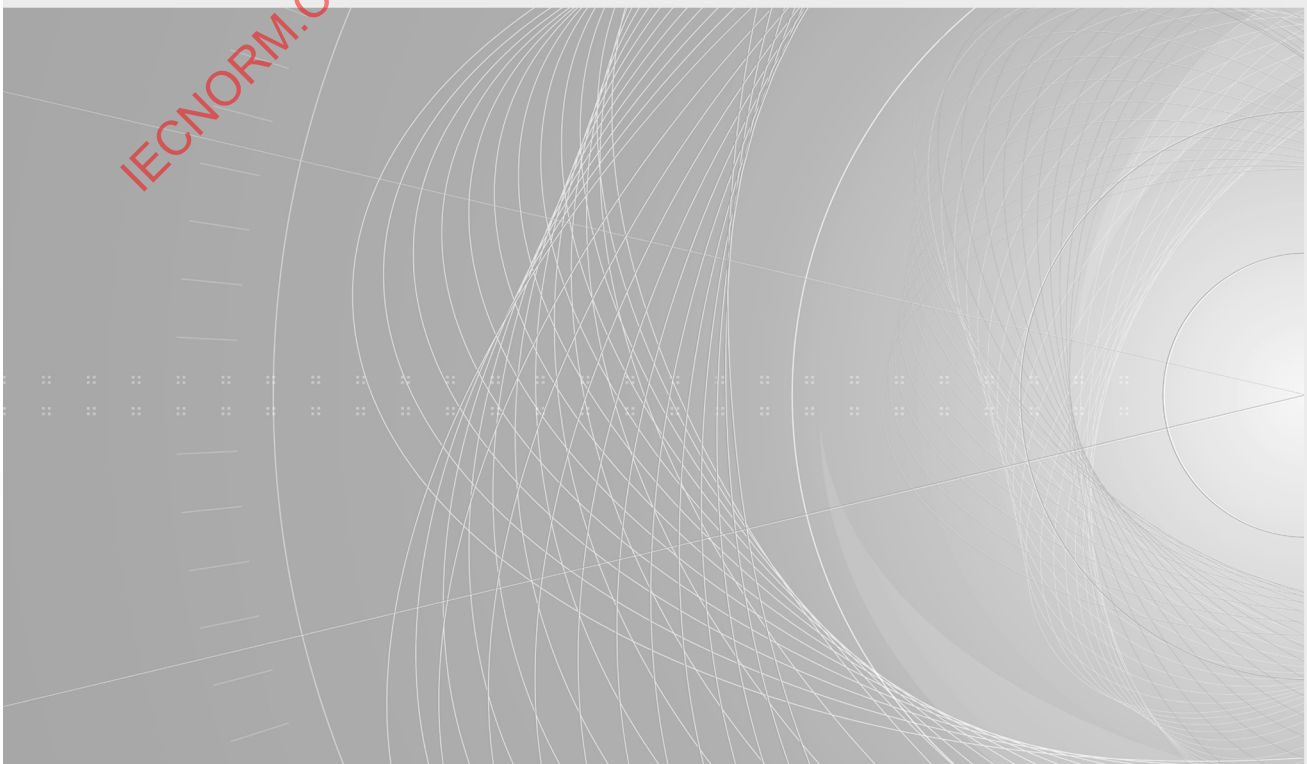
ISO/IEC 14543-5-8

Edition 1.0 2017-08

INTERNATIONAL STANDARD

colour inside

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



ISO/IEC 14543-5-8:2017-08(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 It also gives information on projects, replaced and withdrawn publications.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 14543-5-8

Edition 1.0 2017-08

INTERNATIONAL STANDARD

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ICS 35.240.67

ISBN 978-2-8322-4693-1

CONTENTS

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

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 14543-5-8 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 and 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 device 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 5-8: Intelligent grouping and resource sharing for HES Class 2 and Class 3 – Remote access core protocol

1 Scope

This part of ISO/IEC 14543-5 specifies the core protocol of IGRS user and device remote access, including intelligent grouping and resource sharing. The protocol features are:

a) IGRS RA user and IGRS RA device concepts and relationship management mechanisms,

b) user and device remote discovery and online and offline status management mechanisms,

c) user and device remote access message formats and message exchanging flows, and

d) remote data and service distribution and sharing mechanisms.

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 14543-5-9, *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 9594-8|Recommendation ITU-T X.509, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*

IETF RFC 2616, *Hypertext Transfer Protocol – HTTP/1.1*

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 6120, *Extensible Messaging and Presence Protocol (XMPP): Core*

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

IETF RFC 7622, *Extensible Messaging and Presence Protocol (XMPP): Address Format*

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
binding
relationship established between a user and a device, which represents an own/owned relationship between the user and the device

Note 1 to entry: The user and device with binding relationship are shown in each other's roster. One user can bind multiple devices, and one device can be bound by multiple users.

3.1.2
buddy
relationship established between two users, which represents that the two users trust each other

Note 1 to entry: Two users with buddy relationship are shown in each other's roster.

3.1.3
connection ID
instance identification that identifies the connection between "user and IRSP" and "device and IRSP"

3.1.4
contact group
set of multiple contacts where each has the same attribute

3.1.5
device connection
network connection established between an IGRS RA device and the IRSP

Note 1 to entry: Only one device connection can be maintained at any time. Multiple devices of one user can connect to the IRSP simultaneously.

3.1.6
device connection ID
identification that represents an instance of a connection between an IGRS RA device and the IRSP

EXAMPLE If the device ID is"#igrsdevice@igrs.com" and the connection ID is "home", the device connection ID is "#igrsdevice@igrs.com/home".

Note 1 to entry: A device connection ID is unique. The IRSP tests and guarantees the uniqueness of the device connection ID.

Note 2 to entry: A device connection ID consists of a device ID and a connection ID. A "/" is used to separate these two IDs.

3.1.7
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 "#".

3.1.8
device verification code
string used to examine if the user has the authority to bind a device

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

3.1.9
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.

3.1.10
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 IGRS RA user and IGRS devices. It also provides re-transmission of collaborative messages. The IGRS RA user and IGRS device can start a data connection to the IRSP and supports interconnections using the data connection and re-transmission functions of the IRSP.

3.1.11
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.

3.1.12
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.

3.1.13
interested connection
connection that logged onto the IRSP using a user ID and requested the roster of that user

3.1.14
roster
list that stores all users and devices by which this specific user or device is permitted access

Note 1 to entry: A roster is managed by the IRSP. Each user or device has one and only one roster on the IRSP.

3.1.15
roster item
item in the roster

3.1.16
service ID
identification of a service

3.1.17
sibling
relationship established between two or more devices, which represents that these devices have a binding relationship with the same user, or these devices belong to the same user

Note 1 to entry: Devices with sibling relationship are shown in each other's roster.

3.1.18
user connection
network connection established between an IGRS RA user and the IRSP

Note 1 to entry: Multiple user connections can be maintained simultaneously for one user.

3.1.19
user connection ID
identification that represents an instance of a connection between an IGRS RA user and the IRSP

EXAMPLE If the user ID is "igrsuser@igrs.com" and the connection ID is "office", the user connection ID is "igrsuser@igrs.com/office".

Note 1 to entry: A user connection ID is unique. The IRSP tests and guarantees the uniqueness of a user connection ID.

Note 2 to entry: A user connection ID consists of a user ID and a connection ID. A "/" is used to separate the two IDs.

Note 3 to entry: The connection ID is set by the user when logging in.

