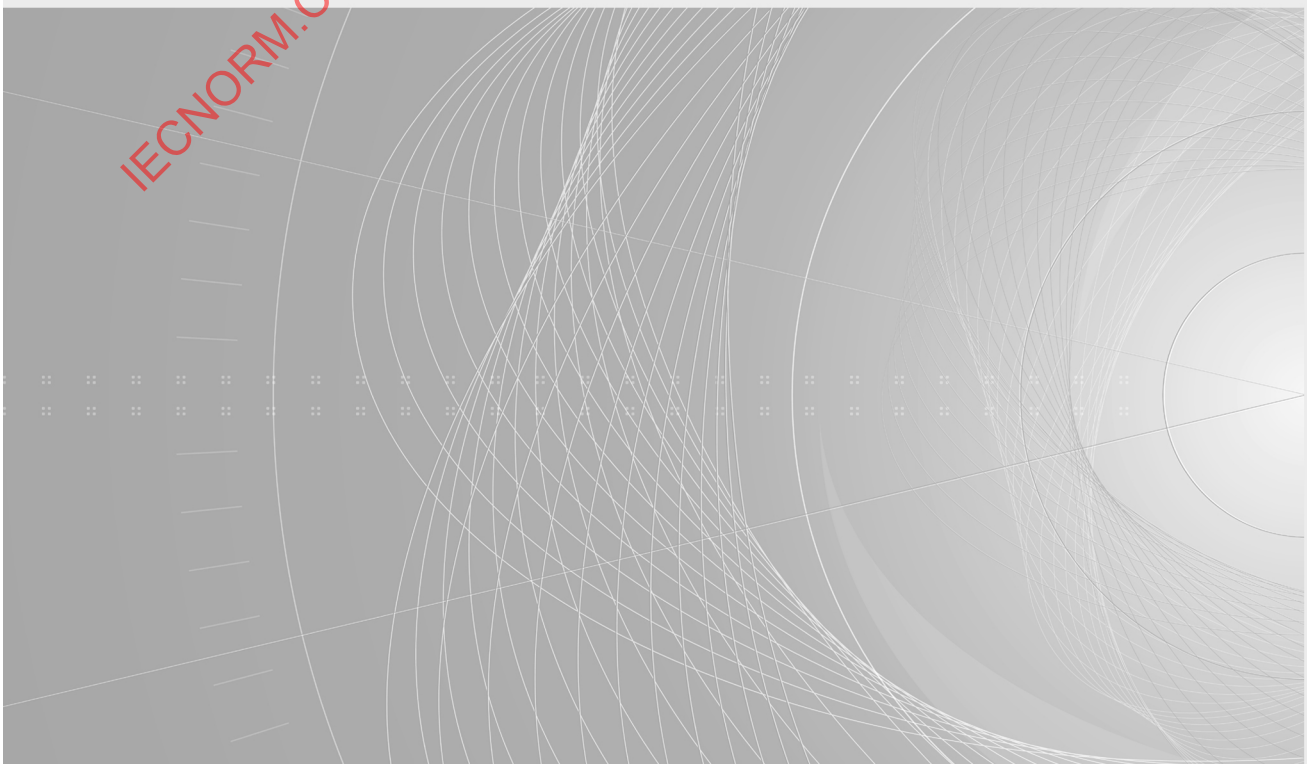
ISO/IEC 14543-5-9

Edition 1.0 2017-08

INTERNATIONAL STANDARD

colour inside

Information technology – Home electronic system (HES) architecture – Part 5-9: Intelligent grouping and resource sharing for HES Class 2 and Class 3 – Remote access service platform



ISO/IEC 14543-5-9:2017-08(en)

IEC Central Office
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 It also gives information on projects, replaced and withdrawn publications.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.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
67 000 electrotechnical terminology entries in English and French extracted from the Terms and definitions clause of IEC publications issued between 2002 and 2015. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

ISO/IEC 14543-5-9

Edition 1.0 2017-08

INTERNATIONAL STANDARD

colour inside

Information technology – Home electronic system (HES) architecture – Part 5-9: Intelligent grouping and resource sharing for HES Class 2 and Class 3 – Remote access service platform

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ICS 35.240.67

ISBN 978-2-8322-4681-8

CONTENTS

INFORMATION TECHNOLOGY – HOME ELECTRONIC SYSTEM (HES) ARCHITECTURE –

Part 5-9: Intelligent grouping and resource sharing for HES Class 2 and Class 3 – Remote access service platform

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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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 National Committees and ISO member bodies.

