DRAFT INTERNATIONAL STANDARD ISO/IEC 29341-25-2

Attributed to ISO/IEC JTC 1 by the Central Secretariat (see page iii)

Voting begins on
2015-09-03

Voting terminates on
2015-12-03

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • ORGANISATION INTERNATIONALE DE NORMALISATION
INTERNATIONAL ELECTROTECHNICAL COMMISSION • МЕЖДУНАРОДНАЯ ЭЛЕКТРОТЕХНИЧЕСКАЯ КОММИСИЯ • COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

PUBLICLY AVAILABLE SPECIFICATION PROCEDURE

Information technology — UPnP Device Architecture

Part 25-2:
Telephony device control protocol — Telephony security best practice

Technologies de l'information — Architecture de dispositif UPnP —

Partie 25-2

ICS 35.200

This Publicly Available Specification (PAS) is being submitted for Fast-track processing in accordance with the provisions of ISO/IEC JTC 1 Directives.

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

© International Organization for Standardization, 2015
International Electrotechnical Commission, 2015



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2015

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

NOTE FROM ITTF

The ballot on the transposition of a PAS into an International Standard follows the JTC 1 PAS procedures contained in the JTC 1 Supplement, F.3.

Reflecting the importance of the PAS process, the JTC 1 secretariat shall also inform JTC 1 national bodies and Liaison Organisations, and those organisations authorized to be PAS submitters, of the initiation of any PAS ballot, the results of the ballot, and the identity of the JTC 1 subcommittee which will be responsible for any future work.

For ballot, JTC 1 National Bodies and the PAS Submitter shall receive both the PAS to be transposed and the accompanying Explanatory Report. During the ballot JTC 1 members may propose changes to the PAS. These can be resolved with the PAS Submitter after completion of the ballot.

The period for combined DIS voting shall be five months. In order to be accepted the DIS must be supported by 75 % of the votes cast (abstention is not counted as a vote) and by two-thirds of the P-members voting of JTC 1.

In the case of a failure of the ballot, JTC 1 shall make known to the Submitter the reasons which have led to the negative result. Based on this information, the Submitter may choose to re-submit a modified specification as a new PAS submission.

Once the Draft International Standard has been approved by JTC 1, it shall progress to the approval stage (FDIS).

© ISO/IEC 2015 — All rights reserved

Normative Terminology Changes

You ***must*** use the command `Old LoCase` from the Review group of the UPnP ribbon tab to locate and process lower case terms whose ISO/IEC meanings differ from their former UPnP meanings. Each such term is marked with a hidden bookmark, so there is no other easy way to identify them. (The former macro, `Review_OldLowerCase_Terms`, has been removed from the Word template `upnp4iecAdjunct.dotm`.)

Unlike upper case normative terms, lower case terms with new meanings cannot be mechanically corrected in the conversion for ISO/IEC. Each Working Committee needs to evaluate each of these terms in context to determine what changes to make.

Marked terms fall into one of the four following categories:

- **Non-normative in UPnP** (possibly with normative intent) → **normative in ISO/IEC**.
  Examples: "required", "shall", "recommended", "should", "may".
  - *Do not change*: Instances that actually had normative intent, but were not upper-cased.
  - *Change*: Instances that really were non-normative, to remain non-normative.
- **Non-normative in UPnP** (possibly with normative intent) → **statutory (legal or regulatory compliance) in ISO/IEC.**
  Example: "must".
  - *Do not change*: Instances that actually had statutory intent.
  - *Change*: Instances that actually had normative intent, but were not upper-cased.
    Example: "must" → "shall".
  - *Change*: Instances that really were non-normative, to remain non-statutory.
- **Non-normative in UPnP** (probably with normative intent) → **non-normative in ISO/IEC.**
  Examples: "mandatory", "prohibited", "optional".
  - *Change*: Instances that actually had normative intent, to be normative in ISO/IEC.