3.1.20
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 RA service platform
NAT	network address translation
RA	remote access
SASL	simple authentication and security layer
TLS	transport layer security
TCP/IP	transmission control protocol/Internet protocol
UI	user interface
XMPP	extensible messaging and presence protocol

4 Conformance

A system that conforms to this document shall be implemented according to Clauses 5 through 14, where the service flow and message exchange mechanism in each functional block shall conform to Clauses 6 through 12. The user and device discovery and online status management shall conform to Clause 13 and the security mechanism in IGRS RA system shall conform to Clause 14.

5 IGRS RA overview

The IGRS RA core protocol extends the IGRS application scenarios from the home and office to the mobile and remote access situations. The applications scope is extended from the LAN area to the Internet for both fixed and mobile devices.

Each IGRS RA user or device shall have a unique user ID or device ID. One user or device can establish relationships with other users or devices. Based on these relationships, one user or device can obtain and exchange the online/offline status, changing messages, etc. from the other relevant users or devices.

This document is based on the concepts of IGRS RA user and IGRS RA device. The contents include:

a) IGRS RA user and IGRS RA device concepts and relationship management mechanisms;

b) user and device remote discovery and online and offline status management mechanisms;

c) user and device remote access message formats and message exchanging flows, and

d) remote data and service distribution and sharing mechanisms.

This document is the core protocol of IGRS RA based on IETF RFC 6120 and IETF RFC 6121.

Three types of interactive relationships can be established and maintained:

1) Binding: relationship between user and device. Binding shows the user ownership of the devices.

2) Sibling: relationship between device and device. When two devices are bound with the same user, these two devices are in a sibling relationship with each other.

3) Buddy: relationship between user and user. Buddy means a trusting relationship.

The detailed relationship definitions and management mechanisms are specified in Clause 10.

6 IGRS RA service functional flow

The IGRS RA request/response messages shall conform to the request/response model of HTTP/1.1 (see IETF RFC 2616). A typical service flow of IGRS RA service is shown in Figure 1.

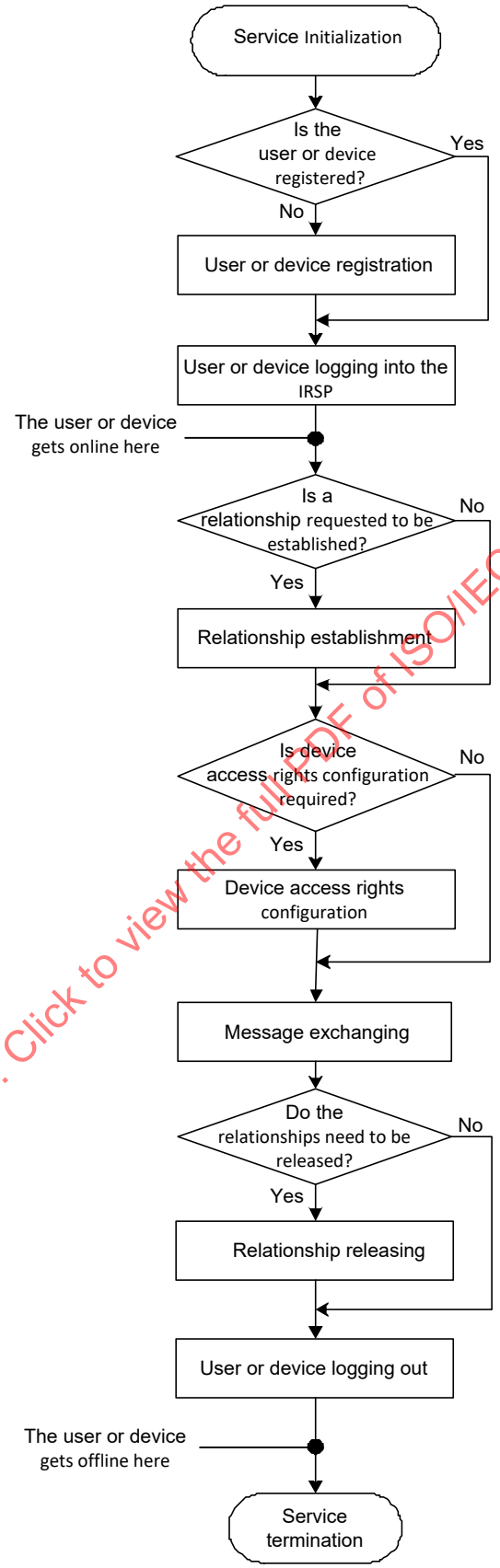


Figure 1 – Typical flow of IGRS RA service

a) Service initialization

User or device service protocol initializes.

b) User or device registration

If this is the first time the user or device is using IGRS service and the user or device has never registered onto the IRSP, he or it shall register onto the IRSP using his or its ID. The detailed registration specifications are shown in Clause 7.

c) User or device logins

The user or device shall use a registered user ID or device ID to log into the IRSP to utilize IGRS RA functions. After successfully logging into the IRSP, the user or device is online.

d) Establishing relationships

A relationship shall be established between user–device, user–user or device–device in order to exchange messages properly.

e) Device access rights configuration

Device owner may selectively grant different device access rights to other users by device access right configuration to reduce user authentication times required. By using this device access rights configuration, the other users can still access the devices even if the device owner is not online. The detailed specifications are shown in Clause 10.

f) Exchanging messages

Functions and services can exchange messages between user–device, user–user or device–device that have established relationships.

g) Releasing relationships

Relationships between user–device, user–user or device–device can be released.

h) User or device logouts

The user or device shall send logout messages to the IRSP prior to exiting the service. After successfully logging out from the IRSP, the user or device is offline. When the user or device loses Internet connection, it is considered as offline too.

i) Service termination

The user or device shall terminate service as the final step.

7 Registration management

7.1 User or device registration flow

After the service is initialized, the user or device shall register onto the IRSP. The user or device registration flow is shown in Figure 2.

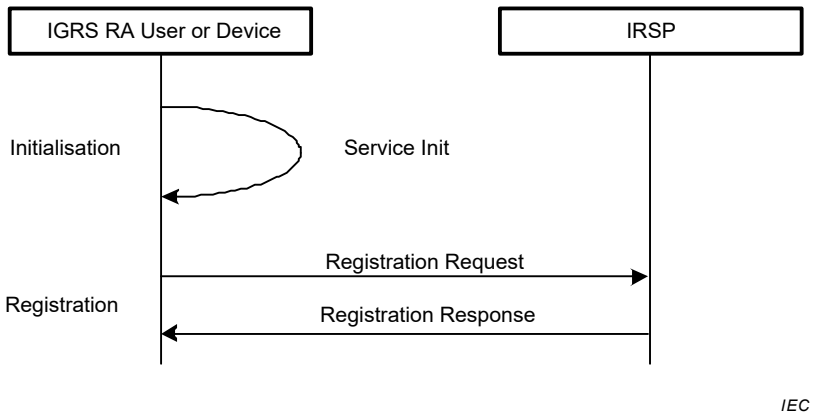


Figure 2 – IGRS RA user or device registration flow

The user or device shall send a registration request message to the IRSP. The IRSP shall send a registration response messages to the user or device according to the registration results.

User registration and device registration are two independent procedures.

7.2 User registration management

The IGRS RA user shall send a registration request message as in Message 1.

Message 1 – User registration request message

http(s)://*Domain Name of the Account Server*/register.xml?name=*local part of the User ID*&password=*Password*&domain=*Domain Name of the Message Server*

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.

The functionalities and the relative information of the Account Server and the Message Server are specified in Clause 7 of ISO/IEC 14543-5-9:2017.

Additional segments may be required in addition to the above message.

The IRSP shall send a registration response message to the IGRS user when it receives the registration request message from an IGRS user. The “http” response status code and the contents of the registration response messages are seen in 7.4.

