-5-7: Remote access system architecture

- Specifies the architecture and framework for remotely accessing IGRS devices and services in the Home Electronic System. The remote access (RA) communications protocol and application profiles are specified in the following parts of ISO/IEC 14543-5:
- ISO/IEC 14543-5-8: Remote access core protocol
- ISO/IEC 14543-5-9: Remote access service platform
- ISO/IEC 14543-5-101: Remote media access profile
- ISO/IEC 14543-5-102: Remote universal management profile
- ISO/IEC 14543-5-103: RA Smart audio interconnection profile
- ISO/IEC 14543-5-104: RA server-based smart lock application
- ISO/IEC 14543-5-105: RA server-based smart lock application test and verification (under development)

  - ISO/IEC 14543-5-11: Remote user interface
  - ISO/IEC 14543-5-12: Remote access test and verification
  - ISO/IEC 14543-5-13: RA Smart home device control using voice recognition (under development)
  - ISO/IEC 14543-5-141: Blockchain application protocols for HES based on IGRS RA specifications: core framework (under development)
  - The relationships among these parts are specified in Part 5-7.

- ISO/IEC 14543-5-8: Remote access core protocol
  - Provides detailed system components, system function modules, basic concepts of IGRS remote access elements and their relationships, message exchange mechanisms and security related specifications.
  - Specifies interfaces between IGRS remote access (RA) client and service platforms. Defines co-operative procedures among IGRS RA clients.
- ISO/IEC 14543-5-9: Remote access service platform
  - Specifies the IGRS RA service platform (IRSP) architectures and interfaces among servers in the service platforms.
  - Based on ISO/IEC 14543-5-8: Remote access core protocol.
- ISO/IEC 14543-5-10#: Remote access application profiles
  - Specifies a device and service interaction mechanism for various applications.
  - Based on ISO/IEC 14543-5-8: Remote access core protocol.
  - ISO/IEC 14543-5-101: Remote media access profile. This part specifies the common requirements for IGRS RA media users and devices in IGRS networks.
  - ISO/IEC 14543-5-102: Remote universal management profile. This part specifies a mechanism for integrating devices with both relatively high and low processing capabilities into IGRS networks. It also specifies universal remote device discovery and a management framework.

  Some of the profiles are under development, including:

  - ISO/IEC 14543-5-103: RA smart audio interconnection profile. This part specifies the interoperability requirements for smart audio devices (audio devices with built-in computing and communication capabilities) and creates various application functionalities to enhance these audio devices. It introduces some new device types and specifies the mandatory device/service discovery, device control, content delivery and audio transcoding methods and interfaces, etc. to enable smart audio device interactions and content services.
  - ISO/IEC 14543-5-104: RA server-based smart lock application. This part specifies a server-based smart lock application that utilizes the ISO/IEC 14543-5 series of standards for device interoperability. It specifies the required device interaction models, message formats and APIs and the authentication and security methods.
  - ISO/IEC 14543-5-105: RA server-based smart lock application test and verification (under development). This part is the verification test specification for ISO/IEC 14543-5-104. It describes the required test cases and relevant pass/fail criteria to validate that a server-based smart lock device/application conforms to the ISO/IEC 14543-5 series of standard protocols (IGRS).
  - Additional application profiles will be specified in the future.
- ISO/IEC 14543-5-11: Remote user interface
  - Specifies adaptive user interface generation and remote device control mechanisms suitable for different remote access applications and devices.
- ISO/IEC 14543-5-12: Remote access test and verification
  - Specifies a standard method to test and verify IGRS-RA compliant device and service interfaces.

– ISO/IEC 14543-5-13: RA smart home device control using voice recognition (under development)

- Specifies the requirements to allow remote access and control of various smart home devices that use the same IGRS RA device interoperability protocols with a variety of voice recognition platforms. This part extends current IGRS RA device types to support the addition of voice recognition message format specifications. It introduces an IGRS RA voice-enabled gateway profile in compliance with the HES gateway (ISO/IEC 15045 series and ISO/IEC 18012 series) and the IGRS RA platform. It extends the HES environment to an external voice recognition service platform (“cross-platform” voice recognition interface platform) that includes specifications for universal voice recognition skill sets and translation interface service, platform security, IGRS RA (IGRS Remote Access Service Platform) message server API, and IGRS RA device control protocol parsing and status update service, etc.

– ISO/IEC 14543-5-14#: Blockchain application protocols for HES based on IGRS RA specifications (under development)

- Specifies a blockchain application framework and profiles for various smart home HES applications.
- Based on the ISO/IEC 14543-5-8: Remote access core protocol.
- Some of the profiles are under development, including ISO/IEC 14543-5-141: Blockchain application protocols for HES based on the IGRS RA specifications: core framework. This is the first in a series of standards that specifies a blockchain application framework to enhance the HES architecture using IGRS RA protocols. Blockchain technology provides additional data storage protection and a trusted authentication mechanism that includes a secure data exchange process. This standard specifies the core framework requirements that establish a reference system architecture, interaction model, blockchain identity authentication, blockchain encryption-method requirements, generic data format template, RA server interface and configuration specification.

INFORMATION TECHNOLOGY – HOME ELECTRONIC SYSTEM (HES) ARCHITECTURE –

Part 5-104: Intelligent grouping and resource sharing for HES Class 2 and Class 3 – RA server-based smart lock application

1 Scope

This part of ISO/IEC 14543-5 specifies the remote access (RA) server-based application framework, device interaction model, flow process and interfaces, and message formats to achieve intelligent grouping, resource sharing and service collaboration among IGRS smart lock devices.