3) IEC, ISO and ISO/IEC publications have the form of recommendations for international use and are accepted by IEC National Committees and ISO member bodies in that sense. While all reasonable efforts are made to ensure that the technical content of IEC, ISO and ISO/IEC publications is accurate, IEC or 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 National Committees and ISO member bodies undertake to apply IEC, ISO and ISO/IEC publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any ISO, IEC or ISO/IEC publication and the corresponding national or regional publication should be clearly indicated in the latter.

5) ISO and IEC do not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. ISO or IEC 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 publication.

7) No liability shall attach to IEC or ISO or its directors, employees, servants or agents including individual experts and members of their technical committees and IEC National Committees or ISO member 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 of, use of, or reliance upon, this ISO/IEC publication or any other IEC, ISO or ISO/IEC publications.

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

9) Attention is drawn to the possibility that some of the elements of this ISO/IEC publication may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

International Standard ISO/IEC 14543-5-9 was prepared by subcommittee 25: Interconnection of information technology equipment, of ISO/IEC joint technical committee 1: Information technology.

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 and ISO websites.

This International Standard has been approved by vote of the member bodies, and the voting results may be obtained from the address given on the second title page.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

A bilingual version of this publication may be issued at a later date.

IMPORTANT – The 'colour inside' logo on the cover page of this publication 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

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

The ISO/IEC 14543-5 series includes the following parts.

– Part 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, including device and service discovery protocol, device and service description, service invocation, security mechanisms, etc.
  - Specifies core protocols for a type of home network that supports streaming media and other high-speed data transports within a home.
– Parts 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:
    – Part 5-21: AV profile
    – Part 5-22: File profile
– Part 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.
– Part 5-4: Device validation
  - Defines a standard method to validate an IGRS-compliant device.
– Part 5-5: Device type
  - Specifies IGRS device types used in IGRS applications.
– Part 5-6: Service type
  - Specifies basic service types used in IGRS applications.
– Part 5-7: Remote access system architecture
  - Specifies the architecture and framework for the remote access of IGRS devices and services in the Home Electronic System. The remote access 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 AV access profile
    – ISO/IEC 14543-5-102: Remote universal management profile
    – ISO/IEC 14543-5-11: Remote user interface
    – ISO/IEC 14543-5-12: Remote access test and verification
  - The relationships among these parts are specified in part 5-7.
– Part 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.

– Part 5-9: Remote access service platform
  - Specifies the IGRS RA service platform (IRSP) architectures and interfaces among servers in the service platforms.
  - Based on Part 5-8: Remote access core protocol

– Parts 5-10#: Remote access application profiles
  - Defines a device and service interaction mechanism for various applications.
  - Based on Part 5-8: Remote access core protocol
  - Two profiles are under development:
    – Part 5-101: Remote AV access profile.[1] This part defines the common requirements for IGRS RA AV users or devices in IGRS networks.
    – Part 5-102: Remote universal management profile.[2] 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.
  - Additional application profiles will be specified in the future.

– Part 5-11: Remote user interface[3]
  - Specifies adaptive user interface generation and remote device control mechanisms suitable for different remote access applications and devices.

– Part 5-12: Remote access test and verification[4]
  - Defines a standard method to test and verify IGRS-RA compliant devices and service interfaces.

---

1 Under preparation. Stage at the time of publication: ISO/IEC DIS 14543-5-101:2017.

2 Under preparation. Stage at the time of publication: ISO/IEC CD 14543-5-102:2016.

3 Under preparation. Stage at the time of publication: ISO/IEC DIS 14543-5-11:2017.

4 Under preparation. Stage at the time of publication: ISO/IEC DIS 14543-5-12:2017.

INFORMATION TECHNOLOGY – HOME ELECTRONIC SYSTEM (HES) ARCHITECTURE –

Part 5-9: Intelligent grouping and resource sharing for HES Class 2 and Class 3 – Remote access service platform

1 Scope

This part of ISO/IEC 14543-5 specifies the basic functionalities, module structures and interfaces in an IGRS RA service platform (IRSP). The service interaction flow and the request/response message formats are also specified.

This document is applicable to remote access of an IGRS sub-network (called an IGRS subnet) for resource sharing and service collaboration among home and/or remote computers, consumer electronics and communication devices.

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 HES Class 2 and Class 3 – Remote access core protocol*

IETF RFC 2818, *HTTP over TLS*

IETF RFC 4422, *Simple Authentication and Security Layer (SASL)*

IETF RFC 5246, *The Transport Layer Security (TLS) Protocol – Version 1.2*

IETF RFC 6121, *Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence*

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1.1
account server
IGRS RA server that processes services related to user and device account information

3.1.2
application server
IGRS RA server or third party server located outside of an IGRS RA system that processes application service-related logical functions

Note 1 to entry: The application server provides the approach to access application service logical functions (also called logics). By using the application server, IGRS RA user or device or other server can access the application service logics.