The specification of user ID is specified in IETF RFC 7622. Additional specifications in IGRS RA system are given as the following.

a) Each IGRS user has one unique user ID, the first character of the user ID shall not be “#”.
b) When the user sets the local part of his/her user ID, the IRSP shall verify if this part is exclusive.
c) The IRSP may provide additional user registration interface in addition to the user registration interfaces based on HTTP.

7.3 Device registration management

The IGRS device shall send a registration request message as in Message 2.

Message 2 – Device registration request message

http(s)://*Domain Name of the Account Server*/register.xml?name=*device ID* & password=*Password*&domain=*Domain Name of the Message Service*&verifycode=*device verification code*&type=*device type*&vendor=*device vendor*&model=*device model*

where the “verifycode”, “type”, “vendor” and “model” are optional parameters. More information can be requested in addition to the above information.

The functions and the relative information of the Account Server and the Message Service are specified in ISO/IEC 14543-5-9.

The service platform shall return a registration response message when it receives a registration request message from the device. The http response status code and contents in the registration response messages are specified in Table 1.

The format of device ID is specified in IETF RFC 7622. Additional specifications in the IGRS RA system are as follows:

a) Each device ID starts with “#”.

b) Each IGRS RA device shall have a unique local part of the device ID. This local part of the device ID is set by the device manufacturers. The IRSP is responsible for checking the uniqueness of the local part of the device ID. When the service platform finds that the local part of the device ID of a new online device already exists, this device shall be treated as the exact same device as the old one (with the same local part in the device ID).

c) In addition to the HTTP based device registration interface, IRSP can provide additional device registration interfaces.

7.4 Registration response status code

The registration response status code sent by the service platform to the registration request user or device is shown in Table 1.

Table 1 – Registration response status code and the contents in the registration response messages

Status code	Result	Message content
200	Success	
400	Parameter error	<error> <code>400</code> <detail>bad request</detail> </error>
421	ID already exists	<error> <code>421</code> <detail>id existed</detail> </error>
500	Internal server error	<error> <code>500</code> <detail>server internal error</detail> </error>

In Table 1, “Result” is not sent, but “Status code” and “Message content” shall be sent.

When the “Status code” is 200, the “Message content” shall be empty.

8 Login

8.1 User or device login flow

After registering to the IRSP successfully, the user or device shall login to the IRSP each time it has Internet access. The flow of user or device logging into the IRSP is given as in Figure 3.

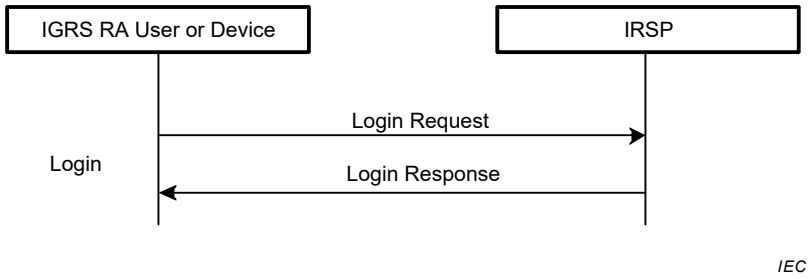


Figure 3 – IGRS RA User or Device Login Flow

The user or device sends a login request message to the IRSP and the IRSP returns a login result response message to the user or device.

8.2 User connection

The establishment, maintenance and termination of an IGRS RA user connection shall follow the Client-to-Server communication interactive flow specified in IETF RFC 6120. The user connection shall follow the TLS protocol specified in Clause 5 of IETF RFC 6120.

In addition, an IGRS RA user connection shall also follow the SASL protocol as specified in Clause 6 of IETF RFC 6120 to implement the authentication process.

8.3 Messages for user connection ID binding

After completing the SASL authentication negotiation, the user connection shall follow the flows specified in Clause 7 of IETF RFC 6120 to implement resource binding.

As one user may be logged in from multiple locations using the same user ID, during the user connection ID binding process, the client shall provide the corresponding connection IDs to represent the locations of the user connection. The connection IDs shall contain relevant user descriptions in order to distinguish the different login instances of this one user.

Whenever an IGRS RA device initiates a user connection, the IGRS RA user should use the model number or some characteristics of the device that this user is connected to as the connection ID of this user connection. That is, the user shall send a user connection ID binding request message shown in Message 3 to the IRSP during the user connection ID binding process as specified in Clause 7 of IETF RFC 6120.

Message 3 – User connection ID binding request message

```
<iq type='set' id='message SN'>
        <bind xmlns='urn:ietf:params:xml:ns:xmpp-bind'>
                <resource>Model number or some characteristics of the device which this
                user is connected to</resource>
        </bind>
</iq>
```

The IRSP shall return the user connection ID binding response message as in Message 4.

Message 4 – User connection ID binding response message

If successful:

```
<iq id='message SN' type='result'>
        <bind xmlns='urn:ietf:params:xml:ns:xmpp-bind'>
                <jid>User connection ID</jid>
        </bind>
</iq>
```

If failed:

```
<iq id=' message SN' type='error'>
        <error type='modify'>
                <bad-request xmlns='urn:ietf:params:xml:ns:xmpp-stanzas'/>
        </error>
 </iq>
```

8.4 Device connection

The establishment, maintenance and termination of IGRS RA device connection shall follow the Client-to-Server communication interactive flow specified in IETF RFC 6120. The device connection shall follow the TLS protocol specified in Clause 5 of IETF RFC 6120.

In addition, an IGRS RA device connection shall also follow the SASL protocol specified in Clause 6 of IETF RFC 6120 to implement the authentication process.

8.5 Messages for device connection ID binding

After the SASL authentication negotiation, the device connection shall follow the flows specified in Clause 7 of IETF RFC 6120 to implement ID binding. The device connection ID may be provided by the device or the IRSP.

The connection ID of a device connection ID binding is to the local part of the device ID. Only one device ID instance shall be found online at any given time. A new connection shall replace the old one if exactly the same device ID logs in again and creates an ID binding.

The device ID binding progress is described in Clause 7 of IETF RFC 6120. The device shall send Message 5 to the IRSP.

Message 5 – Device connection ID binding request message

```
<iq type='set' id='message SN'>
        <bind xmlns='urn:ietf:params:xml:ns:xmpp-bind'>
                <resource>Local part of the device ID</resource>
        </bind>
</iq>
```

The IRSP shall return device connection resource binding response messages as in Message 6.

Message 6 – Device connection ID binding response message

If successful:

```
<iq id='message SN' type='result'>
        <bind xmlns='urn:ietf:params:xml:ns:xmpp-bind'>
                <jid>Device connection ID</jid>
        </bind>
</iq>
```

If failed:

```
<iq id='message SN' type='error'>
        <error type='modify'>
                <bad-request xmlns='urn:ietf:params:xml:ns:xmpp-stanzas'/>
        </error>
</iq>
```

9 Device access rights configuration

9.1 Overview

The purpose of device access rights configuration is to allow the device owner to grant selected device access rights to other users and to reduce the user authentication times required. By acquiring certain device access rights, the permitted users can still use the device even when the device owner is offline.

The device access rights of a user shall be configured by including a device-accessible user list in the device access rights configuration request messages. The device owner can flexibly set the device access rights of all users, including buddies and non-buddies. Only users in the device-accessible user list may access the device.

One device may possess multiple services or functions. For the sake of security and safety, the device owner may not want to make available all the services and functions to the other users. A device-accessible scope shall be configured in the device access rights configuration request messages. This can limit the services and functions that the other users can access. An accessible service list is used to set the device accessible scope.

9.2 Messages for device access rights configuration request

The user sends a device access rights configuration request as in Message 7 by using the user connection to the IRSP to configure the device access rights.