This document is applicable to smart lock devices with direct network connections or connections through an intermediary network to a server for security authentication. This server utilizes a method to minimize the possibility of unauthorized access to these smart locks, while maintaining seamless interoperability among users, smart lock devices and RA servers at home, office or other remote environments.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 14543-5-8, *Information technology – Home Electronic System (HES) architecture – Part 5-8: Intelligent grouping and resource sharing for Class 2 and Class 3 – Remote access core protocol*

ISO/IEC 14543-5-9, *Information technology – Home Electronic System (HES) architecture – Part 5-9: Intelligent grouping and resource sharing for Class 2 and Class 3 – Remote access service platform*

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 14543-5-8, ISO/IEC 14543-5-9 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- IEC Electropedia: available at https://www.electropedia.org/
- ISO Online browsing platform: available at https://www.iso.org/obp

3.1.1
Bluetooth gateway

device that forwards the communication data between a Bluetooth smart lock device (BSLD) and the remote access server (RAS) in the Bluetooth smart lock server management framework (BSLSMF)

Note 1 to entry: A Bluetooth gateway is an implementation of the HES gateway, as specified in 6.4.

3.1.2
Bluetooth smart lock device

lock device that supports Bluetooth 4.0 or above protocol and conforms to the communications protocol and message format specified in this document

3.1.3
Bluetooth smart lock server management framework

server-based remote access framework to manage, authenticate and control Bluetooth smart lock devices

3.1.4
IGRS RA agent service

functional entity that provides the IGRS RA service to IGRS LAN devices

Note 1 to entry: The main functionalities of the IGRS RA agent service are sending instructions to and receiving instructions from the IGRS RA service platform, and translating the instructions of local IGRS networks to and from those of the IGRS RA networks. The IGRS RA agent service provides audio services compatibility between the local IGRS devices and the IGRS RA devices.

3.1.5
remote access client

logical device that a user controls to interact with Bluetooth smart lock devices in a BSLSMF

Note 1 to entry: Typical remote access client (RAC) devices may include: mobile phones, tablets and similar mobile devices etc. In a BSLD control application, an RAC is the terminal device that controls the BSLD in real time and interconnects with the RAS to access relevant data over basic network services such as Wi-Fi, 3G, 4G, and 5G. It is capable of responding to user actions, collecting and updating Bluetooth smart lock device status and other information to users and the RAS.

3.1.6
remote access server

logical device that manages Bluetooth smart lock devices in a BSLSMF

Note 1 to entry: Typical remote access server (RAS) devices include PCs and network storage servers. In a BSLD control application, the RAS is the content management source for an RAC to access via pre-defined interfaces. It is capable of obtaining, processing and storing BSLD information from an RAC, and will respond to RAC requests when certain conditions are met.

3.2 Abbreviated terms

BGW	Bluetooth gateway
BSLD	Bluetooth smart lock device
BSLDM	Bluetooth smart lock device manager
BSLSMF	Bluetooth smart lock server management framework
DDMS	device data management service
HTTP	hypertext transfer protocol
HTTPS	hypertext transfer protocol over secure socket layer
ID	identification
IRSP	IGRS RA service platform
RAC	remote access client
RAS	remote access server

SASL	simple authentication and security layer
SCS	security certification service
TCP/IP	transmission control protocol/Internet protocol
TLS	transport layer security
TPSP	third party service platform
UDMS	user data management service
XMPP	extensible messaging and presence protocol

4 Conformance

A system that conforms to this document shall be implemented in accordance with Clauses 6 through 8, where the IGRS smart lock server management framework – which includes system architecture, interaction models and processes, device functions and services – shall conform to Clause 6, and the standard interfaces and message formats shall conform to Clause 7 and Clause 8, respectively.

5 Overview

This IGRS RA server-based smart lock application standard provides a complete framework to ensure that BSLDs manufactured by different vendors interoperate seamlessly with an RAS and RAC for enhanced device control and secure data management support.

This document includes all of the required device interaction models, message flow methods, control message formats, APIs and the authentication and security methods. The BSLSMF uses a server-based authentication mechanism to minimize the possibility of unauthorized access to the lock and to increase home safety. It is also possible for a third party service platform (TPSP) to access the BSLSMF with a set of management control interfaces to the BSLD, thus enabling many different data or security service functions not specified in this document.

6 Smart lock server management framework

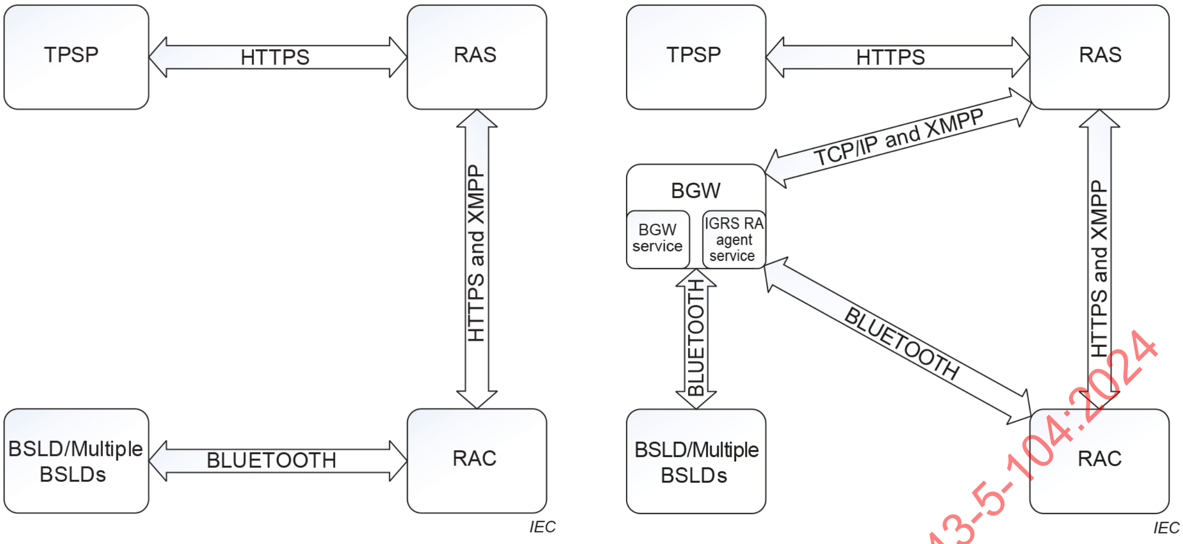
6.1 Overview

The BSLSMF shall provide management, operation and maintenance of BSLDs made by different manufacturers. The end users can use various RACs developed by these BSLD manufacturers to add their own BSLDs to BSLSMF for control management.

