



ISO/IEC 14543-5-1

Edition 1.0 2010-02

INTERNATIONAL STANDARD

**Information technology – Home electronic system (HES) architecture –
Part 5-1: Intelligent grouping and resource sharing for Class 2 and Class 3 –
Core protocol**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 35.240.67

ISBN 2-8318-1076-0

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

FOREWORD.....	8
INTRODUCTION.....	9
1 Scope.....	10
2 Normative references	10
3 Terms, definitions and abbreviations	11
3.1 Terms and definitions	11
3.2 Abbreviations	12
4 Conformance.....	13
4.1 IGRS network.....	13
4.2 IGRS devices	13
5 IGRS architecture.....	14
5.1 Overview	14
5.2 IGRS Core Protocol.....	15
5.3 IGRS Application Profile	15
5.4 IGRS Application	16
5.5 IGRS and other standards	17
6 IGRS device interaction model	18
6.1 Overview	18
6.2 Device online	19
6.3 Device (group) discovery.....	19
6.4 Device pipe setup.....	19
6.5 Device group setup and join	20
6.6 Service discovery	20
6.7 Session setup.....	21
6.8 Service invocation	21
6.9 Session termination.....	21
6.10 Device/Service online/offline event subscription	21
6.11 Device/Service online/offline event notification	22
6.12 Device/Service online/offline event unsubscription	22
6.13 Pipe disconnection	22
6.14 Device group dismiss and secession	22
6.15 Device offline	23
7 IGRS message framework	23
7.1 Overview	23
7.2 IGRS request/notification message structure	24
7.3 IGRS response message structure	25
7.4 IGRS message based on secure device pipe	26
7.4.1 Message authentication code generation	26
7.4.2 Message encryption.....	27
8 IGRS device and service description	27
8.1 IGRS device description	27
8.1.1 Device description template.....	27
8.1.2 Device identifier.....	31
8.1.3 Device group identifier.....	31
8.1.4 Device type identifier	32
8.1.5 Device security mechanism descriptor	33

8.2	IGRS service description	40
8.2.1	Service description template	40
8.2.2	Service identifier	51
8.2.3	Service type identifier	51
8.2.4	Service access control	52
8.2.5	Identity authentication mechanism of service access control	53
8.3	IGRS client description	56
8.4	IGRS user description	56
9	IGRS device grouping	56
9.1	Device advertisement	56
9.1.1	Device online advertisement	56
9.1.2	Device offline advertisement	58
9.2	Device pipe management	58
9.2.1	Unsecure device pipe setup	58
9.2.2	Unsecure device pipe maintenance	58
9.2.3	Secure device pipe setup	59
9.2.4	Secure device pipe teardown	79
9.2.5	Device trust relationship	80
9.2.6	Device online detection	80
9.3	Detailed device description document retrieval	81
9.3.1	Retrieve detailed device description document request	81
9.3.2	Retrieve detailed device description document response	82
9.4	Retrieve detailed device description document based on non-secure pipe	84
9.5	Device group setup	84
9.5.1	Global peer-to-peer device group	84
9.5.2	Specified peer-to-peer device group	84
9.5.3	Centralised device group	86
9.6	Device search	90
9.6.1	Device search based on multicast	90
9.6.2	Device search by proxy	94
9.7	Device online/offline event subscription	97
9.7.1	Device online/offline event subscription request	97
9.7.2	Device online/offline event subscription renewal request	99
9.7.3	Device online/offline event subscription response	100
9.7.4	Device online/offline event unsubscription	101
9.7.5	Device online/offline event notification	102
9.8	Device group search	104
9.8.1	Device group search request message	104
9.8.2	Device group search response message	105
10	IGRS resource sharing	107
10.1	Service online advertisement	107
10.1.1	Service online advertisement based on multicast	107
10.1.2	Service online registration and offline notification based on device pipe	109
10.2	Service search	111
10.2.1	Service search based on multicast	111
10.2.2	Service search by proxy	114
10.3	Service online/offline event subscription	117
10.3.1	Service online/offline event subscription request	117