Message 7 – Device access rights configuration request message

```
<iq type='set' id='message SN' to='Device ID of the configured device'>
        <setaccess xmlns=' http://www.igrs.org/spec2.0/basic#setaccess '>
                <accessuserlist>
                        <jid>User ID</jid>
                        <jid> User ID </jid>
                        ...
                </ accessuserlist >
                <accessservicelist>
                        <serviceid>Service ID</serviceid>
                        <serviceid>Service ID</serviceid>
                        ...
                </accessservicelist >
        </setaccess >
</iq>
```

In the above message, the “accessuserlist” field represents device accessible user list, and the “accessservicelist” field represents accessible service list.

9.3 Messages for device access rights configuration response

When the IRSP receives a device access rights configuration request message from a user, it shall verify the relationship between the user and the configured device. If the user and the configured device have an existing binding relationship, the IRSP regards the user as owner of the configured device, and it shall return a successful device access rights configuration response message to the user. Otherwise, it shall return a failed device access rights configuration response message.

The device access rights configuration response message is given as in Message 8.

Message 8 – Device access rights configuration response message

If successful:

```
<iq type='result' id='message SN' to='User ID'>
        <setaccess xmlns='http://www.igrs.org/spec2.0/basic#setaccess'>
                <deviceid>Device ID of the configured device</deviceid>
        </setaccess>
</iq>
```

If failed:

```
<iq type='error' id='message SN' to='User ID' >
        <setaccess xmlns=' http://www.igrs.org/spec2.0/basic#setaccess ' >
                <deviceid> Device ID of the configured device</deviceid>
                <error type=’cancel’>
                        < not-acceptable xmlns='urn:ietf:params:xml:ns:xmpp-stanzas'>
                        <text xmlns='urn:ietf:params:xml:ns:xmpp-stanzas'>
                                Reason for device access rights configuration failure
                        </text>
                </error>
        </setaccess >
</iq>
```

The reason for device access rights configuration failure can be included into the message optionally.

10 User and device relationship management

10.1 Overview

The concept of “user” is introduced into the IGRS RA system with three types of interactive relationships: “user–device”, “device–device” and “user–user”. These are defined and maintained as collaborative relationships in the IGRS RA system. Moreover, there are two ways to set up the relationships: 1) “Request which needs the approval from the target” and 2) “Request which does not need the approval from the target”. The corresponding message flows are shown in Figure 4 and Figure 5, respectively.

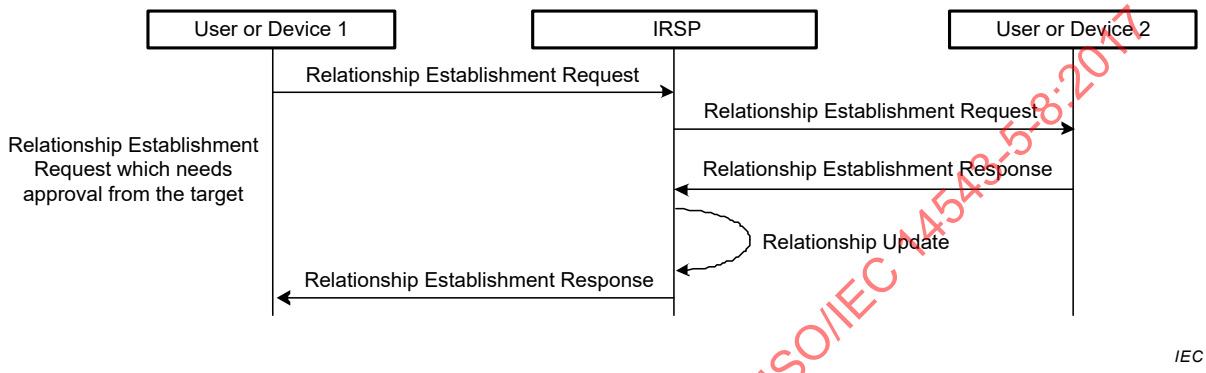


Figure 4 – Flow of relationship establishment request which needs approval from target

In the workflow of Figure 4, the user or device 1 sends a relationship establishment request message to the IRSP. The IRSP forwards the request message to the target user or device 2. The target user or device 2 replies to this relationship establishment request message and sends a relationship establishment response message to the IRSP. Once the IRSP receives the response message, it updates the new relationship if the relationship is established and forwards the response message to the source user or device 1.

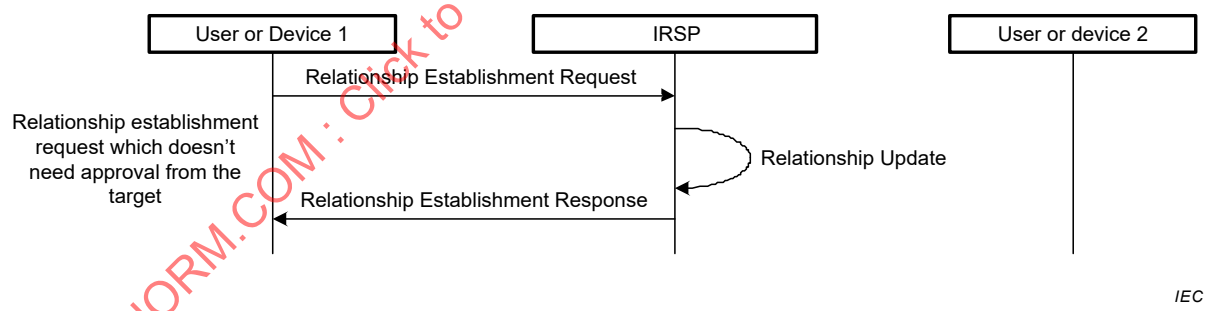
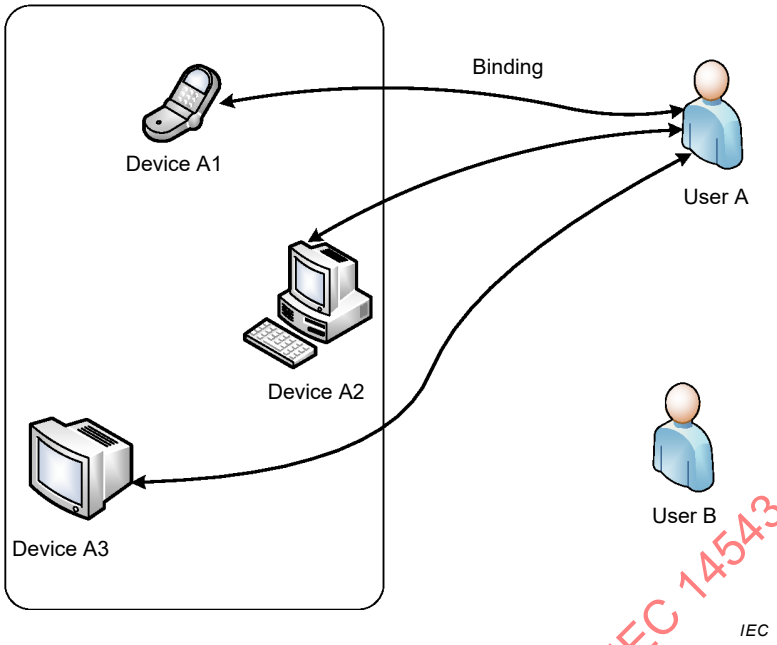