3.1.3
device ID
unique identification of an IGRS RA device

EXAMPLE If the local part of a device ID is “#igrsdevice” and the domain name part of the user ID is “igrs.com”, the device ID is “#igrsdevice@igrs.com”.

Note 1 to entry: A device ID consists of a local part and a domain name part; a “@” is used to separate the two parts. Each device ID starts with a “#”.

3.1.4
device verification code
string used to examine if the user has the authority to bind a device

Note 1 to entry: For the device without user interface, this device verification code is used to bind a device to a user. The device owner guarantees the safety of the device verification code.

3.1.5
IGRS AS
basic service unit composed of one or multiple IGRS servers

Note 1 to entry: Each IGRS AS provides services for a dedicated user and/or device group and constructs an IGRS RA domain. This document defines all of the necessary requirements that allow different IGRS ASs to exchange messages with each other.

3.1.6
IGRS RA device
physical device that is accessible to the IGRS RA user in the IGRS RA system

Note 1 to entry: A binding relationship can be established between an IGRS RA device and an IGRS RA user. A sibling relationship can be established between two IGRS RA devices.

3.1.7
IGRS RA server
instantiation of a service provider that may be included in an IRSP

Note 1 to entry: An IGRS RA server is deployed on the Internet. It maintains relationships among the IGRS RA user and IGRS devices. It also provides re-transmission of collaborative messages. The IGRS RA user and device can start a data connection to the IRSP and supports interconnections using the data connection and re-transmission functions of the IRSP.

3.1.8
IGRS RA service platform
IRSP
collection of multiple IGRS RA servers that are deployed on the Internet to maintain the relationships among IGRS RA user and IGRS RA device and to exchange collaborative messages

Note 1 to entry: IGRS RA user and device can establish connections to the IRSP, can send collaborative messages over these connections and can exchange messages in the servers of the IRSP.

3.1.9
IGRS RA user
entity that uses the IGRS RA devices and application services

Note 1 to entry: Generally, an IGRS RA user is a human being. Each IGRS RA user should have a unique user ID (identification). A bundle relationship can be established between one IGRS RA user and another. A binding relationship can be established between one IGRS RA user and one IGRS device.

3.1.10
message server
IGRS RA server that processes message exchanging logics (transmitting, receiving, forwarding and blocking, etc.)

3.1.11
server address
ID to identify the network location of a server in IGRS RA system

EXAMPLE One IGRS RA server address could be: “www.igrslab.com:8080”.

Note 1 to entry: Server address format in IGRS RA system is “domain name of server:port”.

3.1.12
user ID
unique identification of an IGRS RA user

EXAMPLE If the local part of a user ID is “igrsuser” and the domain name part of the user ID is “igrs.com”, the user ID is igrsuser@igrs.com.

Note 1 to entry: A user ID consists of a local part and a domain name part. A “@” is used to separate the two parts.

3.2 Abbreviated terms

AS	autonomous system
HTTP	hypertext transfer protocol
ID	identification
IGRS	intelligent grouping and resource sharing
IRSP	IGRS remote access service platform
RA	remote access
SHA	secure hash algorithm
SASL	simple authentication and security layer
TLS	transport layer security
XMPP	extensible messaging and presence protocol

4 Conformance

A service platform conforming to this document shall be implemented as specified in Clauses 5 and 6. The message exchange mechanism in an IRSP conforming to this document shall be implemented as specified in Clause 8, and the security mechanism in an IRSP conforming to this document shall be implemented as specified in Clause 9.

5 IRSP overview

The IGRS remote access core protocol is specified in ISO/IEC 14543-5-8, which includes the relationship management between a user or device and a user or device, device discovery and online status management mechanism, message format, message exchange flow and remote access data/service distribution and sharing mechanism.

This document is based on the core protocol of ISO/IEC 14543-5-8 and specifies the service platform side of IGRS RA system structure, message formats and collaborative exchange flows between different servers in the IRSP.

The working scope of the IRSP protocol, the IGRS core protocol and interfaces between them are defined and shown in Figure 1.

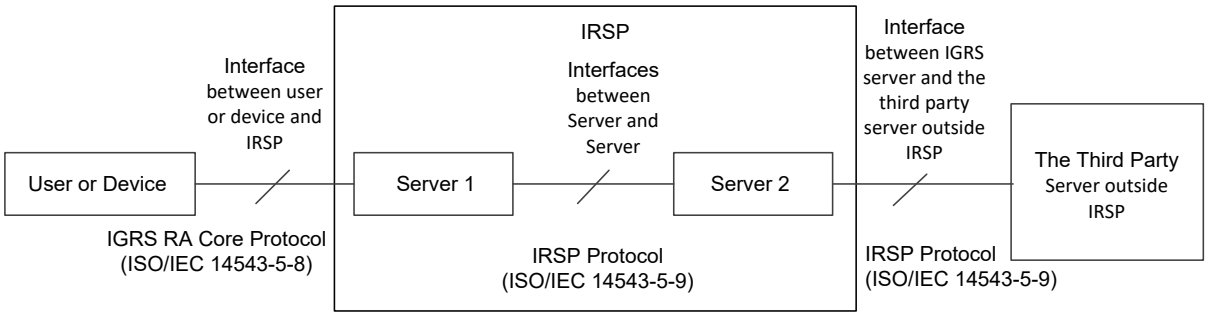


Figure 1 – Interfaces and working scope of IGRS RA core protocol and IRSP protocol

