

ISO/IEC 14543-5-1:2010-02 (E)

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

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
	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
	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