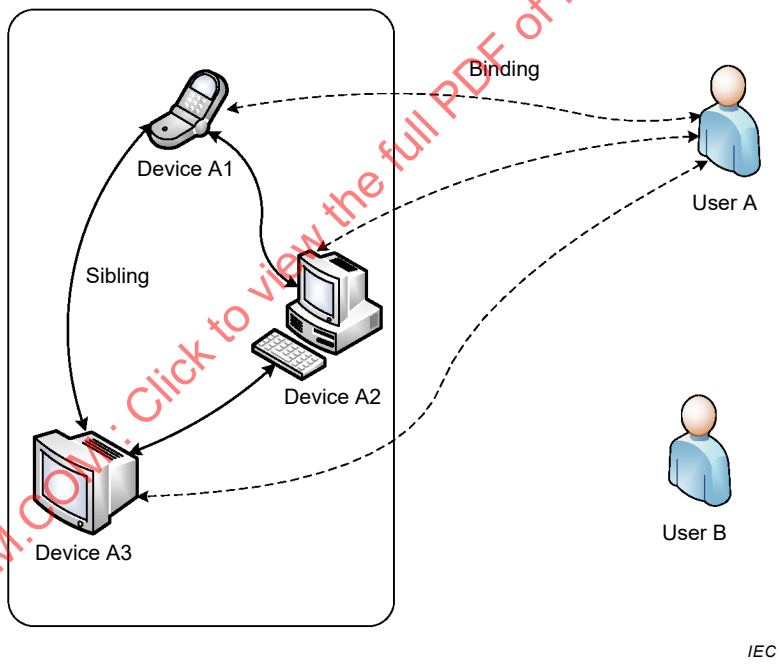
Figure 5 – Flow of relationship establishment request which does not need approval from target

In the workflow of Figure 5, the user or device 1 sends a relationship establishment request message to the IRSP. The IRSP decides if the relationship can be established according to the Pre-approval status of the target user or device 2 that has been stored on the IRSP in advance. Finally, the IRSP updates the new relationship if the relationship is established and sends a relationship establishment response message to the source user or device 1.

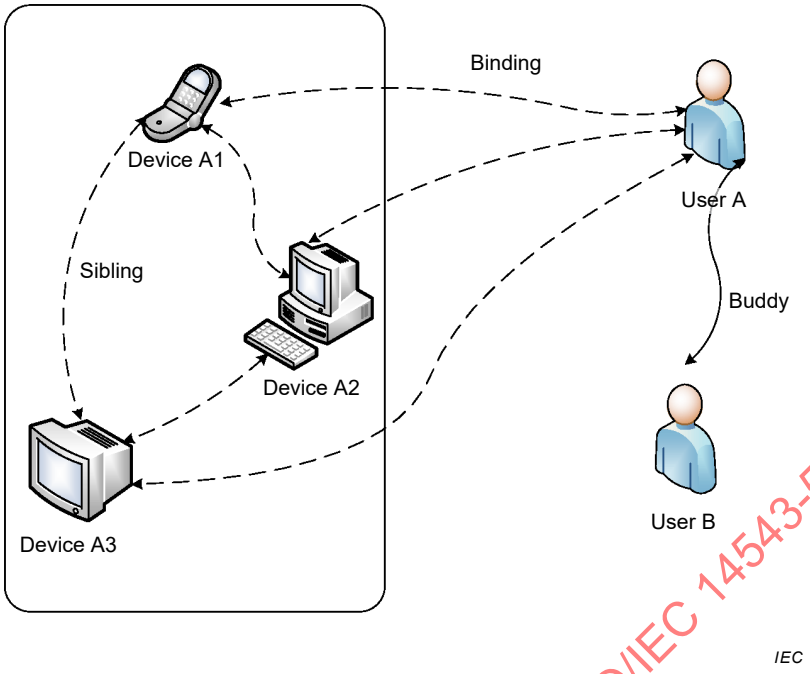
Three types of interactive relationships can be established as shown in Figure 6:



a) Binding between user and device



b) Sibling between device and device



c) Buddy between user and user

Figure 6 – IGRS RA Relationships

a) Binding: user–device

This is a relationship between user and device as shown in Figure 6 a). The binding shows the user ownership of the devices. A "roster" is maintained for each user or device. A user can be found in the corresponding roster of the binding device. By the same token, a device can be found in the corresponding roster of the bound user. The user is permitted to obtain information of the binding device (device IDs, online/offline status, etc.). Collaborative message exchanges are allowed between a user or device and the bound device or user. One user may bind multiple devices and one device may be bound by multiple users.

In Figure 6 a), "User A" owns three devices: A1, A2 and A3. That is, "User A" has binding relationships with "Device A1", "Device A2"and "Device A3". All three devices and User A exist in the others' roster. When "User A" changes its online/offline status, "Device A1", "Device A2"and "Device A3" all receive a notification message. By the same token, when any of the three devices changes its online/offline status, "User A" receives a corresponding notification. "User A" can choose one device as the target and send the collaborative application messages to it. Similarly, any one of the three devices can also set "User A" as the target and send the collaborative application messages.

b) Sibling: device–device

This is a relationship between device and device as shown in Figure 6 b). When two devices are bound with the same user, these two devices are in a sibling relationship with each other. Sibling devices shall be listed in each other's roster. One device shall be allowed to get information about its sibling devices (device IDs, online/offline status, etc.). All sibling devices can exchange collaborative messages with each other.

In Figure 6 b), "Device A1", "Device A2" and "Device A3" all belong to "User A"; thus they are in a sibling relationship with each other and they shall exist in the other siblings' roster. Whenever one of the devices changes its online/offline status, its siblings shall receive the corresponding notifications. Any one of the devices can choose one of its siblings as the target and send the collaborative application messages.

c) Buddy: user–user

This is a relationship between user and user as shown in Figure 6 c). Buddy means a trusting relationship. A buddy user shall be listed in his/her buddies' roster. User shall be allowed to get information (user ID, online/offline status, etc.) of his/her buddies. User can exchange collaborative messages with his/her buddies.

A user can choose to set his/her device access rights to other users. When one user grants device access rights to his/her buddies, the accessible binding devices and this user shall then be listed in his/her buddies' roster. This simplifies the user authentication process of the system; in particular, when the user is not online, other buddies shall still be allowed to access the user's devices. This means that the user's binding devices can be set as the targets and his/her buddies can send collaborative messages to access these devices.

If a user does not give his/her device access rights to the other users, his/her binding device shall not be listed in his/her buddy's roster. His/her buddy shall not be allowed to get information (user ID, online/offline status, etc.) of his/her bound device. His/her buddy cannot send messages to the user's bound device. However, if the user's IGRS RA device maintains both the user connection and device connection simultaneously, the user's buddy can still achieve collaborative applications with the user's bound device indirectly by sending collaborative messages using the user connection, or by sending collaborative messages to the PubSub (Publish-Subscribe) node of the user.

In Figure 6 c), "User A" and "User B" have a buddy relationship. They exist in each other's roster. When one of the users changes the online/offline status, the other shall receive a notification. "User A" or "User B" can set the other one as the target and send collaborative application messages to each other. "User A" can choose to give the device access rights of "Device A1", "Device A2"and "Device A3" to "User B". If the access rights are granted, the three devices shall then be listed in the roster of "User B". Whenever these devices change the online/offline status, "User B" shall receive notifications. "User B" can set the devices as the target and send collaborative messages. "User B" shall also be listed in the rosters of the three devices.The detailed introduction of device access rights configuration is given in Clause 9.

10.2 Relationship management mechanism

The IGRS RA relationship management mechanism is an extension to the general roster management mechanism defined in IETF RFC 6120. The concepts of "User" and "Device" are introduced and the roster management flow is extended.

a) PubSub subscription management in relationship management

A PubSub node is established for each user and device to support different interactive modes. Whenever the IRSP executes any relationship operations between the IGRS RA users and devices, it shall also execute any corresponding PubSub subscription operations simultaneously (see IETF RFC 6120).

b) Recognition of all relationship operations

As described in 10.1, different relationships are established between users and devices. These relationships are stored in the rosters of the users and devices. However, because different relationships have different meanings, when the IRSP processes the roster-related messages, it first needs to determine the types of object (user or device) that are involved before establishing the corresponding relationship.