In the IGRS RA system, the interface between a user or device and an IRSP is specified in ISO/IEC 14543-5-8. The interface between different servers and the interface between an IGRS server and a third party server outside of the IRSP are specified in this document.

When the server 2 in Figure 1 exchanges messages with the third party server, it shall function as a gateway and firewall between the IRSP and the other systems. The message exchange between IGRS server and the third party server is specified in 8.8.

6 IRSP architecture

An IRSP is composed of multiple servers. Some servers with different functions can form an autonomous system (AS). Generally, user and device shall submit registration request to the IRSP after the service initialization. When users and devices in one AS establish relationships with each other, the message server in this AS shall process. When a user or device in one AS wants to establish relationship with another user or device in another AS, they shall communicate through the message servers in both ASs.

The IRSP architecture is shown in Figure 2.

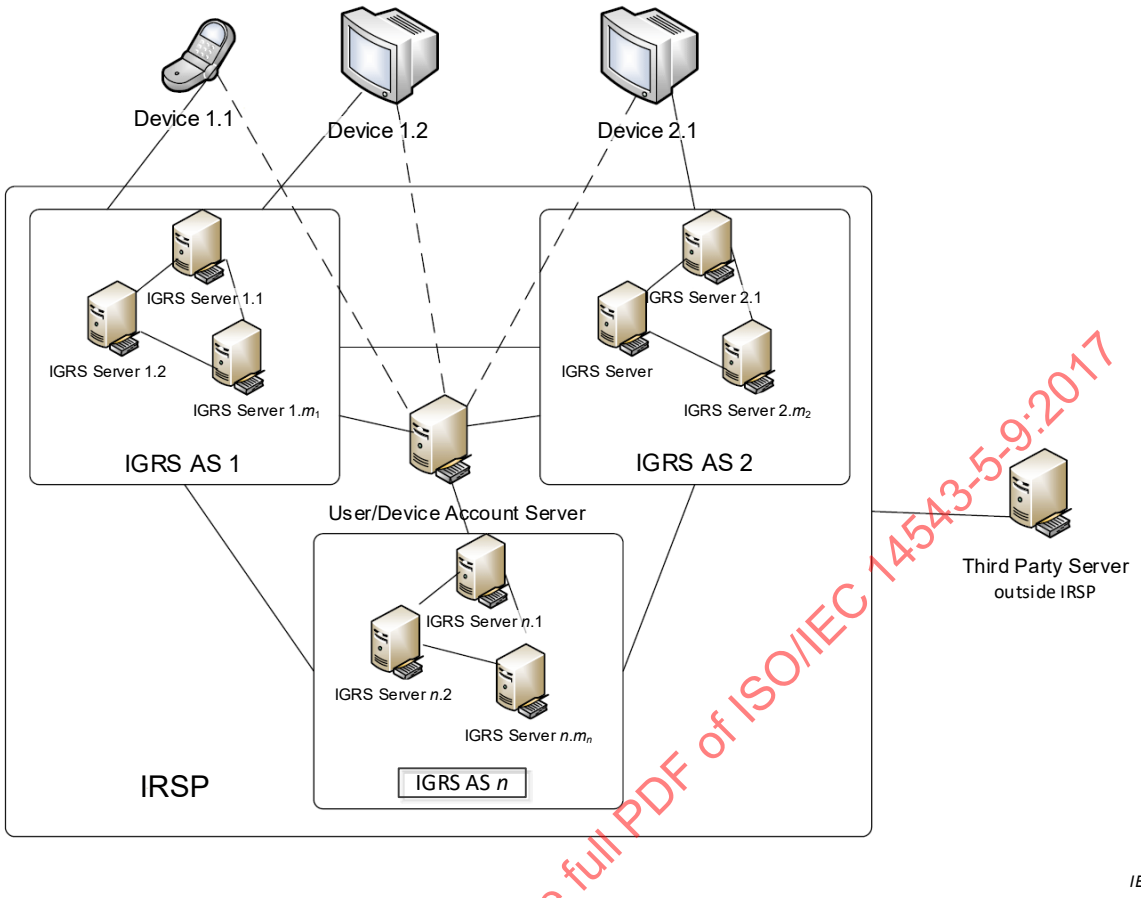


Figure 2 – IRSP architecture

m_k is the server number of the kth IGRS AS (IGRS AS k), and n is the number of the IGRS ASs in the IRSP. The dashed lines in Figure 2 are connections between a user or device and an IGRS account server when the user or device manages accounts (registration, password modification, account deletion, etc.).