    Common replacements:
    "mandatory" → "required" "… is mandatory" → "shall …"
    "prohibited" → "not allowed"
    "optional" → "allowed"
  - *Change*: Instances of "mandatory" and "prohibit(s | ed | ing | ion)" that really were non-normative, to remain non-normative. The *ISO/IEC Directives* use the word "prohibit" in the definition of normative terms, and the word "mandatory" even more broadly in the definition of both normative and statutory terms.
  - *No need to change*: Non-normative instances of "optional".
- **Non-normative in UPnP → normative in ISO/IEC.**
  Examples: "ought", "allow", "permissible", "permit", "accept".

  Change: All instances, to avoid becoming normative.

More information about ISO/IEC normative (and more general "provisioning") terms may be found in the *ISO/IEC Directives, Part 2*, Annex H.

Table 0 — Open issues for ISO/IEC conversion

Status [a]	Document Locations [b]	Description [c]	UPnP Notes	Issue ID
U	5.3	The original definition of non-restrictable did not make sense technically. It effectively recommended that all non-restrictable actions should be called, not that they be allowed to be called.		20918-a
AU	2	Removed RFC 2119 from references, since it no longer applies.		
AU	3	Note that the abbreviated terms have been included with the terms themselves. This is the proper presentation for ISO/IEC documents. Some Telephony documents that were converted earlier have separated the abbreviations from their expansions. These should be corrected in those documents.		
AU	#	Most document-internal cross-references to figures and sections (now clauses, subclauses and annexes) ambiguous. All known occurrences were corrected.		
G-U	#	**Hanging paragraphs, singleton subdivisions** When a clause/subclause is subdivided into subclauses or an annex is subdivided into clauses, neither hanging paragraphs nor singleton subdivisions are allowed. • A *hanging paragraph* is any text, table, figure or any other content between the parent numbered paragraph and the first child subdivision. • A *singleton subdivision* is when there is only one subdivision at any level. There must be at least 2. **Pending GSC action:** GSC will provide a command to detect both hanging paragraphs and singleton subdivisions. **Pending UPnP action:** UPnP editors should correct all hanging paragraphs and singleton subdivisions as they encounter them, but the tool to identify them is coming.		
G-U	#	**Notes and Examples** The *ISO/IEC Directives* require that Notes and Examples be set off by a distinctive font style and/or indentation. Notes and Examples are also not allowed to contain normative statements. **Pending GSC action:** GSC will provide a command for the following UPnP use: **Pending UPnP action:** UPnP editors will use new command to walk through the document, stopping at each Note and Example that does not use the IEC ¶ style "NOTE". Proper informative instances need to be restyled. Instances with normative content need to be reworded, or the normative content moved elsewhere.		

Copyright © 2011 UPnP Forum. All rights reserved.

Status [a]	Document Locations [b]	Description [c]	UPnP Notes	Issue ID
G-U	#	**Cross-reference form** The *ISO/IEC Directives* require that all document cross-references to tables, figures, clauses, subclauses and subclauses be to the referent's (alpha)numeric designator, *not* to its title/caption/label. **Pending GSC action:** GSC will provide a command for the following UPnP use: **Pending UPnP action:** UPnP editors will use new command to walk through the document, stopping at each cross-reference that references the target's text instead of its alphanumeric designator, so that the editor can correct it.		
G	—	**Remove old styles** This document still contains ¶ and character styles used before the ISO/IEC conversion. These style need to be removed. **Pending GSC action:** GSC will provide a command that will automatically remove all of the old styles.		
G	—	**Use only approved styles** Word 2007 and 2010 can be configured to disable use of all styles not in the approved style sets for UPnP and ISO/IEC documents. **Pending GSC action:** GSC will provide a command to toggle the allowing and disallowing of unapproved styles.		
G-U	—	**Dual publishers** UPnP specifications are intended to be published by both UPnP and ISO/IEC. There are some minor differences in content and style between the two publishers. **Pending GSC action:** GSC will provide a command to toggle between publishers and check for document features disallowed by the designated target publisher. This includes but is not limited to: • Normative references may include UPnP documents when UPnP is the publisher. Only their ISO/IEC equivalents are allowed in ISO/IEC publications. • Header/footer contents differ. • Self-references to "this document" in UPnP become "this part of ISO/IEC 29341" in ISO/IEC. **Pending UPnP action:** Be aware of and manage these differences when preparing final versions for publication.		