In order to determine the correct relationship, the user ID or device ID is required. The first character of an IGRS RA device ID shall be "#", and the first character of an IGRS RA user ID shall not be "#" (see 7.2 and 7.3).

c) Rules of relationship establishment

During the process of relationship establishment, if the target object of the relationship establishment is an IGRS RA user, the subscription request of the presence status of the user shall be sent to the online resources of the user. The target user shall decide to accept or reject this subscription request.

If the target object of the relationship establishment is an IGRS RA device with UI, the subscription request to the device presence status shall be sent to the device. The device shall display the subscription request and let the user decide to accept or reject this subscription request.

If the target object of the relationship establishment is an IGRS RA device without UI, or if the user cannot directly process the relationship establishment for whatever reason, a device verification code shall be used to extend the presence status subscription

management. The IGRS RA user or device first creates a user or device verification code. When another user or device wants to subscribe to the presence status of this user or device, he or it shall include a user or device verification code of the target user or device in the subscription request messages. If the user or device verification code in the subscription request message matches the user or device verification code of the target user or device, then the subscription request message is approved automatically. The detailed methods of device verification code generation are outside of the scope of this document.

This document specifies IGRS RA relationship management mechanism in terms of how to establish and release relationships. In the following descriptions, the source is the object that subscribes to the presence status of the others; the target is the object that receives the subscription request.

10.3 Relationship establishment

10.3.1 Messages for relationship establishment request

A source shall follow 3.1.1 of IETF RFC 6121 to send presence subscription request to the target to establish relationship.

When an IGRS RA user intends to establish a binding relationship with an IGRS RA device without UI, the presence subscription request message shall follow Message 9.

Message 9 – Binding relationship establishment request message with device verification code

```
<presence id='message SN' to='target device ID' type='subscribe'>
        <igrs xmlns='http://www.igrs.org/spec2.0/basic#relationship>
                <verifycode> target device verification cade (optional)<verifycode>
        </igrs>
</presence>
```

10.3.2 Relationship establishment request procedure for IRSP

10.3.2.1 Overview

When the IRSP processes the relationship establishment request sent from an IGRS RA user, 3.1.2 of IETF RFC 6121 shall be followed.

10.3.2.2 Target does not exist

When the IRSP receives the relationship establishment request message from the source, it shall first check whether the target exists. If the target user or device ID does not exist in the IRSP, it shall discard the relationship establishment request and stop the subsequent processing.

10.3.2.3 Target exists and IRSP accepts request automatically

If the IRSP finds the target device or user ID and the relationship establishment request satisfies one of the following three conditions:

a) the source has successfully subscribed to the presence status of the target;

b) the source holds Pre-approval status in the roster of the target;

c) the relationship establishment request message includes the device verification code, and it matches the device verification code of the target stored in the IRSP;

then the IRSP shall accept the relationship establishment request automatically and send a relationship establishment acceptance response message to the source as in Message 10.

Message 10 – Relationship establishment acceptance response message

<presence id='*message SN*' from='*target user or device ID*' to='*source user or device ID*' type='subscribed'/>

If the target is online, for each online connection instance of the target, the IRSP shall send an online announcement message as in Message 11 to the source.

Message 11 – Target online announcement message

<presence from='*target user or device ID*' to='*source user or device ID*'/>

If the request is a binding relationship establishment request (the source is an IGRS RA user and the target is an IGRS RA device), the IRSP shall set the group attribute of the target in the roster of the source as MyDevices, and set the group attribute of the source in the roster of the target as MyOwner.

10.3.2.4 Target exists and IRSP forwards request to target

If the relationship establishment request does not satisfy the conditions listed in 10.3.2.3, the IRSP shall forward the relationship establishment request message to all the online resources of the target (generally an IGRS RA user).

If the target has no online resource, the IRSP shall first store the relationship establishment request message and then send the request message to the target when any of the target resources is online.

If the request is not accepted or rejected by any target or the IRSP, the IRSP shall send the above relationship establishment request message to the new online resource of the target whenever a new online resource is created by the target. However, for the same source, the IRSP shall only store the latest relationship management message received from the source. That is, if the source has sent multiple relationship management messages to the target when the target is offline, then when the target goes online, the IRSP shall only send the last relationship management message received from the source to the online resources of the target.

10.3.3 Target accepts or rejects relationship establishment request

When the target receives a relationship establishment request message, it shall accept or reject the request according to its local service logic. The local service logic of the target is defined and implemented by the target itself. For example, the request may be displayed with a UI so that the user may decide whether to accept the request, or the request may be automatically processed depending on the result of comparing the internal device verification code without any user intervention, etc.

If the target accepts the relationship establishment request, the target shall send a relationship establishment acceptance response message as in Message 10 to the source.

The target shall still send a relationship establishment acceptance response message as in Message 10 to the specified source to pre-approve relationship establishment even when a relationship establishment request message is not received. If a target sets “Pre-approval” to a specified source on the IRSP, once the IRSP receives a relationship establishment request message from the source, it shall accept the request according to 10.3.2.3 automatically without forwarding the request message to the target.

If the target rejects the relationship establishment request, it shall return a relationship establishment rejection message to the source as in Message 12.

Message 12 – Relationship establishment rejection response message

<presence id='*message SN*' from='*target user or device ID*' to='*source device or user ID*' type='unsubscribed'/>

10.3.4 IRSP processes relationship establishment acceptance message from target

When the IRSP receives a relationship establishment acceptance response message as in Message 10, it shall be processed as described in 10.3.2.3. However, as there may be no items for the source in the roster of the target (for example, the target sends a relationship establishment acceptance response message as in Message 10 without receiving any relationship establishment request message from the source), additional flow processes are needed to extend those described in 10.3.2.3.

The IRSP shall create or update a corresponding item in the roster of the target. The Jabber ID (JID) attribute of this item is the source user or device ID. The other attributes shall be configured as in Table 2.

Table 2 – Rules of IRSP processing target relationship establishment acceptance response messages

Original status	New status	Forward or not
None	None, Pre-approval	No
None, Pre-approval	None, Pre-approval	No
None + Pending Out	None + Pending Out, Pre-approval	No
None + Pending Out, Pre-approval	None + Pending Out, Pre-approval	No
None + Pending In	From	Yes
None + Pending Out + In	From + Pending Out	Yes
To	To, Pre-approval	No
To, Pre-approval	To, Pre-approval	No
To + Pending In	Both	Yes
From	From	No
From + Pending Out	From + Pending Out	No
Both	Both	No

In the case of the “Forward or not” item being “Yes” in Table 2, the IRSP shall send a relationship establishment acceptance response message as in Message 13 to the source. In addition, if the target is online, for each online resource of the target, the IRSP shall send an online advertisement message as in Message 14.

Message 13 – Relationship establishment acceptance response message

<presence from='*target user or device ID*' to='*source user or device ID*' type='subscribed'/>

Message 14 – Target online advertisement message

<presence from='*target user or device ID*' to='*source user or device ID*'/>

In Table 2, if the new status is “From”, the IRSP shall examine if the relationship establishment acceptance response message is a binding relationship management message. If it is (the source is an IGRS RA user and the target is an IGRS RA device), the IRSP shall set the target group attribute in the source roster as MyDevices, and set the source group attribute in the target roster as MyOwner.

In the above steps, if the IRSP creates or modifies any items, it shall push a message with the created or modified items as in Message 15 to all the interested resources of the target.