Some IGRS IRSP internal servers can construct an IGRS AS by collaborative interconnections. Different IGRS ASs can exchange messages with each other. Generally, a user or device belongs to an IGRS AS domain. All users and devices in one IGRS AS have the same domain name in the user or device IDs. When two IGRS users or devices in one AS exchange messages with each other, they shall follow the message exchanging mechanism within one AS specified in 8.2, 8.3 and 8.4. When two IGRS users or devices belong to different IGRS ASs and want to exchange messages, they shall follow the message exchanging mechanism between different ASs specified in 8.5, 8.6, 8.7 and 8.8.

7 Server types

7.1 Account server

The account server processes user and device account related contents on the IRSP. Generally, one IRSP has only one logical account server.

The functionalities of account server are:

a) managing all user and device accounts in all ASs;

b) verifying the global uniqueness of the local part of user or device ID when the user or device registers and when the user or device information is modified. This ensures that the IGRS RA user or device ID is unique in IGRS system;

c) processing the deletion of user or device account.

The message exchange between the account server and message server is specified in 8.2.

7.2 Message server

The message server processes message exchange logics (transmission, receiving, forwarding and blocking, etc.). Different from an account server, one IRSP may have multiple message servers. One AS may also have multiple message servers.

The functionalities of message server are:

a) verifying user and device login identification;

b) verifying the message exchange security between the user or device and user or device, and between the user or device and the IRSP;

c) managing relationships between the user or device and user or device;

d) handling message operations (transmission, receiving, storing, distribution, discarding, etc.).

In an IGRS RA system, there are several different types of message exchanges between the message server and account server, as well as between the message server and application server:

1) message exchange between the message server and account server is specified in 8.2;

2) message exchange between the message server and application server in the same AS is specified in 8.3;

3) message exchange between the message server and message server in different ASs is specified in 8.5;

4) message exchange between the message server and application server in different ASs is specified in 8.6.

7.3 Application server

The application server processes application services logics (content service, storage service, data analysis, etc.). Two types of application servers are considered in the IGRS RA system:

1) IRSP internal application servers shall follow application logics specified in the IGRS RA application profiles;

2) IRSP external application servers are owned and managed by third party service providers.

These two types of application servers can exchange messages with each other and provide collaborative services to the user/device/AS.

In an IGRS RA system, there are several different types of message exchanges between the application server and message server, and as well as between the application server and application server:

a) message exchange between the application server and message server in the same AS is specified in 8.3;

b) message exchange between the application server and application server in the same AS is specified in 8.4;

c) message exchange between the application server and application server in different ASs is specified in 8.6;

d) message exchange between the message server and application server in different ASs is specified in 8.7;

e) message exchange between an IRSP internal application server and an IRSP external application server is specified in 8.8.

7.4 IRSP external application server

This is a third-party owned and managed application server that exchanges messages with the IRSP and jointly provides collaborative services with IGRS servers.

The communication protocol between IRSP external application servers does not follow the message exchange modes specified in this document. This document only specifies the basic principle of message exchange between the IRSP internal application server and application server outside of the IGRS RA system in 8.8.

8 Messages exchanged between servers

8.1 Overview

Different message exchange models in the IRSP are shown in Figure 3.