In a BSLSMF, each BSLD shall create and upload required device data information to an RAS, which is then shown to the user via the RAC. The RAS is used to record and manage the permission rights, security information, and operational status of each BLSD. The BSLSMF also supports the RAS to provide interface specifications for third party service platforms to access, so the user may connect to other secure data and functional service platforms available on the market in order to expand and complement the standard control methods and data access channels currently allowed by BSLD.

There are two alternatives for the interaction model of the Bluetooth®[1] smart lock device in the server management framework. The first alternative, as shown in Figure 1 a), is for operation with conventional Internet access means without a gateway. The second alternative, as shown in Figure 1 b), provides compliance with the HES gateway to enhance privacy, security, safety, and interoperability capabilities.

[1] Bluetooth® is the registered trademark of Bluetooth SIG, Inc. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO and IEC.



a) **Conventional Internet access**

b) **HES gateway access**

Figure 1 – Interaction models of Bluetooth smart lock device in the server management framework

The RAS, RAC, BGW and BSLD are key components in the BSLSMF, which comprise the device and data management and control process. In this model, the request and response and push message (see 7.7 for specific data formats) communication between the RAS and RAC is based on HTTPS, as specified in IETF RFC 2818, and XMPP protocol requirements specified in ISO/IEC 14543-5-8 for user registration, authentication and basic message flow. A Bluetooth connection is used for authentication and control command message transfer between an RAC and the BSLD.

NOTE Other relevant security mechanisms that can be considered for data transport include SASL (IETF RFC 4422) and TLS (IETF RFC 5246). See the Bibliography for the Bluetooth specification.

The BGW is mainly responsible for establishing the real-time management and remote access of the BSLD. In this scenario, the BSLD is connected through the BGW (via Bluetooth) to the RAS using TCP/IP and XMPP connection (see ISO/IEC 14543-5-8 for device registration, connection and message flow).

BSLSMF has specified a complete system for the secure management and control of BSLD. This framework also supports an optional TPSP that may connect to the RAS through a standard management control interface using HTTPS to offer additional security features or services to the BSLD.

Typical server-based smart lock application scenarios are described as follows.

a) The user can access a BSLD locally through an RAC (e.g. mobile phone, tablet). The RAC interacts with the RAS (e.g. message and application servers that support IRSP protocols and relevant user and device management and data application services) to authenticate and retrieve the relevant data, which then allows the user to see the BSLD status and access information data displayed on the RAC (see conventional Internet access model in Figure 1 a).

b) The user can also access a BSLD that links to a BGW with a persistent connection to the RAS, remotely through an RAC (e.g. mobile phone, tablet). The RAC interacts with RAS to authenticate and retrieve the relevant data, which then allows the user to see the BSLD status and access information data displayed on the RAC (see HES gateway access model in Figure 1 b).

c) The user can manage multiple BSLDs through the RAC with connections to RAS by assigning temporary guest rights to other users, and can receive instant notifications on the operational status (on, off, etc.) of these BSLDs after each status change.

The RAS described in scenarios a), b) and c) may be either a local server or a remote cloud-based server. A remote cloud-based RAS provides more flexibility in enabling different user access methods and serves as a possible path for delivering valued-added data services (including third-party services) to BSLD devices. However, this usually relies on some service providers to maintain the application servers for the user and device management and may be more susceptible to public network attacks. Local RAS deployment, on the other hand, is often more secure with better data privacy protection, but typically offers fewer features and requires more of the user’s involvement in order to obtain future upgrades.

6.2 Bluetooth smart lock server management framework: remote access server (RAS)

The BSLSMF RAS shall comform to ISO/IEC 14543-5-8 and ISO/IEC 14543-5-9 to provide basic registration, authentication, remote access connection, message transport and management control interfaces to the RAC, BGW, BSLD and TPSP. It shall support HTTPS, TCP/IP and XMPP protocols and shall be capable of processing and storing data.

The basic components of the BSLSMF RAS are shown in Figure 2.

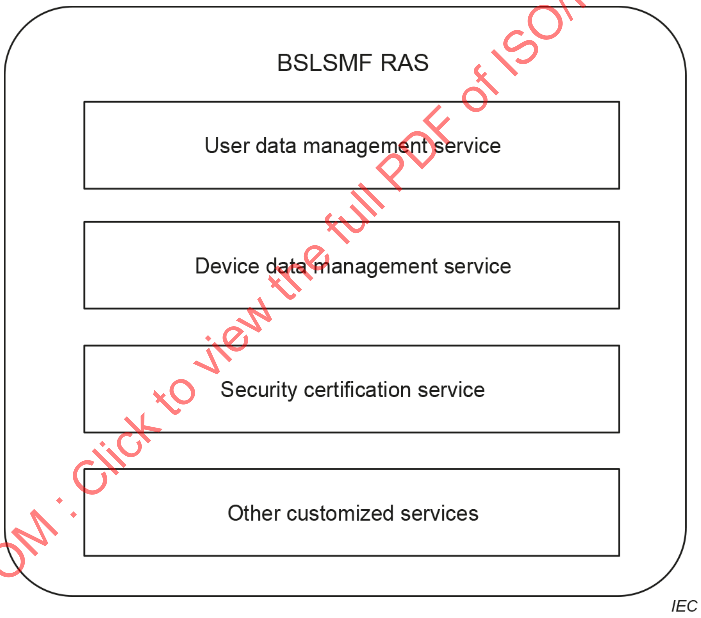

BSLSMF RAS
User data management service
Device data management service
Security certification service
Other customized services
IEC