Message 15 – Roster message pushed by the IRSP to all the interested connections of the target

```
<iq to='interested connection ID of the target' type='set' id='message SN'>
        <query xmlns='jabber:iq:roster'>
                <item jid='source user or device ID' name='name' subscription='new status'>
                        <group>contact group</group>
                </item>
        </query>
</iq>
```

The <group> segment in Message 15 is optional. If the roster does not have a group, then this segment is removed.

10.4 Releasing relationship

Any of the two parties in a relationship can send a relationship releasing request message to the IRSP to release the existing relationship. The relationship releasing flow is shown in Figure 7.

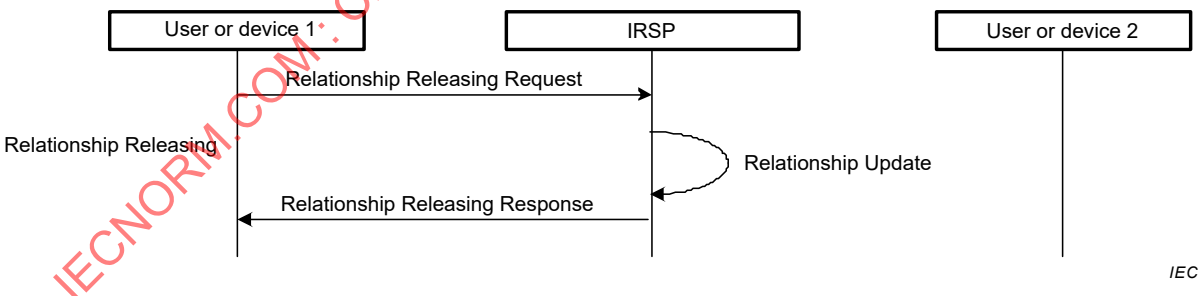


Figure 7 – Flow of relationship releasing

When an IGRS RA user wants to release an existing relationship, he or she shall follow 3.1.1 of IETF RFC 6121 and send a presence unsubscription request message as in Message 16 to the IRSP.

Message 16 – Relationship releasing request message sent by an IGRS RA user

```
<presence id='message SN' to='target user or device ID' type='unsubscribe'/>
</presence>
```

The IRSP shall check if the device ID of the to-be-released device exists in the roster of the user. If it does not exist, the IGRS RA service shall discard the request; otherwise, the IRSP shall follow IETF RFC 6121 to modify the items and send the messages accordingly.

When an IGRS RA device wants to release its relationship with a user, it shall follow 3.1.1 of IETF RFC 6121 to send a presence unsubscription message as in Message 17 to the IRSP.

Message 17 – Relationship releasing request message sent by an IGRS RA device

<presence id='*message SN*' to='*target user ID*' type='unsubscribed'/>
</presence>

The IRSP shall check if the user ID of the to-be-released user exists in the roster of the device. If he/she does not exist, the IGRS RA service shall discard the request; otherwise, the IRSP shall follow IETF RFC 6121 to modify the items and send the messages accordingly.

10.5 Device verification code management

10.5.1 Device verification code management initiated by IGRS RA user

An IGRS RA user shall send device verification code management request message as in Message 18 to create/modify/delete his or its device verification code of his or her devices.

Message 18 – Device verification code management request message sent by IGRS RA user

<iq type='set' id='*message SN*' to='*target device ID*'>
    <queryxmlns='http://www.igrs.org/spec2.0/basic#relationship'>
        <verifycode>*empty or new device verification code*<verifycode>
    </query>
</iq>

IRSP shall set the device verification code of the IGRS RA device in the database as the "verifycode" segment in Message 18 once it receives a device verification code management request message as in Message 18. If the "verifycode" segment is empty, the IRSP shall remove the device verification code of the IGRS RA device. This means that the IGRS RA device has no device verification code in the IRSP. After successfully processing the device verification code management request message, the IRSP shall return Message 19.

Message 19 – Device verification code management acceptance response message for request message sent by IGRS RA user

<iq from='*target device ID*' to='*source user ID of the management request message*'
type='result' id='*message SN*'>
    <query xmlns='http://www.igrs.org/spec2.0/basic#relationship'>
        <verifycode> *'verifycode' in the request message*<verifycode>
    </query>
</iq>

If the IRSP fails to process the device verification code management request message, it shall return a device verification code management error response message as in Message 20.

Message 20 – Device verification code management error response message for request message sent by IGRS RA user

<iq from='*target device ID*' to=' *source user ID of the management request message*' type='error' id='*message SN*'>
<query xmlns='http://www.igrs.org/spec2.0/basic#relationship'>
<verifycode>*'verifycode' in the request message*<verifycode>
</query>
<error type='cancel'>
<internal-server-errorxmlns='urn:ietf:params:xml:ns:xmpp-stanzas'/>
</error>
</iq>

10.5.2 Device verification code management initiated by IGRS RA device

An IGRS RA device shall send device verification code management request message as in Message 21 to create/modify/delete its device verification code.

Message 21 – Device verification code management request message sent by IGRS RA device

<iq type='set' id='*message SN*'>
<queryxmlns='http://www.igrs.org/spec2.0/basic#relationship>
<verifycode> *empty or new device verification code* <verifycode>
</query>
</iq>

IRSP shall set the device verification code of the IGRS RA device in the database as the "verifycode" segment in Message 21 once it receives a device verification code management request message as in Message 21. If the "verifycode" segment is empty, the IRSP shall remove the device verification code of the IGRS RA device. This means that the IGRS RA device has no device verification code in the IRSP. After successfully processing the device verification code management request message, the IRSP shall return Message 22.

Message 22 – Device verification code management acceptance response message for request message sent by IGRS RA device

<iq to='*source device ID of the management request message*' type='result' id='*message SN*'>
<query xmlns='http://www.igrs.org/spec2.0/basic#relationship'>
<verifycode> *'verifycode' in the request message*<verifycode>
</query>
</iq>

If the IRSP fails to process the device verification code management request message, it shall return a device verification code management error response message as in Message 23.

Message 23 – Device verification code management error response message for request message sent by IGRS RA device

<iq to=' *source device ID of the management request message*' type='error' id='*message SN*'>
<query xmlns='http://www.igrs.org/spec2.0/basic#relationship'>
<verifycode>*'verifycode' in the request message*<verifycode>
</query>
<error type='cancel'>
<internal-server-errorxmlns='urn:ietf:params:xml:ns:xmpp-stanzas'/>
</error>
</iq>

11 Message exchange

11.1 Overview

In the IGRS RA system, the messages exchanged between users and devices shall all go through the IRSP. The IRSP shall identify the usability of the exchange request message from the source user or device and terminate the message exchange procedure when the following cases happen:

a) the source user or device does not have the message exchange rights with the target;

b) relationship between the source and target does not allow message exchange between them;

c) request message contains wrong contents.

11.2 User or device ↔ User or device message exchange that needs response

Functional flow is shown in Figure 8.

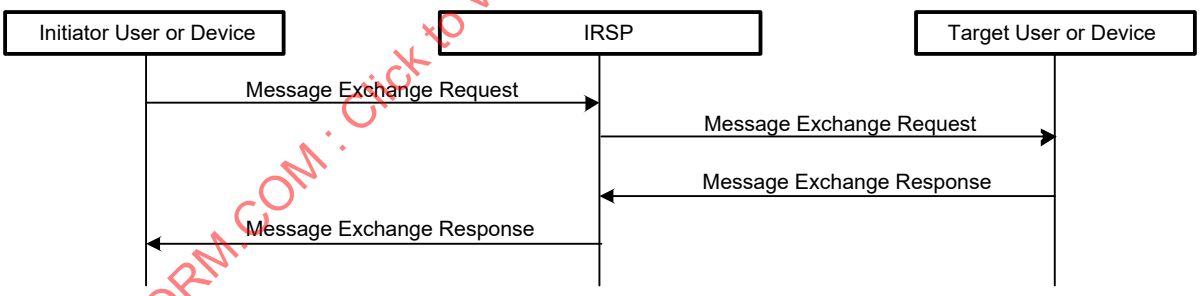


Figure 8 – Flow of message exchange between user or device and user or device that needs response

When a user or device wants to exchange messages with another user or device, and he/she/it needs the target user or device to return a response message, the message exchange source shall send a message exchange request message to the IRSP as in Message 24.