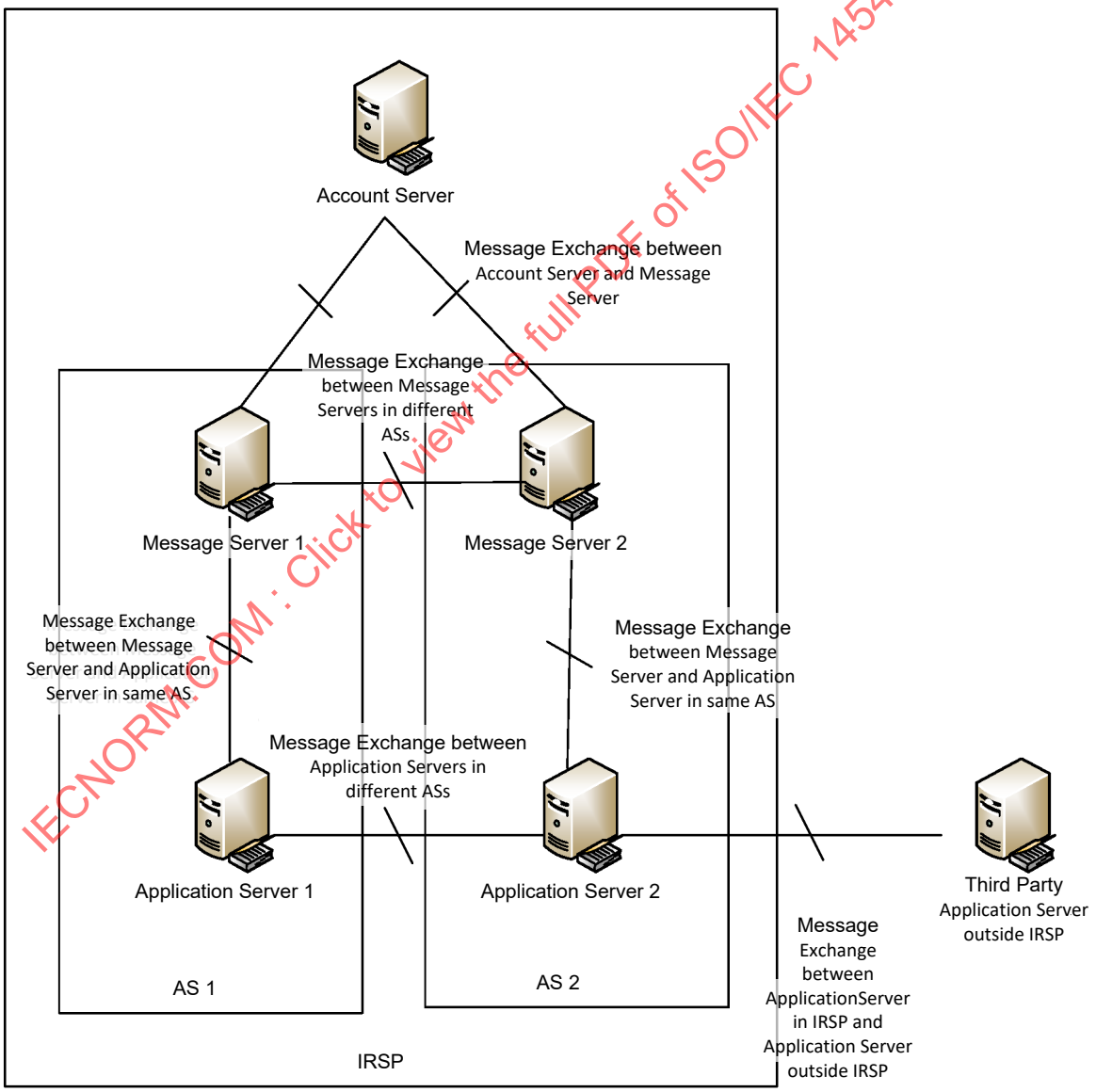


Figure 3 – Message exchange models in IGRS RA system

In IGRS RA system, different servers can exchange messages with each other directly. There are several different message exchange interfaces:

a) between the account server and message server;
b) between the message server and message server in the same AS;
c) between the message server and application server in the same AS;
d) between the message server and message server in different ASs;
e) between the application server and application server in different ASs; and
f) between an IRSP internal application server and an IRSP external application server.

However, the following exchanges have no direct message exchange interface:

1) between the account server and any application server; and
2) between the message server and application server in different ASs.

If a message server wants to exchange any messages with an application server in another AS, it needs to first send the request to an application server in the same AS and then to forward the messages to the target application server.

8.2 Messages exchanged between account server and message server

8.2.1 Register on account server

When a user or device wants to register on account server, the account server shall register a same account on the message server in the same AS that contains the user or device. When a user registers in IGRS RA system, the account server shall send Message 1 to the message server, where the “account server application ID” and “account server token” are pre-assigned by the message server to the account server to authenticate the account server.

Message 1 – User registration message sent from account server to message server

https://*message server address*/user/register.xml?version=1&appid=*account server application ID* &token=*account server token*&name=*local part of user ID*&password=*user password*

NOTE 1 Italics indicate where content is to be inserted; all other text in message definitions is fixed in this document.

NOTE 2 All contents in the message definition are mandatory in this document.

When a device registers, the account server shall send Message 2 to the message server.

Message 2 – Device registration message sent from account server to message server

https://*message server address*/device/register?version=1&appid= *account server application ID*&token= *account server token*&name= *local part of device ID*&password=*device password* &verifycode=*device verification code*&type=*device type*&vendor=*device vendor*&model=*device model*

The “account server application ID” and “account server token” are pre-assigned by message server to the account server to authenticate the account server. The “verifycode”, “type”, “vendor” and “model” are optional. If the user or device has provided additional parameters to the IRSP when it was registered, the additional parameters shall also be included in Message 2.