10.3.2	Service online/offline event subscription renewal request	119
10.3.3	Service online/offline event subscription response	120
10.3.4	Service online/offline event unsubscription	121
10.3.5	Service online/offline event notification	122
10.4	Service description document retrieval	124
10.4.1	Retrieve service description document request	124
10.4.2	Retrieve service description document response	126
10.4.3	Other approaches to retrieve service description documents	127
10.5	Session	127
10.5.1	Session setup condition	127
10.5.2	Common session setup and teardown process	127
10.5.3	Session setup when service access control in master/slave device group is not consistent with device pipe security attribute	131
10.6	Service invocation	137
10.6.1	Service invocation request message	137
10.6.2	Service invocation response message	137
10.6.3	Notification message based on session	138
11	Request/response status codes	139
Annex A	(normative) IGRS service discovery protocols (ISDP)	142
A.1	General	142
A.2	ISDP message format	142
A.2.1	General	142
A.2.2	ISDP start-lines	142
A.2.3	ISDP message headers	142
A.2.4	ISDP processing rules	143
A.3	ISDP usage in IGRS specification	143
Annex B	(normative) Description documents	145
B.1	Specification description	145
B.2	Session description	249
B.3	Service description	250
B.4	Pipe description	253
B.5	Device template	254
B.6	Master slave device group advertisement	256
B.7	Device type list	256
B.8	Peer-to-peer device group advertisement	257
B.9	Device description	257
Bibliography	259

Figure 1 – IGRS specification framework	15
Figure 2 – IGRS application interaction	17
Figure 3 – IGRS device interaction model	18
Figure 4 – Secure device pipe setup	59
Table 1 – IGRS request and notification message	24
Table 2 – IGRS response message	25
Table 3 – Message authentication code	27
Table 4 – Device security mechanism protocol algorithm	40
Table 5 – Service access control policy	53
Table 6 – Device authentication mechanisms and the corresponding encryption algorithm descriptor	56
Table 7 – Device online advertisement	57
Table 8 – Device offline advertisement	58
Table 9 – Pipe setup request based on symmetric-key cryptosystem	60
Table 10 – Pipe setup response based on symmetric-key cryptosystem	61
Table 11 – Pipe setup request based on symmetric-key authentication, encrypted message transmission, and authentication mechanism	61
Table 12 – Pipe setup response based on symmetric-key authentication, encrypted message transmission, and authentication mechanism	62
Table 13 – Pipe setup request based on authentication, encrypted message transmission, and authentication mechanism of public-key cryptosystem	63
Table 14 – Pipe setup response based on authentication, encrypted message transmission, and authentication mechanism of public-key cryptosystem	63
Table 15 – Pipe setup request based on trusted third party authentication, encrypted message transmission, and authentication mechanism	64
Table 16 – Pipe setup response based on trusted third party authentication, encrypted message transmission, and authentication mechanism	64
Table 17 – Authentication request based on identity authentication and message authentication mechanism of symmetric-key cryptosystem	65
Table 18 – Authentication response based on identity authentication and message authentication mechanism of symmetric-key cryptosystem	66
Table 19 – Authentication result request based on identity authentication and message authentication mechanism of symmetric-key cryptosystem	67
Table 20 – Authentication result response based on identity authentication and message authentication mechanism of symmetric-key cryptosystem	67
Table 21 – Authentication request based on identity authentication and encrypted message transmission and authentication mechanism of symmetric-key cryptosystem	68
Table 22 – Authentication response based on identity authentication and encrypted message transmission and authentication mechanism of symmetric-key cryptosystem	69
Table 23 – Authentication result request based on identity authentication and encrypted message transmission and authentication mechanism of symmetric-key cryptosystem	70
Table 24 – Authentication result response based on identity authentication and encrypted message transmission and authentication mechanism of symmetric-key cryptosystem	70
Table 25 – Authentication request based on authentication and encrypted message transmission and authentication mechanism of public-key cryptosystem	71