Message 24 – Exchange request message that needs response

<iq id='*message SN*' from='*source user or device ID*' to='*target user or device ID*' type='get'>
<query xmlns='http://www.igrs.org/spec2.0/basic#control'>
<data>request_data_base64</data>
</query>
</iq>

The IRSP shall receive the exchange request message and forward the received message to the target user or device. The target user or device processes according to the message content and sends the response message to the IRSP. The response message shall be as shown in Message 25.

Message 25 – Exchange request response message for Message 24

If successful:

<iq id='*message SN*' from='*target user or device ID*' to='*source user or device ID*' type='result'>
<query xmlns='http://www.igrs.org/spec2.0/basic#control'>
<data>response_data_base64</data>
</query>
</iq>

If failed:

<iq id='*message SN*' from='*target user or device ID*' to='*source user or device ID*' type='error'>
<error code='503' type='CANCEL'>
<service-unavailable xmlns='urn:ietf:params:xml:ns:xmpp-stanzas'/>
</error>
</iq>

The IRSP shall forward the request response message to the source user or device.

11.3 User or device ↔ User or device message exchange that does not need response

Functional flow is shown in Figure 9.

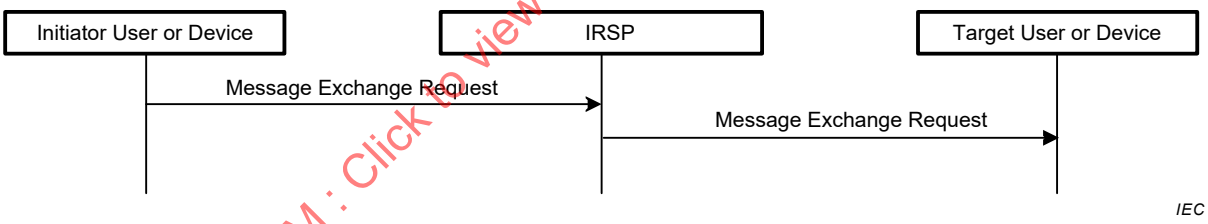


Figure 9 – Flow of message exchange between user or device and user or device that does not need response

This flow is used to exchange messages when one user or device requests a message exchanging with another user or device but does not need the target user or device to respond to the request. The source shall send Message 26 to the IRSP.

Message 26 – Exchange request message that does not need response

<message id='*message SN*' from='*source user or device ID*' to='*target user or device ID*' type='normal'>
<query xmlns='http://www.igrs.org/spec2.0/basic#status'>
<data>data_base64</data>
</query>
</iq>

IRSP shall receive the exchange request message and forward the message to the target user or device. The target user or device does not need to respond to the request.

11.4 User or device ↔ IRSP message exchange

Functional flow is shown in Figure 10.

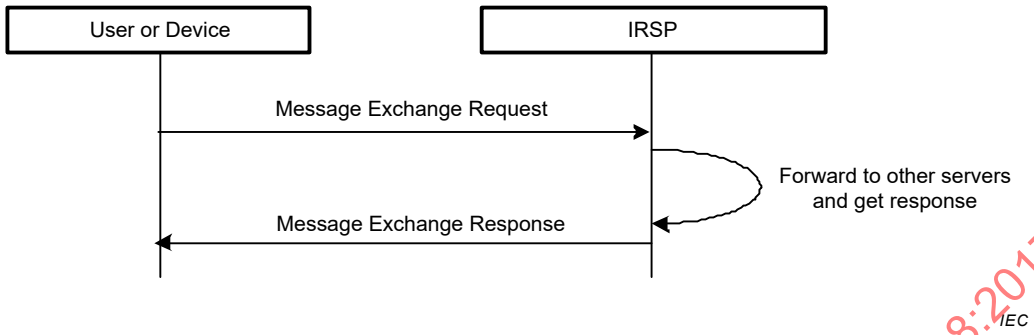


Figure 10 – Flow of message exchange between user or device and IRSP

When a user or device needs to exchange messages with another server in the IRSP, or a third party server outside of the IRSP, the message exchange source shall send a message exchange request message to the IRSP as in Message 27.

Message 27 – Exchange request message that needs response

```
<iq id='message SN' from='source user or device ID' type='set'>
        <query xmlns='http://www.igrs.org/spec2.0/basic#forward'>
                <data>data_base64</data>
        </query>
</iq>
```

IRSP shall forward the message to the corresponding servers according to the request of the message. The corresponding server may be a server in the IGRS RA system, or a third party server outside of the system. After processing the message, the IRSP shall send the exchange response message as in Message 28 to the source user or device.

Message 28 – Exchange request response message for Message 27

If successful:

```
<iq id='message SN' to='source user or device ID' type='result'>
        <query xmlns='http://www.igrs.org/spec2.0/basic#control'>
                <data>response_data_base64</data>
        </query>
</iq>
```

If failed:

```
<iq id='message SN' to='source user or device ID' type='error'>
        <error code='503' type='CANCEL'>
                <service-unavailable xmlns='urn:ietf:params:xml:ns:xmpp-stanzas'/>
        </error>
</iq>
```

11.5 IGRS RA server pushes message to user or device

Functional flow is shown in Figure 11.

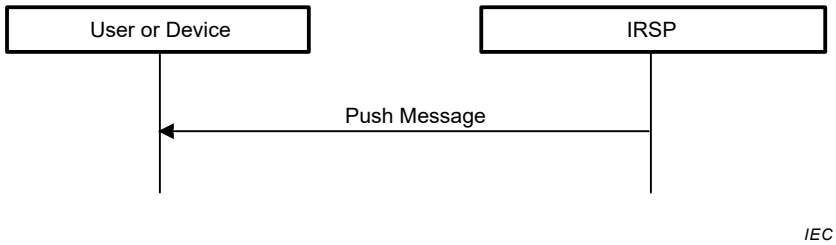


Figure 11 – IRSP pushes message to user or device

When the IRSP needs to push messages to an IGRS RA user or device, this message exchanging flow is used. The message is as in Message 29.

Message 29 – Message pushed from IRSP to IGRS user or device

```
<message from='Domain Name of the server' to='user or device ID' xml:lang='en'
type='normal' id='message SN'>
        <query xmlns='http://www.igrs.org/spec2.0/ basic#pushmessage'>
                <data>push_data_base64</data>
        </query>
</message>
```

11.6 IGRS RA NAT traversal

As shown in Figure 12, a public Internet terminal cannot push any collaborative message to a private network terminal that is behind a NAT device. Also two terminals that are in different private networks cannot exchange collaborative messages directly.

An IGRS RA server has a public Internet routable IP address. Even though an IGRS RA device is behind a NAT device, a data connection to an IGRS RA server can still be established. As a TCP/IP persistent connection is established between the IGRS RA device and server, the IGRS RA server can easily address and push messages to any online IGRS RA device. Additionally, if two IGRS RA devices are both on private networks, they can establish TCP/IP persistent connections to an IGRS RA server. The IGRS RA server can transport the messages and achieve collaborative message exchanges between two devices behind NAT devices.

The IGRS RA NAT traversal mechanism is based on a TCP/IP persistent connection between the user or device and IRSP. Each IGRS RA device behind the NAT device shall establish a persistent connection with IRSP. The IRSP can address each online IGRS RA device by this persistent connection and push messages to the online device.