Figure 2 – BSLSMF RAS components

The BSLSMF RAS is one of the key components in the BSLSMF and shall provide data services to an RAC and manage a BSLD. It includes user data management service (UDMS), device data management service (DDMS), security certification service (SCS) and other customized services.

The various services in the BSLSMF RAS are specified as follows.

a) UDMS: Each user shall create an account in the RAS to store user data provided by an RAC at the time of connection. These user data include:
   1) Phone number: mobile phone number, which is used to verify user identity;
   2) Email address: commonly used email address, which is used to verify user identity;
   3) Password: account password that consists of a string of 6 to 18 characters including letters and numbers, which is used to verify account legitimacy.

After one or multiple users have successfully established a binding relationship to a BSLD, the RAS shall store this relationship data and authenticate user account legitimacy before allowing an RAC to send any operational request to a BSLD.

b) DDMS: After each BSLD joins the RAS, all of the BSLD information shall be stored and managed by the RAS, which then allows the RAC to retrieve the corresponding device data after successful authentication. A single BSLD is permitted to bind with multiple users.

In the BSLSMF, each BSLD shall be authenticated when connecting to the RAS via the RAC.

c) SCS: The data in the RAS shall only be provided to a legitimate RAC to ensure the security of each BSLD. When an RAC sends a request to obtain BSLD data, the RAS shall first authenticate the user information provided by the RAC. Once the authentication passes, the RAS shall then send the relevant information to the RAC using AES128 CBC encryption.

d) The RAS also supports a number of other customized services based on different smart lock applications.

6.3 Bluetooth smart lock server management framework: remote access client (RAC)

An RAC is the client that interacts with a user to access and manage a BSLD. A typical RAC can simply be an application on a mobile phone or tablet device. The RAC shall use Bluetooth to discover nearby BSLDs and add them to the BSLSMF RAS for future access.

Through the RAC, the user shall be able to request data from the RAS in order to gain access to certain information about the user and a relevant BSLD. The management function on the RAC shall allow the user to add, modify and delete BSLD information.

The basic components of BSLSMF RAC are shown in Figure 3.

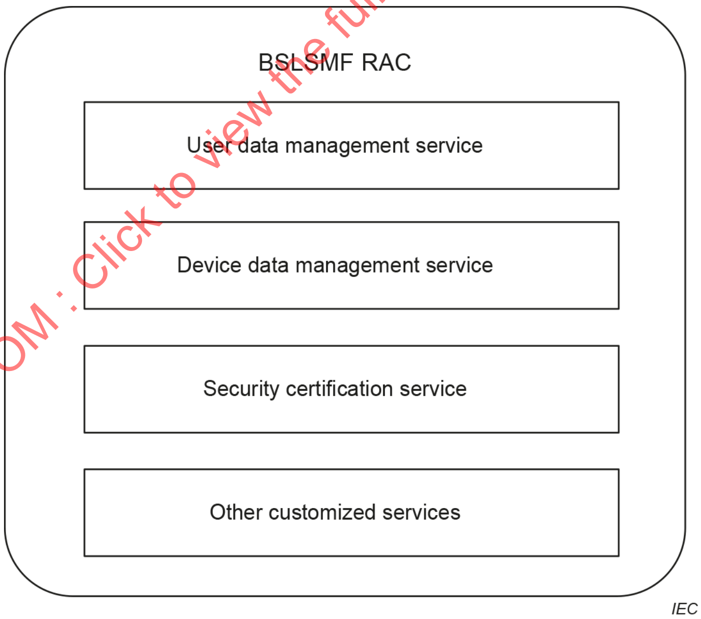

BSLSMF RAC
User data management service
Device data management service
Security certification service
Other customized services
IEC

Figure 3 – BSLSMF RAC components

The RAC shall provide user data management service (UDMS), device data management service (DDMS), security certification service (SCS), and a number of other customized services. Before presenting BSLD and account information to the user, an RAC shall first send a request to the RAS to retrieve the relevant data. The RAC gathers the UDMS and DDMS from the RAS and is synchronous within the RAC. Any updates to the UDMS and DDMS performed by the RAC are reflected back up to the RAS.

The various services in a BSLSMF RAC are specified as follows.

a) UDMS: An RAC should provide a visual interface for users to check and manage their account information after authentication. The user account data include:

   1) Phone number: mobile phone number, which is used to verify user identity;

   2) Email address: commonly used email address, which is used to verify user identity;

   3) Password: account password that consists of a string of 6 to 18 characters including letters and numbers, which is used to verify account legitimacy.

b) DDMS: An RAC shall allow the user to check all BSLDs that bind to the account and support the addition of a new BSLD and the modification and deletion of any existing BSLDs. Moreover, the RAC shall also be able to check and modify BSLD attributes during operation. BSLD attributes include:

   1) Status: current status of the BSLD;

   2) Firmware version: current device firmware version, e.g. 1.0; it is used to verify software for any future update;

   3) Operation record: all past operation information on the device.

c) SCS: An RAC shall authenticate the user whenever the user is attempting to add a BSLD, retrieve BSLD user information and access BSLD. In addition, the RAC shall also verify that the same user account is not being used by a different RAC when retrieving BSLD information. The BSLSMF RAS shall not allow the same user to use different RACs to access a BSLD at the same time. Each BSLD ID shall be unique when the RAC adds a new BSLD to the BSLSMF. The data transport shall use AES128 CBC-based encryption for security.

d) An RAC also supports a number of other customized services based on different smart lock applications.