Copyright © 2011 UPnP Forum. All rights reserved.

[a] **Status key:**

- • Informational, requires no action by anyone.
- G An issue that awaits action by G Shults Consulting (GSC).
- G-U An issue that awaits action by GSC, and then requires follow-up action by UPnP.
- U An issue that requires action by UPnP.
- U? An issue that GSC considers closed, but UPnP might disagree. UPnP should review.
- AU An issue that was resolved during conversion by GSC, but that UPnP needs to understand to avoid problem recurrence
- ✓ Issue is closed.

[b] **Document Locations**:

- # Numerous instances, not specifically identified.
- — Document generic, not tied to specific locations.

[c] GSC: G Shults Consulting, ISO/IEC conversion contractor

Copyright © 2011 UPnP Forum. All rights reserved.

Telephony:1 Security Best Practice

For UPnP Version 1.0

Status: Standardized DCP (SDCP)

Date: March 22, 2011

Document Version: 1.0

Service Template Version: 2.00

This Standardized DCP has been adopted as a Standardized DCP by the Steering Committee of the UPnP Forum, pursuant to Section 2.1(c)(ii) of the UPnP Forum Membership Agreement. UPnP Forum Members have rights and licenses defined by Section 3 of the UPnP Forum Membership Agreement to use and reproduce the Standardized DCP in UPnP Compliant Devices. All such use is subject to all of the provisions of the UPnP Forum Membership Agreement.

THE UPNP FORUM TAKES NO POSITION AS TO WHETHER ANY INTELLECTUAL PROPERTY RIGHTS EXIST IN THE STANDARDIZED DCPS. THE STANDARDIZED DCPS ARE PROVIDED "AS IS" AND "WITH ALL FAULTS". THE UPNP FORUM MAKES NO WARRANTIES, EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE STANDARDIZED DCPS, INCLUDING BUT NOT LIMITED TO ALL IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OF REASONABLE CARE OR WORKMANLIKE EFFORT, OR RESULTS OR OF LACK OF NEGLIGENCE.

Copyright © 2011 UPnP Forum. All rights reserved.

Authors [a]	Company
Yu Zhu (Editor)	Huawei
Yoshiki Nishikawa	NTT
Jeyoung Maeng	Samsung
Mayuresh Patil	Samsung
Mahfuzur Rahman	Samsung
Jooyeol Lee (Chair)	Samsung
Enrico Grosso	Telecom Italia
Massimo Messore	Telecom Italia
Davide Moreo	Telecom Italia
Alessandro De Vincentis	Telecom Italia

[a] Note: The UPnP Forum in no way guarantees the accuracy or completeness of this author list and in no way implies any rights for or support from those members listed. This list is not the specifications' contributor list that that is kept on the UPnP Forum's website.

Copyright © 2011 UPnP Forum. All rights reserved.

CONTENTS

1 Overview and Scope 7
1.1 Introduction 7
2 Normative references 7
3 Terms, definitions and abbreviated terms 8
4 Text conventions 9
5 Security Policies 10
5.1 Access Control and User Roles 10
5.2 General Policies 11
5.3 Security Policies for Telephony Services 11
5.3.1 *CallManagement:1* 11
5.3.2 *MediaManagement:1* 12
5.3.3 *Messaging:1* 12
5.3.4 *InputConfig:1* 13
5.3.5 *ConfigurationManagement:1* 13
6 Call Monopolization using DeviceProtection 14
6.1 TelCP-Level Call Monopolization 14
6.1.1 Incoming Call Handling (TelCP-Level) 15
6.2 User-Level Call Monopolization 17
6.2.1 Incoming Call Handling (User-Level) 18
6.3 Secure PHONE-based Call Monopolization 20
7 Secure Media Sessions 20
7.1 Secure A/V Call Session between TS and TC 20
8 Secure Input Sessions 23
Annex A (informative) Bibliography 25