Table 26 – Authentication response based on authentication and encrypted message transmission and authentication mechanism of public-key cryptosystem	72
Table 27 – Authentication result request based on authentication and encrypted message transmission and authentication mechanism of public-key cryptosystem	73
Table 28 – Authentication result response based on authentication and encrypted message transmission and authentication mechanism of public-key cryptosystem	74
Table 29 – Authentication request based on authentication, encrypted message transmission, and authentication mechanism of trusted third party	75
Table 30 – Authentication response based on authentication, encrypted message transmission, and authentication mechanism of trusted third party	76
Table 31 – Authentication result request based on authentication, encrypted message transmission, and authentication mechanism of trusted third party	77
Table 32 – Authentication result response based on authentication, encrypted message transmission, and authentication mechanism of trusted third party	78
Table 33 – Secure device pipe setup confirmation request.....	78
Table 34 – Secure device pipe setup confirmation response	79
Table 35 – Secure device pipe teardown notification message.....	80
Table 36 – Trust relationship formed between devices after pipe setup.....	80
Table 37 – Device online detection request message.....	81
Table 38 – Device online detection response message	81
Table 39 – Device description document retrieval request message.....	82
Table 40 – Device description document retrieval response message	83
Table 41 – Device group advertisement message of specified peer-to-peer device group	85
Table 42 – Device leaves a specified peer-to-peer device group quit group message	86
Table 43 – Device group advertisement message of master-slave device group	87
Table 44 – Request message to join a master-slave device group	88
Table 45 – Response message to join a master-slave device group.....	88
Table 46 – Device group dissolve notification message sent by master device.....	89
Table 47 – Withdraw notification message sent by slave device.....	89
Table 48 – Device search request message.....	90
Table 49 – Device search response message	92
Table 50 – Device search request that slave device generates to master device.....	94
Table 51 – Device search response message	96
Table 52 – Device event subscription request message	98
Table 53 – Device online/offline event subscription renewal request message	100
Table 54 – Device online/offline event subscription response message.....	101
Table 55 – Device online/offline event unsubscription message	102
Table 56 – Device online/offline event notification message.....	103
Table 57 – Device group search request message	105
Table 58 – Device group search response message	106
Table 59 – Service online advertisement message.....	108
Table 60 – Service offline advertisement message.....	109
Table 61 – Service online registration notification message	110
Table 62 – Service offline notification message.....	111
Table 63 – Multicast-based service search request message	112

Table 64 – UDP unicast-based service search request message.....	113
Table 65 – Service search request message by proxy.....	115
Table 66 – Service search response message by proxy	116
Table 67 – Service online/offline event subscription request message	118
Table 68 – Service online/offline event subscription renewal request	120
Table 69 – Service online/offline event subscription response.....	121
Table 70 – Service online/offline event unsubscription message	122
Table 71 – Service online/offline event notification message.....	123
Table 72 – Retrieve service description document request message.....	125
Table 73 – Retrieve service description document response message	126
Table 74 – Common session setup request message.....	128
Table 75 – Token setup and structure	129
Table 76 – Common session setup response message	130
Table 77 – Common session teardown notification message.....	131
Table 78 – Retrieve session encryption key generation request	133
Table 79 – Retrieve session encryption key generation response	134
Table 80 – Session encryption key transfer request message	135
Table 81 – Session encryption key transfer response message.....	136
Table 82 – Service invocation request message.....	137
Table 83 – Service invocation response message	138
Table 84 – Notification message based on session	139
Table 85 – Response status code category.....	140
Table 86 – Response status code definition	141

INFORMATION TECHNOLOGY – HOME ELECTRONIC SYSTEM (HES) ARCHITECTURE –

Part 5-1: Intelligent grouping and resource sharing for Class 2 and Class 3 – Core protocol

FOREWORD

- 1) ISO (International Organization for Standardization) and IEC (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. Their preparation is entrusted to technical committees; any ISO and IEC member body interested in the subject dealt with may participate in this preparatory work. International governmental and non-governmental organizations liaising with ISO and IEC also participate in this preparation.
- 2) In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.
- 3) The formal decisions or agreements of IEC and ISO on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC and ISO member bodies.
- 4) IEC, ISO and ISO/IEC publications have the form of recommendations for international use and are accepted by IEC 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.
- 5) In order to promote international uniformity, IEC 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 publication and the corresponding national or regional publication should be clearly indicated in the latter.
- 6) ISO and IEC provide no marking procedure to indicate their approval and cannot be rendered responsible for any equipment declared to be in conformity with an ISO/IEC publication.
- 7) All users should ensure that they have the latest edition of this publication.
- 8) 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 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.
- 9) 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.
- 10) Attention is drawn to the possibility that some of the elements of this International Standard 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 14543-5-1 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 web site.