6.4 Bluetooth smart lock server management framework: Bluetooth gateway (BGW)

The BGW shall be used for forwarding data between the BSLD and the RAS. When the BSLD status changes or updates data to the RAS, the BSLD shall establish a connection with the BGW via Bluetooth and then send the data to the BGW, which forwards the data to the RAS. The BGW shall first complete a registration process (see ISO/IEC 14543-5-8) with the RAS before any connection is established. After a successful authentication process, the BGW shall establish a TCP/IP connection to the RAS. Data transmission between the BGW and the BSLD shall require security certification. AES128 CBC encryption shall be used for all data transports.

Through the RAC, the user shall access the BSLD that interconnects to a BGW (if present in the system) both locally (via Bluetooth) and remotely (via connection to the RAS).

The basic components of BSLSMF BGW are shown in Figure 4.

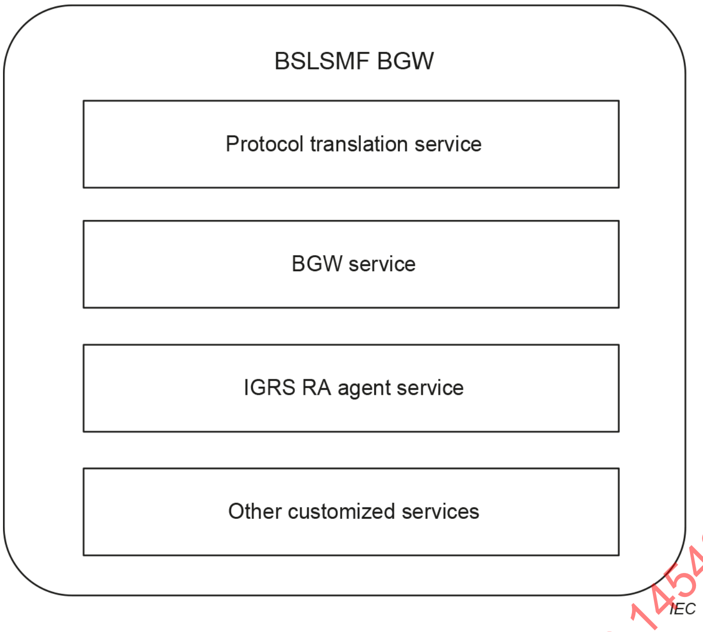


Figure 4 – BSLSMF BGW components

The BGW shall provide protocol translation service, BGW service, IGRS RA agent service, and a number of other customized services.

The various services in a BSLSMF BGW are specified as follows.

a) Protocol translation service: after interconnecting with various RAC and BSLD devices in the home via Bluetooth: this service mainly functions as a translation service that extracts invoked Bluetooth protocol services or messages and converts to the relevant command messages defined in this document and the IGRS protocols defined in ISO/IEC 14543-5-8.

b) BGW service: implementation of the BGW service will be specified in the future International Standard ISO/IEC 18012-3.

c) IGRS RA agent service: sends instructions to and receives instructions from the IGRS RA service platform, and translates the instructions of local IGRS networks to and from those of the IGRS RA networks.

d) A BGW also supports a number of other customized services based on different smart lock applications.

The BGW enables interactions between IGRS RAC devices and BSLD devices in the home. The BGW is an implementation of the HES gateway (ISO/IEC 15045 series and ISO/IEC 18012 series) that includes a service functioning as an IGRS RA agent, which is used for those BSLD devices that cannot be discovered over the Internet as shown in Figure 1 b). All IGRS RAC devices and the IGRS RAS shall use published IGRS protocols (ISO/IEC 14543-5-8) to discover and interconnect with each other.

The BGW message flow process with the RAS and BSLD is shown in Figure 5.