The returned registration response status code and contents in the registration response message sent from the message server to the account server are shown in Table 1.

Table 1 – Registration response status code and contents in registration response message

Status code	Result	Message content
200	Successful	
400	Wrong parameter	<error> <code>400</code> <detail>bad request</detail> </error>
421	ID existed	<error> <code>421</code> <detail>id existed</detail> </error>
500	Server internal error	<error> <code>500</code> <detail>server internal error</detail> </error>

In Table 1, “Result” is not sent and “Status code” and “Message content” shall be sent. When the “Status code” is 200, the “Message content” is empty.

8.2.2 Modify the user or device information

When a user or device wants to modify the user or device information, e.g. password, the account server shall make corresponding modifications. When a user’s information is modified, the account server shall send Message 3 to the message server.

Message 3 – User information modification message sent from account server to message server

https://*message server address*/user/modify?version=1&appid=*account server application ID* &token=*account server token*&name=*local part of user ID*&password=*user password*

The “account server application ID” and “account server token” are pre-assigned by message server to the account server to authenticate the account server.

When the information of a device is modified, the account server shall send Message 4 to the message server.

Message 4 – Device information modification message sent from account server to message server

https://*message server address*/device/modify?version=1&appid= *account server application ID*&token= *account server token*&name= *local part of device ID*&password=*device password* &verifycode=*device verification code*&type=*device type*&vendor=*device vendor*&model=*device model*

The “account server application ID” and “account server token” are pre-assigned by message server to the account server to authenticate the account server. The “verifycode”, “type”, “vendor” and “model” are optional. If the user or device provided additional parameters to the IRSP when it was registered, the additional parameters shall also be included in Message 4.

The returned information modification response status code and contents in the information modification response message sent from the message server to the account server are shown in Table 2.

Table 2 – Information modification response status code and contents in information modification response message

Status code	Result	Message content
200	Successful	Empty
400	Wrong parameter	<error> <code>400</code> <detail>bad request</detail> </error>
422	ID does not exist	<error> <code>422</code> <detail>id not existed</detail> </error>
500	Server internal error	<error> <code>500</code> <detail>server internal error</detail> </error>

8.2.3 Delete account on the IRSP

When a user or device wants to delete his/her/its account on the IRSP, the account server shall delete the account on corresponding message server. When a user deletes himself/herself on the IRSP, the account server shall send Message 5 to the message server.

Message 5 – User deletion message sent from account server to message server

https://*message server address*/user/remove?version=1&appid=*account server application ID* &token=*account server token*&name=*local part of user ID*

The "account server application ID" and "account server token" are pre-assigned by message server to the account server to authenticate the account server.

When a device deletes itself on the IRSP, the account server shall send Message 6 to the message server.

Message 6 – Device deletion message sent from account server to message server

https://*message server address*/device/remove?version=1&appid= *account server application ID*&token= *account server token*&name=*local part of device ID*

The "account server application ID" and "account server token" are pre-assigned by message server to the account server to authenticate the account server.

The returned user or device deletion response status code and contents in the deletion response message sent from the message server to the account server are shown in Table 3.

Table 3 – Deletion response status code and contents in deletion response message

Status code	Result	Message content
200	Successful	Empty
400	Wrong parameter	<error> <code>400</code> <detail>bad request</detail> </error>
422	ID does not exist	<error> <code>422</code> <detail>id not existed</detail> </error>
500	Server internal error	<error> <code>500</code> <detail>server internal error</detail> </error>

8.2.4 Reset device verification code on IRSP

When a user or device wants to reset device verification code on IRSP, the account server shall synchronize the new device verification code to the account. The message server shall send Message 7 to the account server to synchronize the device verification code.

Message 7 – Device verification code reset message sent from message server to account server

https://*account server address*/modifyVerifyCode.xml?deviceid= *local part of device ID*&verifycode=*new device verification code or empty*

The returned device verification code reset response status code and the content of the device verification code response message sent from the account server to the message server are shown in Table 4.

Table 4 – Device verification code reset response status code and contents in the device verification code reset response message

Status code	Result	Message content
200	Successful	Empty
400	Wrong parameter	<error> <code>400</code> <detail>bad request</detail> </error>
422	ID does not exist	<error> <code>422</code> <detail>id not existed</detail> </error>
500	Server internal error	<error> <code>500</code> <detail>server internal error</detail> </error>

8.3 Messages exchanged between message server and application server in same AS

8.3.1 User or device uploads message to application server through message server

When a user wants to upload messages (e.g. user subscription information) to the application server through the message server, the message server shall send Message 8 to the application server.