Figure 1 — DP-based TelCP-level Call Monopolization 15
Figure 2 — Incoming call handling (TelCP-level) 16
Figure 3 — DP-based User-level Call Monopolization 17
Figure 4 — Incoming call handling (User-level) 19
Figure 5 — SRTP-based media session set up by a TelCP 21
Figure 6 — Secure input session set up by an ICP 23

Table 0 — Open issues for ISO/IEC conversion 2
Table 1 — *CallManagement:1* Actions 11
Table 2 — *MediaManagement:1* Actions 12
Table 3 — *Messaging:1* Actions 12
Table 4 — *InputConfig:1* Actions 13
Table 5 — *ConfigurationManagement:1* Actions 13

Copyright © 2011 UPnP Forum. All rights reserved.

1 Overview and Scope

This document is intended to serve as guidelines for implementing the UPnP *DeviceProtection* service [6] for UPnP Telephony version 1 Devices (i.e. *TelephonyServer:1* and *TelephonyClient:1*). Specifically, this document: recommends security policies for telephony services (e.g. default roles, and restricted set of Telephony actions, etc.), provides solutions for monopolization of calls using *DeviceProtection*, and discusses user privacy protection.

1.1 Introduction

UPnP Telephony enables telephony services (e.g. phone calls and messages) available to the home network. However, when telephony devices are exposed to the home network that is not trusted, there would be security threats. For example, a control point could discover a Telephony Server (TS) and make costly phone calls using the TS. Considering user privacy, a user's call logs and messages which are considered private can be read by a control point. Moreover, a malicious control point could discover conversations when a user is calling on a Telephony Client (TC) by eavesdropping of the traffic between the TS and the TC. The malicious control point could also steal user's information (e.g. accounts for online services) when the user is using input services by eavesdropping of the traffic between the input sender and receiver devices. When the home network is not trusted, the *DeviceProtection* service [6] can be implemented to the telephony devices as an option to provide secure means of using the telephony services in the home network. However, in a trusted home network, the security is not an issue since every home user trusts each other. In this document, guidelines for implementing *DeviceProtection* to UPnP Telephony devices are discussed, including:

- The default roles to be implemented, the recommended restricted telephony actions, and some other recommended security policies with regard to the implementation of the *DeviceProtection* service for the telephony specifications.
- The monopolization of calls using *DeviceProtection*.
- The protection of input data between the input sender and the receiver devices, and the voice/video communications between the TS and the TC using *DeviceProtection*.

However, security issues such as how to prevent a TS/TC or control point controlled by a malware are considered out of the scope of this document.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.~~This section lists the normative references used in this specification and includes the tag inside square brackets that is used for each such reference:~~

[1] – UPnP Device Architecture, version 1.0, UPnP Forum, June 13, 2000.
Available at: http://www.upnp.org/specs/architecture/UPnP-DeviceArchitecture-v1.0-20000613.htm.
Latest version available at: http://www.upnp.org/specs/arch/UPnP-arch-DeviceArchitecture-v1.0.pdf.

[2] – Data elements and interchange formats – Information interchange -- Representation of dates and times, International Standards Organization, December 21, 2000.
Available at: ISO 8601:2000.

~~[3] – IETF RFC 2119, Key words for use in RFCs to Indicate Requirement Levels, S. Bradner, 1997.~~
~~Available at: http://www.faqs.org/rfcs/rfc2119.html.~~

Copyright © 2011 UPnP Forum. All rights reserved.