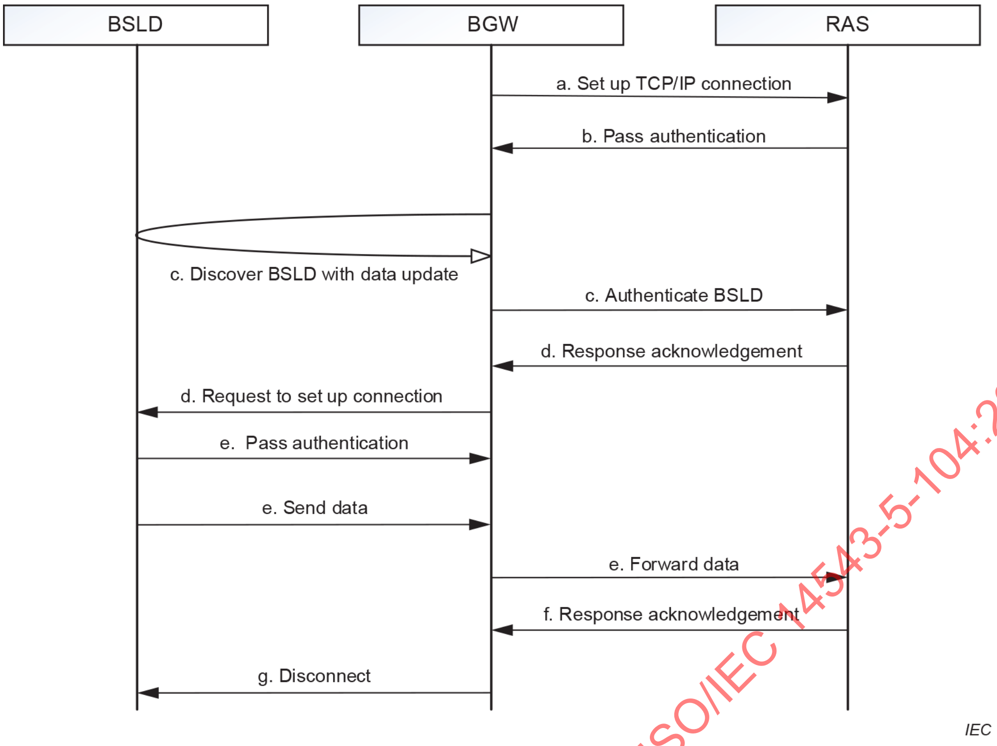

BSLD
BGW
RAS
a. Set up TCP/IP connection
b. Pass authentication
c. Discover BSLD with data update
c. Authenticate BSLD
d. Response acknowledgement
d. Request to set up connection
e. Pass authentication
e. Send data
e. Forward data
f. Response acknowledgement
g. Disconnect
IEC

Figure 5 – BGW message flow process

The BGW message flow process is as follows.

a) The BGW sends a request to set up a TCP/IP connection to the RAS.

b) After the RAS receives the connection request from the BGW, it authenticates the device; and if it has been registered and authenticated, the connection is maintained; otherwise, the connection is off.

c) After the connection between the BGW and the RAS is successfully established, the BGW scans and discovers a nearby BSLD via Bluetooth. If the BGW receives a BSLD broadcast message that indicates there are data updates to the RAS, it first forwards the BSLD information to the RAS for authentication.

d) If the BSLD authentication passes the RAS, the BGW sends a connection request including authentication information to the BSLD. See Clause 8 b) for detailed message format.

e) The BSLD sends the updated data to the RAS through the BGW.

f) The RAS receives the data sent by the BGW and returns a response message.

g) After receiving the response message from the RAS, the BGW disconnects from the BSLD.

6.5 Bluetooth smart lock server management framework: Bluetooth smart lock device (BSLD)

BSLDs produced by different manufacturers that adopt the communication protocols specified in this document shall be able to register in the BSLSMF RAS. The user can control a BSLD via an RAC only after the device has been successfully added to the RAS.

The BSLD shall encrypt all data with AES128 CBC during data transport. After the BSLD is registered in the RAS, the RAC shall write the account information to the BSLD via Bluetooth, which is then used for authentication during subsequent connections.

The BSLD registration process to the RAS is shown in Figure 6.

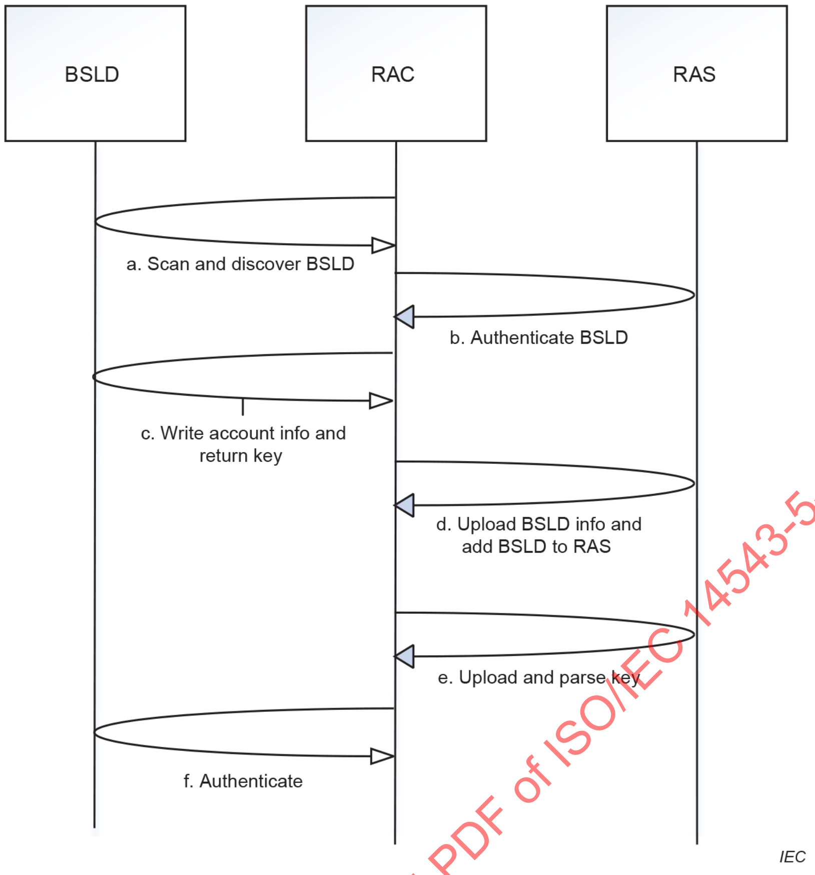

BSLD
RAC
RAS
a. Scan and discover BSLD
b. Authenticate BSLD
c. Write account info and return key
d. Upload BSLD info and add BSLD to RAS
e. Upload and parse key
f. Authenticate
IEC

Figure 6 – BSLD registration process to RAS

The BSLD registration process to the RAS is as follows.

a) After discovering the BSLD through scanning for broadcast data via Bluetooth, the RAC obtains basic information about the BSLD by parsing this broadcast data, which includes:

   1) device unique identifier: globally unique device ID, which usually contains the MAC address of the device and is fixed to 12 characters in length;

   2) device type: the BSLD type, e.g. 0 for hotel lock, 1 for home lock;