Message 8 – Message sent from message server to application server when user uploads message

https://*application server address*/*user uploading message service URI*?userid=*local part of user ID* &data=*data to be uploaded*

When a device wants to upload messages (device status information, device alarm information, etc.) to the application server through the message server, the message server shall send Message 9 to the application server.

Message 9 – Message sent from message server to application server when device uploads message

https://*application server address*/*device uploading message service URI*?deviceid=*local part of device ID* &data=*data to be uploaded*

8.3.2 Device uploads online/offline notification to application server through message server

When the device comes online, the message server shall send a device online notification message as in Message 10 to the application server.

Message 10 – Message sent from message server to application server when device comes online

https://*application server address*/*device online-offline notification service URI*?deviceid=*local part of device ID*&type=online

When the device goes offline, the message server shall send a device offline notification message as in Message 11 to the application server.

Message 11 – Message sent from message server to application server when device goes offline

https://*application server address*/*device online-offline notification service URI*?deviceid=*local part of device ID*&type=offline

8.3.3 Application server pushes message to user or device through message server

The application server shall push messages, e.g. text message or subscription message, to the user or device through the message server. When the application server pushes message to a user, the application server shall send Message 12 to the message server.

Message 12 – Message sent from application server to message server when application server pushes message to a user

https://*message server address*/*push service URI*?userid=*local part of user ID*&data=*pushed message contents*

When the application server pushes message to a device, the application server shall send Message 13 to the message server.

Message 13 – Message sent from application server to message server when application server pushes message to a user

https://*message server address*/*push service URI*?deviceid=*local part of device ID*&data=*pushed message contents*

8.3.4 Response status code for message exchange between message server and application server in same AS

After receiving the message exchange request from the message server, the application server shall return response status codes as in Table 5.

Table 5 – Response status code for message request from message server to application server

Status code	Result	Message content
200	Successful	Empty
400	Wrong parameter	<error> <code>400</code> <detail>bad request</detail> </error>
500	Server internal error	<error> <code>500</code> <detail>server internal error</detail> </error>

After receiving the message exchange request from application server, the message server shall return response status codes as in Table 6.

Table 6 – Response status code for message request from application server to message server

Status code	Result	Message content
200	Successful	Empty
400	Wrong parameter	<error> <code>400</code> <detail>bad request</detail> </error>
422	ID does not exist	<error> <code>422</code> <detail>id not existed</detail> </error>
500	Server internal error	<error> <code>500</code> <detail>server internal error</detail> </error>

8.4 Messages exchanged between application servers in same AS

8.4.1 Overview

Two application servers in the same AS can exchange messages. When two application servers exchange user-related messages, the source application server shall send Message 14 to the target application server.

Message 14 – Message sent from source application server to target application server when they exchange user related message

https://*target application server address*/*message exchange service URI*?userid=*local part of user ID*&data=*pushed message contents*

When two application servers exchange device-related messages, the source application server shall send Message 15 to the target application server.

Message 15 – Message sent from source application server to target application server when they exchange device related message

https://*target application server address*/*message exchange service URI*?deviceid=*local part of device ID*&data=*pushed message contents*

8.4.2 Response status code for message exchange between application servers in same AS

When two application servers exchange messages in the same AS, the returned message exchange response status code is shown in Table 7.

Table 7 – Response status code for message request from one application server to another application server in same AS

Status code	Result	Message content
200	Successful	Empty
400	Wrong parameter	<error> <code>400</code> <detail>bad request</detail> </error>
500	Server internal error	<error> <code>500</code> <detail>server internal error</detail> </error>

8.5 Messages exchanged between message servers in different ASs

The message exchange between message servers in different ASs shall follow the message routing protocol between the servers specified in IETF RFC 6121.

8.6 Messages exchanged between application servers in different ASs

The message exchange between application servers in different ASs shall be negotiated and determined by the individual application servers' providers.

8.7 Messages exchanged between message server and application server in different ASs

A message server and application server in different ASs shall not be allowed to exchange messages directly. This is to avoid potential security issues in the direct message exchange between the message server in one AS and an unsecure application server in another AS.

The message exchange between message server and application server in different ASs shall be achieved through first exchanging the message between the message server and application server in the same AS (see 8.3), and then exchanging the message between application servers in different ASs (see 8.6).

8.8 Messages exchanged between IRSP internal application server and IRSP external application server

8.8.1 Overview

When an IRSP internal application server exchanges messages with an IRSP external application server, a high-level security mechanism shall be used to guarantee the overall security of the IRSP.

8.8.2 IRSP internal application server sends message to third party IRSP external application server

When an IRSP internal application server sends messages to a third party IRSP external application server, it shall follow the message format and security requirement of the third party application server. The IRSP internal application server shall first convert the message format according to the requirement of the third party application server before sending out the message. When it receives the message from the third party application server, it shall perform a reverse message format conversion and then process the message accordingly.