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.

INTRODUCTION

ISO/IEC 14543-5, Intelligent Grouping and Resource Sharing for HES (IGRS), is divided into six parts:

➤ **IGRS Part 5-1: Core Protocol**

- Specifies the TCP/IP protocol stack as the basis and the HTTP protocol as the message-exchanging framework among devices.
- Defines 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 transport within a home.

➤ **IGRS Parts 5-2#: Application profile** (under consideration)

- Based on the IGRS Core Protocol.
- Defines a device and service interaction mechanism, as well as application interfaces used in IGRS Basic Applications.
- Multiple application profiles are being developed, including:
 - Part 5-21: AV Profile (under consideration)
 - Part 5-22: File Profile (under consideration)
- Additional application profiles are planned (part numbers to be assigned; these projects are under consideration)
 - Part 5-2w: DVD Profile
 - Part 5-2x: QoS Profile
 - Part 5-2y: DMCP Profile
 - Part 5-2z: Universal Control Profile

➤ **IGRS Part 5-3: Basic Application** (under consideration)

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

➤ **IGRS Part 5-4: Device Validation** (under preparation)

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

➤ **IGRS Part 5-5: Device Types** (under consideration)

- Defines IGRS Device types used in IGRS applications.

➤ **IGRS Part 5-6: Service Types** (under consideration)

- Defines basic service types used in IGRS applications.

INFORMATION TECHNOLOGY – HOME ELECTRONIC SYSTEM (HES) ARCHITECTURE –

Part 5-1: Intelligent grouping and resource sharing for Class 2 and Class 3 – Core protocol

1 Scope

This part of the ISO/IEC 14543 specifies the services and protocol of the application layer for use by IGRS Devices in the Home Electronic System. An IGRS Device (Intelligent Grouping and Resource Sharing Device) includes the communications protocol specified in the multiple parts of ISO/IEC 14543-5. The objective of this standard is to enable resource sharing and service collaboration among devices. This standard describes:

- the interoperability mechanism;
- the process and messaging format of device discovery and device grouping;
- the process and messaging format of resource sharing among IGRS Devices;
- IGRS Device and service description requirements.

This standard is applicable to resource sharing and service collaboration among computers, consumer electronics, and communication devices in a Local Area Network (LAN) or Personal Area Network (PAN) environment, especially in a wireless dynamic network.

2 Normative references

The following referenced documents are indispensable for the application 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.

The provisions of the referenced specifications other than ISO/IEC, IEC, ISO and ITU documents, as identified in this clause, are valid within the context of this International Standard. The reference to such a specification within this International Standard does not give it any further status within ISO or IEC. In particular, it does not give the referenced specification the status of an International Standard.

ISO/IEC 9594-8:2005, *Information technology – Open Systems Interconnection – The directory: Public-key and attribute certificate frameworks*

ISO/IEC 10118-3:2004, *Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions*

ISO/IEC 18033-3, *Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers*

ISO/IEC 19790, *Information technology – Security techniques – Security requirements for cryptographic modules*

ISO/IEC 29341-1:2008, *Information technology – UPnP Device Architecture – Part 1: UPnP Device Architecture Version 1.0*

IEEE 1363:2000, *Standard Specifications For Public Key Cryptography*

IETF RFC 1510: *The Kerberos Network Authentication Service (V5)*

IETF RFC 1766: *Tags for the Identification of Languages*

IETF RFC 2234: *Augmented BNF for Syntax Specifications: ABNF*

IETF RFC 2616: *Hypertext Transfer Protocol -- HTTP/1.1*

IETF RFC 2774: *An HTTP Extension Framework*

IETF RFC 3447: *Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1*

W3C-REC-XML-1998-210:1998, *Extensible Markup Language (XML) 1.0*

W3C SOAP 1.2: *Simple Object Access Protocol Version 1.2*
<http://www.w3.org/2002/12/soap-envelope>

W3C WSDL 2.0: *Web Service Description Language Version 2.0*
<http://www.w3.org/TR/wsd20/>