   3) device manufacturer identification, which is unique to each BSLD manufacturer;

   4) BLSD device status: status code, e.g. 0 for unregistered, 1 for on, 2 for off.

b) The RAC sends the device unique identifier of the BSLD to the RAS. The RAS authenticates the BSLD device using DDMS and SCS based on this device unique identifier and returns the result to the RAC.

c) After receiving the authentication result from the RAS, the RAC sends the user account information to the BSLD to indicate that this RAC "owns" the BSLD. The BSLD shall save the account information and return a secret key data to the RAC. See Clause 8 a) for the detailed message format.

d) After receiving the secret key data from the BSLD, the RAC sends the basic information about the BSLD to the RAS, which then stores the data and adds it to RAS.

e) After the BSLD is successfully added to the RAS, the RAC uploads the received secret key data to the RAS, which saves and returns it to the RAC after an AES128 CBC decryption process.

f) After the RAC receives the decrypted secret key data from the RAS, the RAC reassembles the key data to generate a new key and then sends the user ID encrypted with the new key to the BSLD. See Clause 8 b) for the detailed message format.

g) The BSLD generates a new secret key using the same algorithm as the method used by RAC in step f). After the BSLD receives the data sent by the RAC, it decrypts the user ID using the new key it generated. If the decrypted user ID matches the saved ID, the current connection is maintained and the result is returned to the RAC. Otherwise, the connection is terminated.

The BSLD control flow process is shown in Figure 7.

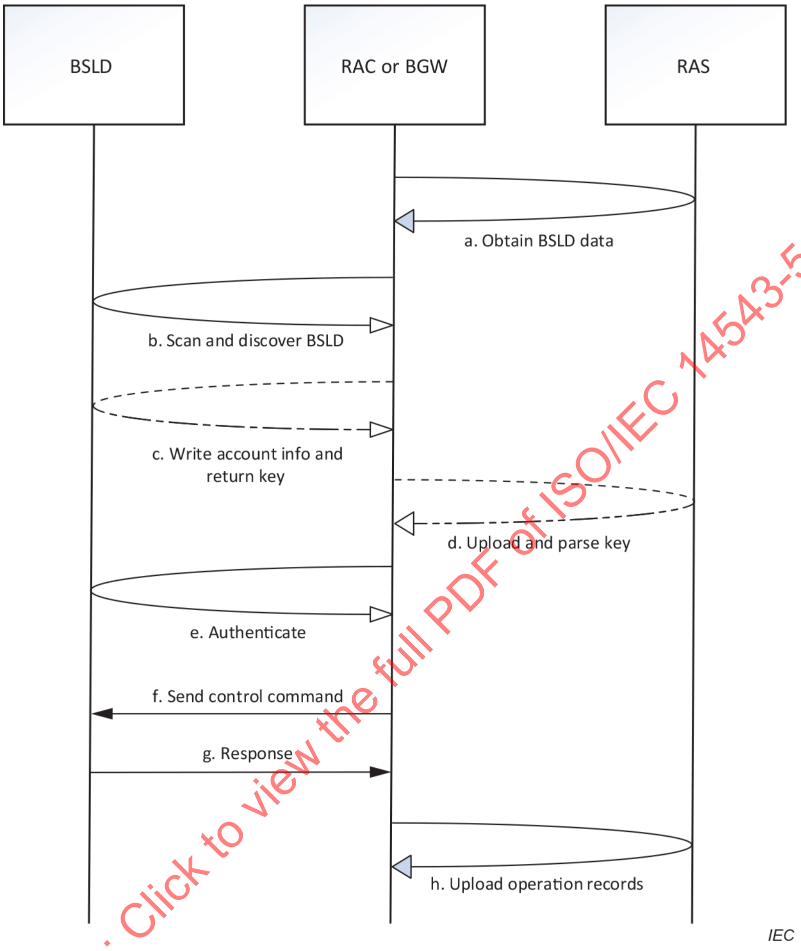


Figure 7 – BSLD control flow process

BSLD control process is as follows:

a) The RAC or BGW first sends a request to the RAS to obtain BSLD data. After the RAS receives the request, it returns BSLD information to the RAC or BGW.

b) After receiving the BSLD information from the RAS, the RAC or BGW scans the nearby BSLDs via Bluetooth. It determines the operational BSLD by comparing the returned device unique identifier.

c) If the BSLD is in an unregistered state, it follows the registration process described in Figure 6. If the BSLD is in a registered state, then the process goes directly to step d).

d) The RAC or BGW establishes a connection to the BSLD via Bluetooth and sends the user ID to the BSLD using AES128 CBC encryption.

e) After the BSLD receives the data sent by the RAC or BGW, it obtains the user ID after decryption. The decrypted ID is compared to the stored user ID. If a match is found, the current connection is maintained. Otherwise, the connection is terminated. See Clause 8 b) for detailed message format.

f) The RAC or BGW sends control commands to the BSLD after it establishes a connection with the BSLD. All commands sent from the RAC or BGW to the BSLD shall be encrypted via AES128 CBC. See Clause 8 c) for detailed message format.

g) After the BSLD receives the command from the RAC or BGW, it decrypts and executes the command, and then returns the result to the RAC or BGW.

h) After receiving the results from the BSLD, the RAC or BGW shall upload the operation records to the RAS to be stored.

NOTE In this framework, both RAC and BGW serve the same function of relaying BSLD messages to the RAS. The main difference is that BGW, which is often a stationary device, is needed for remote RAC access application.

6.6 Bluetooth smart lock server management framework: third party service platform (TPSP)

A TPSP may obtain BSLD related data from the RAS and also send relevant control commands to the RAS to allow for building more diversified application scenarios outside of the standard interaction flow process specified in this document. The BSLSMF supports a standard management control interface based on a BSLD to enable basic access for these TPSPs.

7 Standard interfaces between remote access client and server management framework

7.1 User registration management

The registration request message format sent from the RAC user to the RAS is shown in Figure 8.

http(s)://*RAS domain name*/user/register?phone=*phone number*&email=*email address*&password=*password*

Figure 8 – User registration request message

In Figure 8 to Figure 12, and Figure A.1, italics indicate where content is to be inserted; all other text in message definitions is fixed in this document.

All contents in the message definition are mandatory in this document.

In addition to the mandatory message field requirement in Figure 8, more field contents may be included in the message as extensions to further describe user information.

After receiving the registration request message from the user, the RAS shall return the registration response message; see 7.6 for the HTTP response status code and message contents. HTTP is specified in IETF RFC 2616.

It should be noted that the RAS may also provide more user registration interfaces in addition to the HTTP-based user registration interface.

Annex A shows an example of user registration request and response message exchanged between RAC and RAS.

7.2 User authentication management

The authentication request message format sent from the RAC to the RAS is shown in Figure 9.

http(s)://*RAS domain name/*user/login?account=*mobile phone number or email address*&password=*password*

Figure 9 – User authentication request message

In addition to the mandatory message field requirement in Figure 9, more field contents may be included in the message as extensions to further describe user authentication information.

After receiving the authentication request message from the user, the RAS shall return the authentication response message; see 7.6 for the HTTP response status code and message contents.

The RAS may also provide more user authentication interfaces in addition to the HTTP-based user authentication interface.

7.3 Bluetooth smart lock device (BSLD) discovery

The BSLD authentication request message format from the RAC to the RAS is shown in Figure 10.

http(s)://*RAS domain name/*device/check?token=*User login permission identifier*&identify=*device unique identifier*

Figure 10 – BSLD authentication request message

The "token" is the user login permission identifier returned by the user authentication management interface.

In addition to the mandatory message field requirement in Figure 10, more field contents may be included in the message as extensions.

After receiving a BSLD authentication request message, the RAS shall return the authentication response message; see 7.6 for the HTTP response status code and message contents.

It should be noted that the RAS may also provide more BSLD authentication interfaces in addition to the HTTP-based BSLD authentication interface.

7.4 Bluetooth smart lock device (BSLD) registration management

The BSLD registration request message format sent from the RAC to the RAS is shown in Figure 11.

http(s)://*RAS domain name/*device/register?token=*User login permission identifier*&identify=*device unique identifier*&type=*device type*&vendor=*device manufacturer*

Figure 11 – BSLD registration request message

The "type" and "vendor" fields are optional.

In addition to the mandatory message field requirement in Figure 11, more field contents may be included in the message as extensions.

After receiving a BSLD registration request message, the RAS shall return the registration response message; see 7.6 for HTTP response status code and its message contents.

Each BSLD device identifier is created by an individual smart lock manufacturer and shall be globally unique within the RAS. For authentication purposes, when the RAS checks certain device identifiers sent by an RAC, it shall treat the existing device with a matching identifier as the same device.

The RAS may also provide more BSLD registration interfaces in addition to the HTTP-based BSLD registration interface.

7.5 Bluetooth smart lock device (BSLD) removal management

The BSLD removal request message format sent from the RAC to the RAS is shown in Figure 12.

http(s)://*RAS domain name/*device/check?token=*User login permission identifier*&identify=*device unique identifier*

Figure 12 – BSLD removal request message

The "token" is the user login permission identifier returned by the user authentication management interface.

In addition to the mandatory message field requirement in Figure 12, more field contents may be included in the message as extensions.

After receiving a BSLD removal request message, the RAS shall return the removal response message; see 7.6 for the HTTP response status code and message contents.

The RAS may also provide more BSLD removal interfaces in addition to the HTTP-based BSLD removal interface.

7.6 Response status code

The response status codes and their message contents returned by the RAS are shown in Table 1.

Table 1 – Response status codes and their message contents

Status code	Result	Message content

0	Success	{
		    code: 0,
		    data: {
		        …
		    }
		}

Any non-zero value	Failure	{
		    code: 1,
		    message: {
		        …
		    }
		}

Only "status code" and "message content" in Table 1 are sent in the response message.

When "status code" is 0, the "message" field shall be empty; when "status code" is a non-zero value, the "data" field shall be empty.

The data format of the message content used in Table 1 is JSON (see IETF RFC 4627).

7.7 Generic message format used between remote access client (RAC) and remote access server (RAS)

Message push data format between the RAS and the RAC is shown in Table 2.

Table 2 – Message push data format between RAS and RAC

Data format

{
        type: 0,
        id: 0,
    content: {
        …
    }
}

In Table 2, "type" is the push message type; "id" is the device unique identifier; and "content" is the specific message content to be pushed.

8 Standard data format used among remote access client (RAC), Bluetooth gateway (BGW) and Bluetooth smart lock device (BSLD)

The mandatory communication protocol data format among an RAC, BGW and BSLD is shown as follows.

Command ID	Command type	Command value	Check byte	Timestamp
1 byte	1 byte	9 bytes	1 byte	4 bytes

The basic protocol contains 1-byte command ID, 1-byte command type, 9-bytes command value, 1-byte check byte, and 4-bytes timestamp, for a total of 16 bytes.

1) command ID: the value range is from 0 to 255; each command adds 1; and the count wraps around to 0 again after reaching 255; the command ID goes up each time a request command is sent.
2) command type: the type of command to be executed.
3) command value: the data contained in each command.
4) check byte: the value result of a bitwise exclusive OR operation of command ID, command type and command value.
5) timestamp: the number of seconds between the current system time and 00:00:00 on 1 January 2000.